

IT SECURITY

4

IDEE

PER APPROFONDIRE
IL TEMA

Sicurezza
e PMI
Un obiettivo
da perseguire
strategica-
mente

Virtualizzazione
Contenere
i costi e
semplificare
la gestione

E-mail
e internet
Il controllo
in azienda

SFIDE E OPPORTUNITÀ

Una guida per comprendere meglio
i **rischi informatico-aziendali**



La protezione per le piccole imprese sta per diventare ancora più...

semplice

con i servizi Worry-Free™ Business Security

www.trendmicro.it

EDITORIALE

Di fronte alla crescita delle minacce e degli attacchi ai sistemi informativi non sembra crescere in modo adeguato la consapevolezza e la sensibilità al tema della sicurezza informatica.

Complessità e sicurezza

Lo si dice da lungo tempo, tanto che pare essere un "tormentone" ma la domanda da porre è: come mai questo accade? Come mai crescono il valore e l'importanza dei dati affidati alla rete e all'informatica e invece la protezione di quei dati e di quei valori non si adegua alle nuove sfide?

Uno dei fattori decisivi, credo, stia nella difficoltà che le persone in generale hanno ad affrontare i cosiddetti "sistemi complessi" e la rete, e di conseguenza la sua protezione, è indubbiamente diventata un sistema estremamente complesso. Quando pensiamo ai milioni di calcolatori collegati in rete, ai milioni di apparati mobili che diventano sempre più simili a computers e sempre meno a telefoni, abbiamo idea della complessità che si genera?

Di fronte agli attacchi di denial of service perpetrati ai danni di intere nazioni, ci si è domandati se esista una possibile difesa a questa forma di attacco e la risposta non è semplice né tantomeno lineare: di fronte ai sistemi complessi le risposte lineari creano addirittura più guasti che soluzioni.

I sistemi complessi sono una sfida per la nostra mente perché tendiamo a ragionare per modelli di tipo causa-effetto e quindi le risposte più semplici e dirette sembrano anche le più giuste mentre in realtà non è così. Pensiamo a temi come quello dell'ecologia, della fame nel mondo, dell'immigrazione: ogni risposta semplice, magari emotivamente populista, ingenera addirittura un peggioramento del problema che si voleva risolvere.

Per la sicurezza informatica la questione oggi sul tavolo è proprio questa: dobbiamo

"Dobbiamo essere consapevoli del fatto che il nostro pianeta informatico è un sistema estremamente complesso e nessuno possiede la soluzione univoca per proteggerlo"



Gigi Tagliapietra, Presidente del CLUSIT - Associazione Italiana per la Sicurezza Informatica

essere consapevoli del fatto che il nostro "pianeta informatico" è un sistema estremamente complesso e che nessuno possiede la soluzione univoca per proteggerlo.

Bisogna sì utilizzare tecnologie sempre più adeguate alle minacce ma occorre soprattutto adeguare i propri modelli organizzativi. Bisogna certamente costruire difese degli archivi più sensibili ma occorre anche sviluppare una rete di relazioni e di rapporti di fiducia con chi ci potrà aiutare quando dovessimo subire un attacco.

Dobbiamo certamente coltivare e sviluppare le competenze ma dobbiamo anche rendere pienamente consapevoli gli utilizzatori, tutti gli utilizzatori ad ogni livello aziendale e civile.

Un compito arduo, certamente, ma è il solo che ci può garantire la soluzione.



IN EVIDENZA



Claudio Telemo
Comitato Direttivo CLUSIT coordinatore progetti "Rischio IT e piccola impresa"

PAGINA 04

"Molte PMI stentano a riconoscere i vantaggi della sicurezza dei propri sistemi informativi anche quando non si trattano informazioni particolarmente riservate."

MEDIAPLANET

IT SECURITY,
SECONDA EDIZIONE,
SETT/OTT 2010

Managing Director:
Mattias Rentner

Editorial Manager: Gianluca Cò

Designer: Daniela Borraccino

Project Manager:
Giuseppe Baldo
Telefono: +39 02 49 58 36 02
E-mail: giuseppe.baldo@mediaplanet.com

Distribuito con:
Milano Finanza - Italia Oggi
Stampa: RDS WEBPRINTING Srl

Contatti Mediaplanet:
Telefono: +39 02 49 58 36 00
Fax: +39 02 49 58 36 25
E-mail: info.it@mediaplanet.com

Il patrimonio informativo delle imprese si conserva "off - site"

Costituita nel 2009, dal conferimento di ramo aziendale da Data Bank che opera sul mercato dal 1985, **Data Storage Security** ha sviluppato un'articolata gamma di servizi per risolvere tutte le problematiche relative alla protezione dei patrimoni informativi aziendali. "L'evoluzione della domanda del mercato, dice Simone Rossi, presidente del CdA di DSS, vede una tendenza sempre più marcata, da parte delle imprese, alla focalizzazione sui rispettivi core business e all'outsourcing anche di attività strategiche, tra le quali la gestione e la conservazione delle informazioni; per questo, grazie alla nostra indiscussa leadership nazionale nella somministrazione di servizi di custodia e di gestione di archivi elettronici, abbiamo oggi consolidato l'attività di off-site storage".

"Data Storage Security, spiega Rossi, dispone di caveau di massima sicurezza situati in aree dell'intero territorio nazionale strategiche dal punto di vista logistico, in cui sono custoditi esclusivamente supporti informatici; i nostri caveau sono dotati di impianti di ricircolo aria con filtri di depolverizzazione, mentre la sicurezza attiva dei locali è garantita da sistemi anti-intrusione e da sensori



di rilevazione fumi collegati a impianti antincendio con spegnimento automatico a gas; i sistemi sono costantemente monitorati via radio da un istituto di vigilanza che presiede al controllo degli accessi alle sedi operative della Società".

"Tra i nostri punti di forza, conclude Rossi, vi sono la totale reperibilità dei supporti (24 ore al giorno per 365 giorni l'anno) e la grande attenzione alla protezione fisica dei dati: per assicurare le migliori condizioni di conservazione dei supporti ed evitare sofferenze dovute a escursioni termiche e accumuli di umidità, le condizioni ambientali del caveau sono stabilmente mantenute entro i range 18°-24° di temperatura e 45%-55% di umidità, ottimali per la conservazione delle unità ad alta capacità".



Data Storage Security s.r.l.
Via La Bionda, 16 - 43036 Fidenza
Sito: www.dssecurity.it
e-mail: gestione@dssecurity.it
tel 0524 523 521

NEWS

La sicurezza come investimento

La sicurezza, storicamente, è sempre stata una spesa "a fondo perduto": qualcosa di cui era palese la necessità e che si doveva fare e basta - a partire dalle prime palizzate intorno ai villaggi per proteggersi dai predatori notturni. Ancora oggi ragioniamo allo stesso modo, e raramente spendiamo di persona sulla sicurezza a meno di essere stati, ahinoi, vittime di un qualche evento dannoso: ci pesa anche la ricorrenza dell'RC auto (anche se nessuno sano di mente può razionalmente immaginarla facoltativa).

Pensare quindi alla sicurezza come un qualcosa che possa dare un "ritorno", come un BOT o un CCT, è davvero difficile: ma una volta fatto il "salto" mentale si intuisce che questo ROSI - Return On Security Investment - può essere molto interessante e potenzialmente utile. Un anno

fa sì è quindi costituito un Gruppo di Lavoro (GdL) sul tema, su iniziativa di AIEA, Clusit e Oracle, e con la partecipazione di Deloitte, Ernst & Young, KPMG e PriceWaterhouseCoopers.

Il primo frutto del lavoro è stato presentato a Milano il 16 marzo scorso, nel corso del Security Summit.

Un volumetto di 60 pagine, che delinea un metodo di lavoro rigoroso per la valutazione del ritorno di un "investimento" in sicurezza: anche se una trattazione puramente finanziaria è risultata di difficile attuazione (è molto improbabile che si abbiano in modo affidabile tutti i dati che sarebbero necessari), si è constatato che il processo di costruzione del ROSI produce comunque una grande quantità di informazioni estremamente valide come supporto decisionale per il management.



MAURO CICOGNINI,
Comitato Direttivo CLUSIT, Responsabile attività di Formazione

Il documento è stato pubblicato in versione 1.0, ufficialmente migliorabile: c'è un "placeholder" in particolare per i Case Studies, e spazio per altri contributi dal campo, che sono sempre bene accetti.

Anche per meglio supportare l'esecuzione dei Case Studies, da marzo ad oggi il GdL ha affinato gli strumenti operativi, che nella prima versione del documento erano soltanto abbozzati: essi, nella versione più aggiornata, sono pubblicati a fianco del metodo ROSI sul sito rosi.clusit.it. Gli strumenti, così come il testo del metodo, sono rilasciati con licenza Creative Commons Attribution-ShareAlike 2.5: sono quindi liberamente utilizzabili da chiunque, anche a fini commerciali, purché chi li usa ne dichiari l'origine e pubblichi a sua volta con la stessa licenza eventuali opere derivate.

Con gli strumenti migliorati ed i risultati dei primi lavori il GdL sta per dare alle stampe la versione 2.0 del metodo.

Rivolto al mondo dei professionisti dell'Ict e della sicurezza in azienda, Security Summit, dopo le 4 edizioni di Milano e Roma nel 2009 e 2010, si è confermato l'appuntamento più qualificato e approfondito del settore, con un programma convegnistico e formativo che ha visto il coinvolgimento di oltre 150 docenti e relatori. Il prossimo appuntamento è a Milano, dal 15 al 17 marzo 2011. Confermato il format: interventi di scenario da parte di prestigiosi keynote Speakers internazionali, 3 diversi percorsi formativi (tecnico, legale e sulla gestione della sicurezza) e atelier tecnologici, tutti con attribuzione di crediti CPE.



www.securitysummit.it

T-Systems: "dalla protezione IT alla sicurezza globale"

Conoscere il rischio per studiare la difesa

In questi ultimi anni l'esigenza di sicurezza ICT si è andata amplificando di pari passo con il ruolo assunto dai sistemi informativi aziendali e dalla loro progressiva "apertura": accessi eseguiti in mobilità, community sempre più ampie. Per questo, l'approccio alla sicurezza ha superato il concetto tradizionale di controllo perimetrale (firewall), assumendo la connotazione di un vero e proprio processo. Per proteggere in modo efficace il proprio business è oggi necessaria una visione globale



matematico e rendendo anche possibile il calcolo del ritorno sull'investimento e la definizione di un budget adeguato.

e sistemica, partendo dalla conoscenza dei rischi e tenendo conto di tutti gli aspetti: risorse, organizzazione, informazioni, asset. Lo standard internazionale ISO 27001 esprime questa visione, garantendo la corretta implementazione di un Sistema di Sicurezza per la protezione del business. Attraverso l'attenta analisi del rischio, è possibile indirizzare in modo corretto l'investimento in sicurezza, quantificando il costo dai danni provocati da violazioni al sistema infor-

matico e rendendo anche possibile il calcolo del ritorno sull'investimento e la definizione di un budget adeguato.

Offrire sicurezza a 360°

In questo scenario, **T-Systems**, (www.t-systems.it) si propone ai propri Clienti come partner consulenziale affidabile, in grado di garantire la compliance agli standard e alle normative in corso e di fornire servizi di **Security Assessment**: dalle componenti organizzative e di processo a quelle tecnologiche, con un approccio a progetto o con una cadenza periodica. **T-Systems** offre servizi che coprono tutte le tematiche, garantendone la governance attraverso soluzioni che consentono di monitorare, per citarne alcuni, dati relativi alla navigazione internet, accessi alle reti aziendali, log delle applicazioni e dei database, sistemi antivirus e antispyware. Questo approccio consente di elevare il livello di sicurezza, ridurre i rischi, semplificare l'adeguamento alle normative e ottimizzare le operazioni. Un elemento qualificante dell'offerta **T-Systems** è rappresentato dalle soluzioni di **Identity Access Management**, che consentono di definire e attivare politiche di sicurezza a partire dal riconoscimento dell'identità dell'utilizzatore e della determinazione del suo profilo, in termini di diritti e permessi di accesso alle informazioni.

Inoltre, la crescente consapevolezza in fatto di sicurezza di rete che si è andata sviluppando in tempi recenti, ha condotto **T-Systems** a mettere a punto un'offerta modulare e flessibile dedicata al **Managed Network Security**. I vantaggi sono molteplici, tra i quali spiccano l'adozione delle più moderne tecnologie e di strumenti all'avanguardia, la conformità agli standard collaudati e basati su negoziazioni dinamiche delle chiavi di cifratura, la struttura di monitoraggio e gestione centralizzata, competenza e disponibilità nell'elaborare soluzioni personalizzate di network security sulla base di specifici scenari e ambienti



di rete, integrando strumenti di gestione remota e dispositivi di analisi locali.

Le implicazioni che l'interruzione dei servizi informatici può avere sul business, impone alle aziende un sempre maggiore interesse verso il tema della **Business Continuity** e al suo interno, del Disaster Recovery. Si tratta, nel primo caso, di misure atte a prevenire i rischi di inoperatività e assicurare la continuità del servizio nell'eventualità di un evento disastroso. Il **Disaster Recovery** mira invece a minimizzare gli effetti del disastro attraverso il recupero degli elementi computer-based, per la rapida ripresa dei processi di business. In quest'ambito **T-Systems** ha realizzato progetti importanti, supportando i Clienti in vari settori industriali con un presidio dell'intero processo di progettazione e realizzazione e con notevoli riflessi sulla qualità del servizio erogato.

T-Systems propone modelli di sicurezza end-to-end attraverso la perfetta sinergia tra una profonda conoscenza dei diversi rami di business e l'impiego di elevati standard tecnologici, che costituiscono un reale valore competitivo.

...T...Systems...

Rischio informatico nelle piccole imprese

Le piccole e medie imprese rappresentano una componente importante dell'economia italiana ed europea: garantire loro la possibilità di partecipare in sicurezza all'economia globale, anche attraverso la sicurezza dei loro sistemi informativi, è fondamentale. La stessa Agenzia Europea ENISA (www.enisa.eu) ha dedicato diverse iniziative alla sicurezza delle PMI. Tuttavia, molte PMI stentano a riconoscere i vantaggi della sicurezza dei propri sistemi informativi, anche quando non si trattano informazioni particolarmente riservate. Eppure, particolarmente nel caso delle piccole imprese, sicurezza e buona gestione dei sistemi informativi sono affini: sistemi sicuri sono anche sistemi più stabili ed

affidabili, mentre sistemi insicuri comportano più frequenti disservizi, rallentamenti e perdite di dati; insomma, non serve avere grandi segreti perché un piccolo investimento in sicurezza possa essere vantaggioso. Le soluzioni e gli standard usati abitualmente si adattano però meglio alle grandi aziende che attualmente assorbono la maggior parte del mercato della sicurezza, nei settori delle telecomunicazioni, della finanza e delle assicurazioni, mentre si adattano peggio a piccole realtà in cui anche solo il concetto di separazione dei ruoli è impraticabile. Se da una parte è necessario che le soluzioni di sicurezza vengano adattate alle specificità delle singole aziende (aspetto troppo spesso trascurato da chi offre pro-



Claudio Telmon
Comitato
Direttivo CLUSIT
coordinatore
progetti
"Rischio IT e
piccola impresa"

dotti e consulenza), dall'altra questa personalizzazione ha un costo che difficilmente è ragionevole per una PMI. Per superare questa impasse, nell'ambito del progetto Assintel "e-security per le PMI", finanziato da Unioncamere Lombardia e Regione Lombardia, l'attività del CLUSIT è focalizzata proprio sul tentativo di individuare delle modalità di offerta adatte alle piccole realtà, non solo di prodotti da scaffale, ma anche di soluzioni più articolate e di

consulenza.

Da una prospettiva diversa, se è vero che la singola PMI si può sentire poco "appetibile" ad esempio per lo spionaggio industriale via Internet (ma è recente la notizia del worm Stuxnet che effettua questo tipo di attività in modo automatico addirittura su sistemi SCADA), è anche vero che in un contesto di insicurezza generalizzato, quando una PMI diventa interessante è molto probabile che sia vulnerabile. La sicurezza e la sensibilizzazione delle PMI è quindi un obiettivo da perseguire strategicamente creando un'attenzione diffusa al problema, e non può essere lasciato solo alla buona volontà delle singole piccole imprese.

Sicurezza delle carte di pagamento

Acquistare con una carta di pagamento invece del contante è sempre più comune anche in Italia, sia nei negozi sia on-line; al contempo crescono però anche le frodi, troppo spesso agevolate dalla poca consapevolezza di clienti ed esercenti. I maggiori brand (Visa, MasterCard etc.) si sono coalizzati da anni per aumentare la sicurezza delle carte e hanno dato vita a varie iniziative per tutelare i consumatori. Lo standard PCI-DSS, dedicato alla sicurezza dei dati delle carte si applica agli esercenti e ai loro fornitori; molto attento alle operazioni elettroniche, è alla base di programmi sponsorizzati dalle banche, i quali introducono sanzioni per gli inadempienti e agevolazioni per chi si adegua. PCI-DSS raccoglie una serie di misure per ridurre le frodi, che vanno dalla gestione delle tecnologie informatiche alla conservazione del cartaceo e all'organizzazione aziendale. Questo approccio, già applicato con successo negli USA, sta ora sbarcando in Europa. Per approfondire il tema si segnala il gratuito quaderno CLUSIT (http://www.clusit.it/download/Q08_web.pdf).

Fabio Guascogni,
Team Manager



Proteggere dalle intercettazioni illegali

"Per molte aziende, dice Carlo Marchini, amministratore delegato di PrivateWave Italia, la riservatezza delle chiamate telefoniche (o quanto meno di alcune conversazioni particolarmente importanti) è un'esigenza imprescindibile. Purtroppo, le normali linee telefoniche non garantiscono questo tipo di sicurezza e, per contro, vi sono casi in cui non è possibile incontrarsi di persona per discu-

tere i dettagli di una trattativa di lavoro e quindi la discussione stessa deve essere necessariamente condotta per telefono. Per questo, è fondamentale poter comunicare in modo sicuro con telefoni fissi e cellulari, sia in entrata che in uscita".

"Oggi, la moderna tecnologia ha risolto questo problema, spiega Marchini, facendo in modo che, quando si desidera essere sicuri di non essere ascoltati, il te-



Carlo Marchini
Amministratore
Delegato
di Khamsa

lefono concordi con la controparte una chiave di sessione relativa a quella specifica telefonata che, al termine della conversazione, viene distrutta; naturalmente, le telefonate devono avvenire tra i dipendenti di una azienda; al momento della telefonata, sarà sufficiente digitare un prefisso prestabilito prima del numero da chiamare e il software si attiverà automaticamente, proteggendo la telefonata da ogni tentativo di intercettazione; in questo modo si possono effettuare chiamate cifrate senza modificare l'uso normale del telefono".

Da PrivateWave Italia, Enterprise VoIP Security Suite: dalla ricerca, l'eccellenza tecnologica nel campo della sicurezza

PrivateWave Italia, società specializzata nello sviluppo di tecnologie per la sicurezza delle comunicazioni, fa della ricerca e dell'eccellenza tecnologica il suo punto di forza. Si presenta ora sul mercato con **Enterprise VoIP Security Suite**, la soluzione più avanzata di convergenza fisso-mobile per tutelare le conversazioni

aziendali. **Enterprise VoIP Security Suite** protegge le telefonate lungo tutto il canale voce, dai telefoni fissi ai cellulari (e viceversa). Inoltre, se un'azienda possiede già un centralino VoIP, non è necessario sostituirlo ma sarà sufficiente affiancargli il security gateway e utilizzare il software PrivateGSM per telefonare in modalità

protetta, integrando la sicurezza pre-esistente nel perimetro aziendale con quella verso l'esterno. Se invece l'azienda non utilizza ancora un centralino VoIP, potrà dotarsi del sistema Farosec di PrivateWave, con il quale sarà possibile telefonare in sicurezza verso i telefoni fissi aziendali e verso i cellulari che hanno installato PrivateGSM. Grazie a **Enterprise VoIP Security Suite**, le comunicazioni tra imprese e professionisti che utilizzano la soluzione avverranno quindi nella più totale privacy. La flessibilità delle soluzioni proposte permette inoltre ad ogni azienda di trovare la configurazione ottimale minimizzando i costi e l'impatto sulle infrastrutture esistenti.

PrivateWave

numero verde: 800 990036

www.privatewave.com info@privatewave.com

Servizi SaaS, sicurezza informatica a misura di PMI

Con oltre 2.300 nuovi codici maligni registrati ogni ora a livello mondiale, per le aziende diventa sempre più difficile tenere il passo con la complessità degli attacchi informatici e avvalersi di adeguati e sistemi di sicurezza. A maggior ragione per le imprese di piccole e medie dimensioni che spesso dispongono di risorse IT limitate e non hanno né il tempo né le competenze specifiche per la gestione della sicurezza. Tra le soluzioni studiate per rispondere a queste esigenze sono i servizi di protezione erogati in modalità Software-as-a-Service (SaaS). I servizi SaaS, noti anche come servizi "in hosting", convertono il software da un 'prodotto' in un 'servizio' ovviando all'esigenza di acquistare, installare e gestire il software stesso con conseguenti implicazioni di costi di infrastrut-



Carla Targa
Marketing &
Communication
Manager di
Trend Micro Italy

tura e personale specializzato. Le aziende potranno, quindi, "affittare" la soluzione di sicurezza pagando su base mensile o annuale un canone. Questo approccio permette una forte riduzione dei costi diretti (ad esempio per l'hardware del server) e semplifica sia l'implementazione sia l'amministrazione della soluzione stessa, ottimizzando gli investimenti. Può, inoltre, aumentare la qualità e l'affidabilità della soluzione offrendo un ritorno sull'investimento (ROI) più rapido e proficuo a confronto delle tradizionali soluzioni in locale.

Un altro fondamentale vantaggio che scaturisce dalla scelta di affidarsi ai servizi in hosting è la possibilità di poter contare sulla competenza del provider che si occupa completamente della gestione del servizio, oltre che del suo costante aggiornamento, permettendo all'azienda di concentrarsi sul proprio business. Con oltre vent'anni di esperienza nel mercato della sicurezza, Trend Micro è in grado di offrire alle Piccole e Medie Imprese servizi di protezione pensati appositamente per le loro esigenze: veloci da installare, semplici da configurare ed efficaci nel bloccare ogni genere di minaccia. In particolare, i servizi in hosting di Trend Micro comprendono Worry-Free Business Security Services, che offrono monitoraggio e protezione automatica a tutti i computer, sia

utilizzati in ufficio sia all'esterno dagli utenti mobili, e Hosted Email Security, la soluzione specifica per la protezione sempre aggiornata della posta elettronica da minacce come lo spam o il phishing. "In una congiuntura economica difficile come l'attuale, le soluzioni SaaS, per i significativi vantaggi offerti, diventano un modello ancora più valido per garantire la protezione dei dati nelle aziende", commenta Carla Targa, Marketing & Communication Manager di Trend Micro Italy. "Poiché il software è disponibile su richiesta, esso può essere aggiornato o ampliato immediatamente, in modo da soddisfare requisiti di sicurezza in costante evoluzione: è sufficiente aumentare o ridurre il numero di utenti coperti dall'abbonamento", conclude Carla Targa.



www.clusit.it

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, è la più importante e autorevole associazione italiana nel campo della sicurezza informatica.

Oggi rappresenta oltre 500 organizzazioni, appartenenti a diversi settori: Ricerca, Industria, Commercio e Distribuzione, Banche e Assicurazioni, Pubblica Amministrazione, Sanità, Consulenza e Audit, Servizi, Telecomunicazioni, Informatica.

Furto d'identità (e di soldi) in quattro mosse!

Sei sicuro che i soldi sono al sicuro nel tuo conto corrente?

Il tema che riguarda l'identità nell'era digitale è importante, ma diventa estremamente importante, quando il suo furto produce danni patrimoniali o penali. Dietro a ogni furto d'identità riuscito, si cela la falla di un "sistema di autenticazione".

I sistemi di autenticazione sono quei sistemi (informatici o tradizionali) che identificano le persone. Il processo di identificazione si fonda sulle "credenziali di autenticazione". L'esito positivo dell'attività di autenticazione può essere definito come accreditamento. Sull'accreditamento, a loro volta, si fondano i "sistemi di autorizzazione", ovvero quei sistemi che definiscono i privilegi di una persona accreditata. Al ladro d'identità, le informazioni personali della vittima interessano al fine di superare il processo di autenticazione, e ottenuto l'accreditamento, poter illegittimamente utilizzare i privilegi della vittima. Il furto di identità non è fine a se stesso ma è sempre funzionale alla commissione di almeno un altro reato, se non di una lunga serie. Inoltre, quell'identità rubata è una merce rivendibile sul mercato nero della c.d. "Underground Economy", che, negli ultimi mesi, ha visto una pericolosa escalation, arrivando a "fatturare" cifre uguali o addirittura superiori al traffico di armi, al traffico di esseri umani e di droga. L'attuale "insicurezza" che è alla base del furto di identità è alimentata da diverse cause, una delle principali, risiede nell'ambiguità propria di un sistema ibrido (tradizionale-elettronico)



Andrea Violetti

Presidente Associazione
Informatici Professionisti

che, anziché caratterizzare un momento transitorio di passaggio dalla cultura tradizionale (carta) a quella elettronica (byte), costituisce la normalità. È proprio questa normalità che ritroviamo nella circolare ABI (Prot. SP/001812 Roma, 9 aprile 2004) riguardo appunto agli incassi commerciali interbancari.

Per velocizzare tali processi una banca domiciliataria deve rispondere in via telematica entro 7 giorni, in termini di accettazione o diniego, per una richiesta di incasso RID da una banca di allineamento. Questo significa che in applicazione del regolamento Sitrad-SIARI-ICI-002, la banca domiciliataria deve rispondere alla banca di allineamento con l'accettazione o il diniego di una disposizione di incasso da essa ricevuta. La ris-

posta viene data per vie telematiche controllando in automatico solo: NOME, COGNOME, CODICE FISCALE E IBAN; sempre per brevità, la "verifica della firma" non viene fatta e non si viene avvisati. La vulnerabilità, di questo processo misto, tradizionale-elettronico, per la "truffetta", è servita.

L'Osservatorio sulla Privacy e Sicurezza Informatica di Associazione Informatici Professionisti, ha effettuato un semplice test, scaricabile in versione integrale, che dimostra come sia purtroppo facile reperire dati riferibili alla nostra sfera privata.

La soluzione che auspichiamo è che ABI intervenga nel regolamento tornando alla presentazione del RID presso la propria filiale o più modernamente ponendo la richiesta di pagamento in attesa di una accettazione/diniego nell'home banking del cliente. Ci piace concludere questa nostra disavventura citando Ben Bernanke, Presidente di Federal Reserve, che nel 2009 è stato derubato della sua identità, per dividere con lui il "mal comune" e per invitare tutti voi a controllare i vostri conti correnti.

L'articolo in versione integrale è scaricabile da www.aipnet.it o da www.opsi.aipnet.it. È stato redatto in collaborazione con: l'Avv. Alessandro Frillici (Cism-Cgeit) Coordinatore Opsi, Alessio Penasilico, Corrado Giustozzi, Marco Calamari, Matteo Flora, Paolo Giardini, Raoul Chiesa.

Virtualizzazione: quali vantaggi per la sicurezza delle imprese italiane

La Virtualizzazione sta cambiando il modo di lavorare in molti comparti dell'ICT, estendendosi a imprese diverse per dimensioni e tipologie di mercato. Non ci soffermeremo sui vantaggi tecnico/economici che spingono ad adottare questa tecnologia, già ampiamente pubblicizzati: indubbiamente va segnalata la facilità e la velocità con cui è possibile creare, testare od eliminare nuovi ambienti operativi. Semplicità e reattività determinano una maggiore capacità di comprendere e risolvere i problemi, e pertanto una maggiore sicurezza, soprattutto nella piccola e media impresa.

Per fare un esempio, le infezioni da worm possono essere mitigate semplicemente ed economicamente, tramite l'isolamento logico dei servizi in macchine virtuali (VM) differenti, compartimentazione che era difficile da realizzare in passato per i costi dell'HW o per la limitazione degli spazi fisici.

Queste tecnologie, infatti, hanno creato le condizioni per migliorare l'affidabilità e la continuità operativa: le risorse economiche risparmiate possono essere investite per assicurare la ridondanza dei servizi, tramite cluster o sfruttando le potenzialità di features delle soluzioni di virtualizzazione: ne è un esempio la possibilità di "spostare" l'esecuzione di una VM da un sistema a un altro in tempo reale, vuoi per svolgere manutenzione o per risolvere un pro-

blema di natura hardware. Analogamente, la virtualizzazione permette di ridurre gli investimenti "a priori" nella messa in esercizio di nuove applicazioni aziendali, senza impatti negativi sull'affidabilità: all'aumentare dei carichi di lavoro, è possibile riassegnare le risorse disponibili per le singole VM (CPU, RAM, Disco), o riorganizzare la distribuzione delle VM sui diversi server o sedi. Il tutto in tempo reale e senza interruzioni di servizio. Anche su procedure già in essere (ed essenziali) le ricadute sono positive: i backup sono più semplici. Ad esempio è sufficiente copiare l'intera VM, anche in tempo reale. Di conseguenza i restore sono più veloci e meno complessi. In aggiunta, l'HW sul quale si ripristina il servizio può essere diverso (necessario in caso di danni fisici) o dislocato su altre sedi. Ripristinare una VM, in questi casi, permette, infatti, di conservare i programmi installati e tutte le configurazioni e personalizzazioni fatte.

La portabilità delle VM su hardware impone di riconsiderare l'importanza del configuration/asset management, essendo possibile predisporre "template" di VM che potranno poi essere clonate per dare vita a sistemi già pronti per il setup dei servizi. Il template, in fase di creazione, può essere reso più sicuro svolgendo attività di hardening e installando i necessari software di sicurezza (an-

tivirus, etc...). Disponendo così di un parco di sistemi omogeneo, derivato da un numero limitato di template, possono essere create VM ad hoc per il test di aggiornamenti software e di nuovi prodotti. Esistono inoltre soluzioni pensate per mantenere sicuri i template stessi, evitando infezioni da "accensione di VM obsolete e vulnerabili". A fronte di quanto detto è tuttavia necessario sottolineare un aspetto importante: la virtualizzazione può aiutare a contenere i costi e a semplificare la gestione ma deve essere comunque subordinata ad una corretta pianificazione ed implementazione. Se per l'azienda è una nuova tecnologia, avere chiari gli obiettivi da raggiungere ed affidarsi ad un professionista esperto è in molti casi la strada corretta per massimizzare i benefici di sicurezza e acquisire il necessario know how per mantenerli tali nel tempo.



Luca Bechelli
Security Consultant,
C.D. e Comitato
tecnico Scientifico Clusit



Alessio L.R. Pennasilico
Security Evangelist,
C.D. e Comitato
tecnico Scientifico Clusit

Il controllo di e-mail e internet in azienda

Quali sono i limiti alla possibilità del datore di lavoro di controllare l'utilizzo di internet e della posta elettronica da parte dei dipendenti?

L'art. 4 dello Statuto dei Lavoratori (L. 300/1970), pur stabilendo al primo comma il divieto generale di utilizzo di "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", prevede al secondo comma che "Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna (omissis)".

Il principale problema è quindi definire quando i controlli posti in essere a tutela del patrimonio aziendale e tesi ad accertare comportamenti illeciti dei lavoratori (i cd. "controlli difensivi") rientrino nell'applicazione dell'art 4 comma 2 dello Statuto dei lavoratori. Una sentenza della Corte di Cassazione (n. 4375 del 23.02.2010) ha stabilito in un caso concreto che "L'installazione e l'utilizzazione di un programma informatico che consenta al datore di lavoro di

controllare gli accessi dei dipendenti a siti internet devono essere autorizzate con accordo sindacale o dalla Direzione provinciale del lavoro.

In mancanza dell'autorizzazione, i dati acquisiti non possono essere utilizzati per eventuali contestazioni disciplinari". Secondo la Suprema Corte non è possibile escludere i controlli diretti a accertare comportamenti illeciti dei lavoratori dall'applicazione dell'art. 4 comma 2 della L. 300/1970, "quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal contratto di lavoro e non la tutela di beni estranei al rapporto stesso".

Parte della dottrina ritiene che esolino dall'applicazione della suddetta norma i controlli diretti a tutelare l'azienda dall'avvenuto compimento di illeciti di natura penale nei suoi confronti ma non, per esempio, apparecchiature e applicativi che consentono un monitoraggio indiretto e costante della prestazione lavorativa, seppur installati per esigenze di sicurezza aziendale.



Gabriele Faggioli
Comitato Direttivo Clusit. Resp. ufficio legale ed esperto in informatica & telecomunicazioni law.

IDEA
4

Sotto l'Alto Patronato della Presidenza della Repubblica



SICUREZZA SUL LAVORO. LA PRETENDE CHI SI VUOLE BENE.

Qualunque azienda tu diriga, far tornare a casa chi lavora è un dovere. E la cultura della sicurezza è la miglior prevenzione degli infortuni. Segui le regole che tutelano il bene più importante per la tua azienda: te ed i tuoi collaboratori. Informati su

www.sicurezza.lavoro.gov.it



Ministero del Lavoro
e delle Politiche Sociali

PecStock



PecStock è la soluzione semplice ed efficace che permette di risolvere i problemi di archiviazione e consultazione della Posta Elettronica Certificata (PEC). Si installa in un attimo ed è subito funzionante, senza complicate e lunghe configurazioni. Non dovete cambiare abitudini o programma di posta elettronica: PECStock si integra perfettamente in Microsoft® Office Outlook® e non richiede praticamente alcun intervento da parte dell'utente per le funzioni di archiviazione.

La linea aVtomic Solution: **ADTOMIC** **Snuko** **Sp@mLimitz** **PecStock**

blufile
SECURITY SOLUTION

www.blufile.it
info@blufile.it

www.avtomic.com
support@avtomic.com

Blufile, distributore esclusivo di aVtomic antivirus, vanta dieci anni di esperienza in campo informatico ed una rete di vendita che conta 900 rivenditori su tutto il territorio nazionale. Entra a far parte della nostra squadra, diventa anche tu rivenditore Blufile.