ISACA VENICE Chapter

Quaderni

Vulnerability Assessment e Penetration Test

Linee guida per l'utente di verifiche di terze parti sulla sicurezza ICT

ISACA VENICE Chapter
mail: info@isacavenice.org
sito: www.isacavenice.org

Trust in, and value from, information systems
Venice Chapter

INDICE

Premessa

In assenza di termini di riferimento oggettivi le misure di sicurezza adottate da ciascuna organizzazione sono naturalmente correlete alla percezione del rischio. Dove tale percezione è chiara e condivisa le misure di sicurezza sono predisposte in modo quasi naturale.

Infatti ogni azienda si assicura contro eventi come l'incendio ed il furto, e anche se assicurata nessuna azienda tralascia di chiudere a chiave gli uffici, di far installare un antifurto nel magazzino, o anche di ingaggiate guardie giurate per controllare gli stabili.

Spesso invece le misure volte a prevenire il manifestarsi di rischi attinenti la sicurezza logica, quella che difende le reti ed i sistemi aziendali da accessi indesiderati e da modifiche malevole, vengono trascurate, a volte anche sotto le spinte competitive a comunicare di più, a integrare i propri dati con quelli dei propri clienti o fornitori, a diffondere il proprio know how tra i dipendenti.

E, contemporaneamente, l'azienda deve continuare a proporre prodotti sempre migliori, con caratteristiche diverse, con costi più bassi rispetto alla concorrenza. Qual' è il senso di spendere tanto per sviluppare un nuovo prodotto o un nuovo servizio, per poi non proteggere adeguatamente i risultati di questo investimento?

Tuttavia un accesso indesiderato o fraudolento ai sistemi informativi di un’azienda può causare danni anche gravi, che possono arrivare a mettere a repentaglio la sopravvivenza aziendale. Ad esempio, nell'estate del 2012 una media azienda del padovano è stata sottoposta ad attacco da parte di enti esterni.

Non è chiaro quale fosse l'obbiettivo dell'attacco, ma nei fatti sono stati cancellati tutti i dati, inclusi i dati gestionali, i documenti di progetto e quelli commerciali: il danno subito è stato ingente, con un fermo di diversi giorni. Il fatto è stato denunciato alla polizia postale, e sembra che l'obiettivo dei malviventi fosse quello impadronirsi di alcuni segreti industriali. Questa azienda, come quasi tutte quelle che subiscono tali incidenti, non vuole tuttavia essere citata.

Un penetration test ha una utilità analoga a quella di un controllo notturno: un ente esterno, su richiesta, controlla periodicamente che l'azienda sia sufficientemente protetta da accessi indesiderati dall'esterno. I risultati consentono di capire i punti deboli che potrebbero essere sfruttati da malintenzionati, e quindi di porvi rimedio evitando gli errori banali e limitando i danni.

Numerosi documenti discutono le attività di analisi della sicurezza quali vulnerability assessment e penetration test dal punto di vista del fornitore, proponendo metodologie e pratiche di riferimento. Un numero minore di documenti è invece dedicato al punto di vista del cliente, e ancora più ridotta è l’attenzione rivolta alle PMI, piccole e medie imprese.

Obiettivo di questo documento è circostanziare il valore aggiunto di un buon penetration test per una PMI, descrivere le caratteristiche desiderabili per l'esecuzione di un penetration test e suggerire linee guida per la selezione dei fornitori atti a svolgere attività di tale natura. Sono state definite in particolare buone pratiche e aspetti critici cui porre attenzione nel commissionare un Penetration Test da parte di una PMI.

Non vi è dubbio che se occorre un livello di sicurezza elevato, bisogna tener conto di tutta la complessità della gestione della sicurezza, fra cui un affinamento dei dati, delle misure e delle tecnologie corrispondenti. A questo proposito, le idee e il modello qui presentati sono ritenuti coprire un livello di sicurezza accettabile per le piccole organizzazioni, i cui investimenti in sicurezza sono più ridotti. Forme più avanzate di sicurezza (ad esempio, componenti infrastrutturali critiche) richiederebbero una trattazione più ampia che va al di là dello scopo del presente documento.

Il valore del patrimonio immateriale delle PMI è spesso noto soltanto in parte. Questo è tipicamente il caso di uno degli asset più importanti, vale a dire, le informazioni. È indispensabile che i responsabili delle PMI comprendano il valore delle informazioni contenute all’interno del proprio sistema aziendale e dispongano di un quadro entro il quale valutare ed implementare la sicurezza delle informazioni.

Prendendo spunto dalla esecuzione di una analisi da parte di un fornitore esterno si suggerisce di avviare, comprendere ed attuare processi formali di sicurezza del patrimonio informativo, comprendenti anche misure tecniche ed organizzative. Senza misure di questo tipo, l’azienda può risultare seriamente danneggiata da minacce involontarie/attacchi deliberati ai propri sistemi informativi, tali da poter determinare in ultima analisi la cessazione dell’attività.

Anche se è la formula più economica per la PMI abbiamo scartato autovalutazioni specifiche di Penetration Test che invece è accettabile se ci si limita ad analisi automatiche di livello più basso denominate Vulnerabilty Assesment. Pertanto la metodologia proposta serve per identificare team di specialisti indipendenti esterni (il cosiddetto "Tiger Team)[1]".

Ringrazio tutti i partecipanti al gruppo di approfondimento per l'impegno e la disponibilità offerta nella realizzazione di questo documento.

Luca Moroni

Venezia, 16 aprile 2014

GRUPPO DI APPROFONDIMENTO

Coordinamento:

Luca Moroni	CISA, ITIL v3 Foundation (Via Virtuosa)

Controllo Qualità:

Mauro Bregolin	CISA, CRISC, QSA, COBIT5Foundation (Kima – Gruppo IKS)
Orillo Narduzzo	CISA, CISM, CGEIT, CRISC, CCSA, COBIT5Foundation, COBIT5TR
Andrea Pederiva	CISA, COBIT5Foundation, COBIT5TR
Pierlugi Sartori	CISSP, CISM, CGEIT, CRISC, MBCI (Informatica Trentina SPA)

Gruppo di approfondimento:

Luca Moroni	CISA, , ITIL v3 Foundation (Via Virtuosa)
Francesco Beni	CRISC, PMP, C|CISO, LA 27001, LA 22301, MBA (Almaviva SPA)
Sergio Boso	LA 27001
Luigi Bovino	CISA (Deloitte ERS)
Giuseppe Esposito	CISA, PMP, LA27001, LA22301, LA9001, ITIL-V3 Foundation, ISO2000 Foundation
Claudio Fusco	CISA
Marco Ivaldi	OPSA, OPST, OWSE, PCI QSA, PCI ASV, Prince2 Foundation (@ Mediaservice.net Srl)
Andrea Pontoni	CISA, COBIT5Foundation, COBIT5TR
Andrea Tonini	CISA, ITIL v3 Foundation, ISO2000 Foundation (YARIX Srl)

Si ringraziano in particolare @ Mediaservice.net Srl e Yarix Srl per i contributi professionali e i contenuti condivisi con il Gruppo di Approfondimento

[1] http://en.wikipedia.org/wiki/Tiger_team

Scopo del Documento

L'IT di tutte le imprese, in quanto connesso con servizi e ambienti esterni, è soggetto ad attacchi e vulnerabilità che possono compromettere la sicurezza dei dati aziendali. L'esecuzione di sistematici Vulnerability Assessement e Penetration Test è ormai una buona pratica adottata generalmente per analizzare il grado di sicurezza rispetto a minacce esterne. In tale contesto il supporto offerto all'Utente ed alla Piccola-Media Impresa è suscettibile di miglioramenti.

Per offrire un contributo alla selezione di un approccio adeguato a tali stakeholder, ISACA VENICE Chapter ha avviato un Gruppo di Approfondimento per redigere delle linee guida per l'Utente e le PMI nell'utilizzo di verifiche di sicurezza, in particolare Vulnerability Assessment e Penetration Test svolte da terze parti.

Lo scopo del presente documento è quello di illustrare i risultati ottenuti dal Gruppo di Approfondimento, stimolando nei lettori l'interesse all'argomento trattato ed agli opportuni approfondimenti.

Destinatari del documento

Questo articolo si pone come obiettivo quello di definire i requisiti che una azienda deve valutare nel commissionare un servizio di Penetration Test ad un fornitore esterno.

I destinatari naturali del documento sono i responsabili che nella PMI intendono commissionare una analisi di sicurezza sulle risorse informatiche dell'azienda che vi possono trovare, oltre ad un'esposizione razionale dei concetti ed un'omogeneizzazione delle definizioni, lo spunto per la pratica creazione di una metodologia più specifica sulla gestione del rischio IT, utile nel proprio ambito lavorativo.

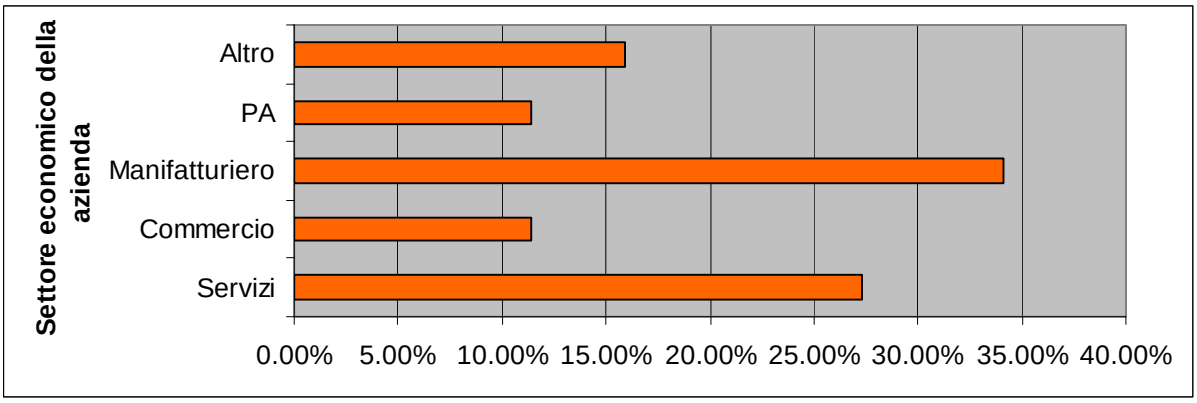
Quick Survey

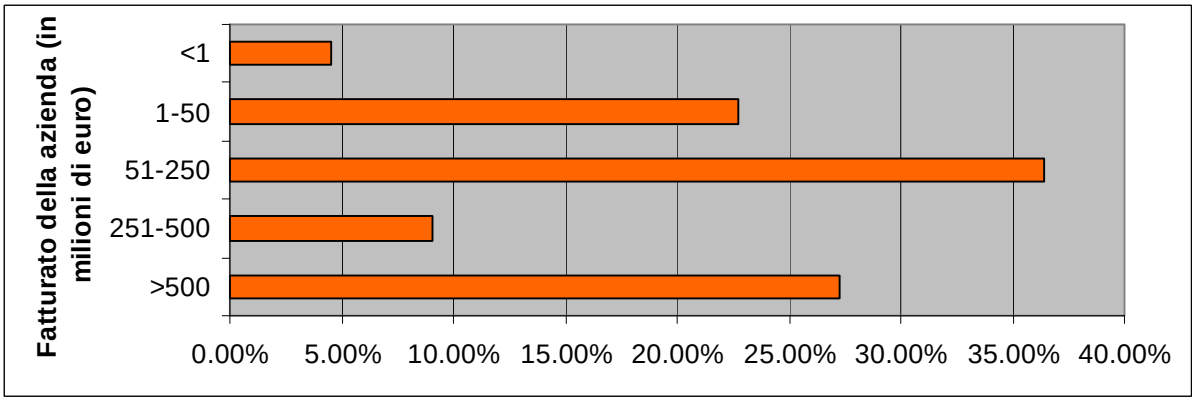
Il Gruppo di Approfondimento ha predisposto un Quick Survey per rilevare più approfonditamente il livello di utilizzo di queste tecniche da parte delle imprese del Nord Est d'Italia.

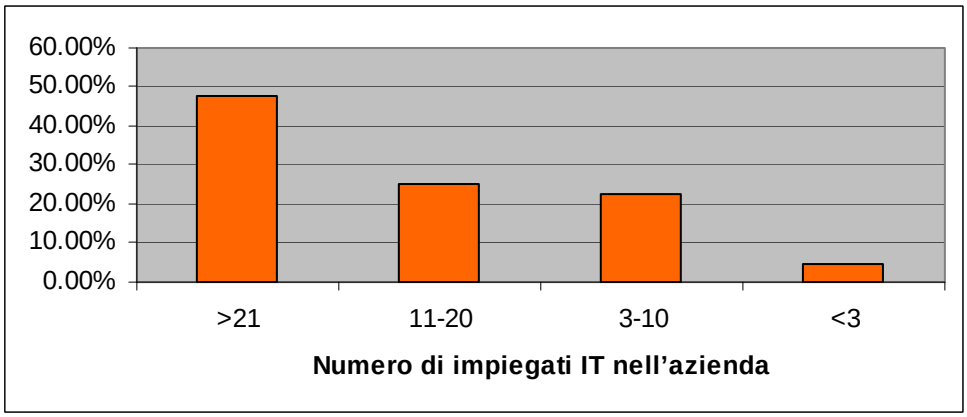
Nello specifico questi sono stati i quesiti:

- Ogni quanto svolge un PENETRATION TEST
- Su quale base sceglie il fornitore
- Ha mai svolto delle analisi di sicurezza nel perimetro interno. Dove l'analisi è composta da una serie di processi che simulano le azioni normalmente svolte da un dipendente o consulente nella rete interna.
- Quale sono gli aspetti per le attività svolte in passato di cui sono stato PIU' soddisfatto (anche più di una risposta)
- Quale sono gli aspetti per le attività svolte in passato di cui sono stato MENO soddisfatto (anche più di una risposta)

Tale indagine trova riscontro e viene utilizzata in più punti del presente documento fornendo anche degli spunti di riflessione. Il campione delle aziende che hanno risposto costituito da 50 questionari compilati è suddiviso nel seguente modo:


Settore economico della azienda
Altro
PA
Manifatturiero
Commercio
Servizi
0.00% 5.00% 10.00% 15.00% 20.00% 25.00% 30.00% 35.00% 40.00%


Fatturato della azienda (in milioni di euro)
<1
1-50
51-250
251-500
>500
0.00% 5.00% 10.00% 15.00% 20.00% 25.00% 30.00% 35.00% 40.00%


60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
>21
11-20
3-10
<3
Numero di impiegati IT nell'azienda

1 Introduzione

In un periodo di contenimento dei costi quelli sulla sicurezza riguardano oggi: costo monetario dei dispositivi, protezioni, strumenti, servizi, aggravio dei tempi per attenersi a procedure, aumento di complessità operativa. Ma la Sicurezza è anche investimento, se si considerano le conseguenze della assenza o inadeguatezza delle misure protettive. Il problema è come bilanciare costi con esigenze pertanto rischi con protezioni.

Il Global Risk Report 2012 del World Economic Forum, analizzando le 50 principali minacce globali dei prossimi 10 anni e classificandole per impatto e probabilità, nella sezione “Rischi tecnologici” pone al primo posto il Cybercrime.

La vulnerabilità nel settore dell‘information security è definita come elemento di un particolare settore che possa compromettere la sicurezza informatica dell’intero sistema.

Per sicurezza informatica si intende la tutela delle seguenti caratteristiche: confidenzialità, integrità, disponibilità ed autenticazione. Qualora una debolezza del sistema informativo comprometta una delle sopradette caratteristiche si riscontra una vulnerabilità.

L’analisi di vulnerabilità è il passo successivo alla visione dell’architettura, definizione degli obiettivi e valutazione dei beni aziendali. L’obiettivo di un test è quello di verificare il comportamento a fronte di una sollecitazione in una particolare condizione e verificare lo scostamento rispetto alle attese.

Le vulnerabilità sono individuabili principalmente in tre categorie, che rappresentano tre diversi livelli da analizzare per la sicurezza: la rete, i sistemi e gli applicativi. Successivamente sono riportate le definizioni dei livelli che analizzeremo e le relative problematiche.

1.1 Richiami di legge

L’adozione di specifiche misure di sicurezza logica costituisce in sempre più numerosi settori un obbligo normativo previsto dalla legge o dai regolementi di settore. Vedi ad esempio le norme concernenti i settori finanziario, assicurativo e delle carte di credito.

Per il settore delle comuinicazioni elettroniche ad esemio dal primo giugno 2012 è in vigore il Decreto legislativo 28 maggio 2012, n. 69 che recepisce, tra l'altro, la direttiva 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.

Grande rilievo assume la sicurezza e l'integrità delle reti di comunicazione elettronica accessibili al pubblico, con riferimento alle quali il ministero individua adeguate misure di natura tecnica e organizzativa per assicurare la sicurezza delle reti e dei servizi di comunicazione elettronica accessibili al pubblico, nonché per garantire l'integrità delle reti.

Oggi il fornitore di un servizio di comunicazione elettronica accessibile al pubblico (ma è prevedibile che sia recepito globalmente), oltre ad istituire una politica di sicurezza per il trattamento di dati personali, deve mettere in atto regolarmente le misure di:

- monitoraggio;
- prevenzione;
- correzione;
- attenuazione.

Le autorità nazionali, al fine di difendere gli interessi dei cittadini, devono assicurare un elevato livello di protezione dei loro dati personali e della loro vita privata.

Devono dotarsi pertanto di mezzi necessari per:

- disporre dei dati completi ed affidabili sugli incidenti di sicurezza che hanno compromesso i dati personali degli utenti;
- controllare le misure adottate dai fornitori;
- diffondere le best practices tra i fornitori.

Il fornitore, appena viene a conoscenza di una violazione che comporta accidentalmente o in modo illecito la distruzione, la perdita, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio, deve notificarla all'autorità nazionale competente includendo:

- informazioni di dettaglio sulla violazione;
- le conseguenze della violazione;
- le misure proposte o adottate per porvi rimedio.

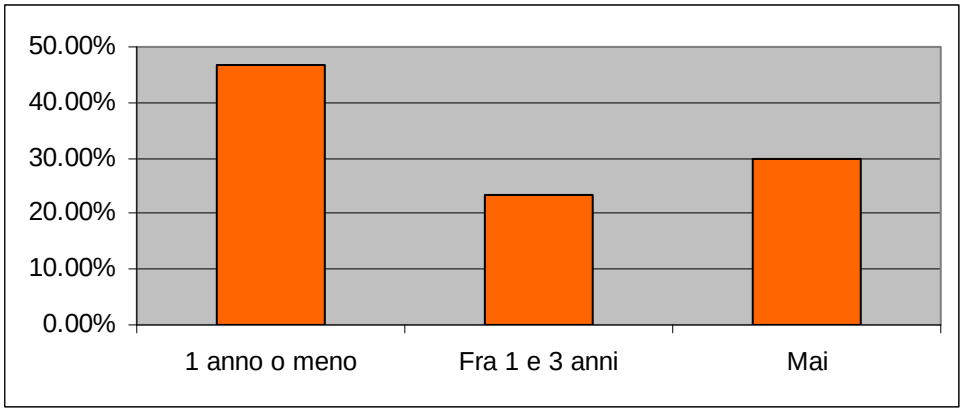
L'esecuzione del servizio di verifica dei parametri funzionali della rete (penetration/intrusion test) risponde inoltre alle prescrizioni del Testo Unico materia di protezione dei dati personali e precisamente a quanto indicato nel Disciplinare Tecnico in materia di misure minime di sicurezza - Allegato B al D.L. 196/2003. In particolare il punto 16 del citato Allegato B specifica le regole da seguire contro l'accesso abusivo dei sistemi informatici, secondo quanto indicato dall'articolo 615-ter del Codice Penale.

In generale per i responsabili ICT di tutte le organizzazioni per le quali la continuità operativa e/o la protezione delle informazioni e della proprietà intelletuale costituiscono fattori critici di successo, assicurarsi che i controlli di sicurezza posti in essere dalle proprie strutture ICT sono in linea con le normative applicabili e le buone pratiche di settore, costituisce elemento imprescindibile per l'esercizio diligente e professionale dei propri compiti.

1.2 L' analisi del livello di sicurezza IT

L'analisi di Vulnerabilità è un passo necessario per fotografare le problematiche del sistema informativo. E' il passo necessario per sapere le debolezze del sistema a 360 gradi, per poi decidere come proteggere il sistema e le trasmissioni dati. E' un passo necessario poiché spesso valutare a priori il problema e risolverlo senza una precedente analisi di vulnerabilità porta a delle protezioni provvisorie, e spesso inutili, con il conseguente danno economico.

Sulla base di una recente indagine svolta da ISACA VENICE CHAPTER sulla frequenza con cui aziende dell'area Nord Est svolgono una analisi di sicurezza è emerso questo dato indicativo.

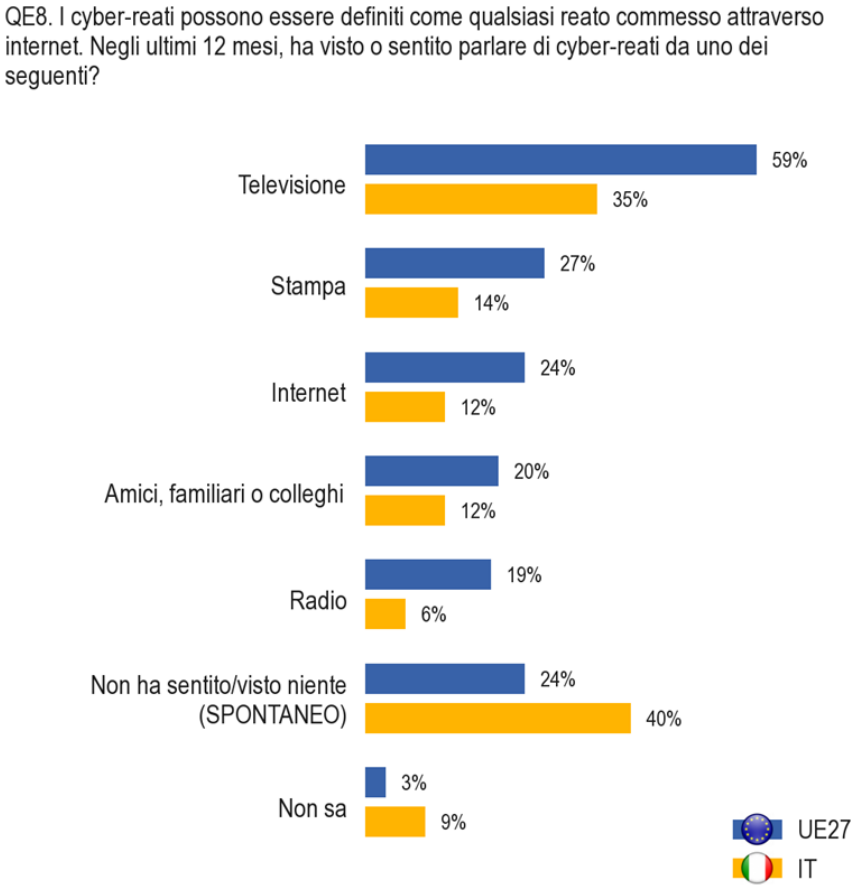


Considerando le statistiche sugli incidenti informatici, la maggior parte degli attacchi (circa il 65%) sono stati realizzati con tecniche ben note. Per cui con la realizzazione di un Penetration Test queste vulnerabilità potrebbero essere mitigate, se non eliminate, con una certa facilità.

Come indicato dal Clusit nel report 2012 i rischi informatici come lo spionaggio industriale o l'accesso abusivo ai sistemi nella PMI non sono generalmente percepiti. I rischi correlati alle informazioni possono portare a situazioni critiche, quando vanno ad investire l'essenza dell'organizzazione, sul piano aziendale e legale. I rischi correlati alle informazioni possono portare pertanto a categorie di rischio più generali e a maggiore criticità quali:

- **rischio legale/legato agli adempimenti è il rischio derivante da violazioni o mancato rispetto di leggi**, norme contabili, regolamenti, prassi o norme etiche. I rischi legali o correlati agli adempimenti possono esporre l'organizzazione a pubblicità negativa, ammende, sanzioni penali e civili, pagamento dei danni e annullamento dei contratti. Il furto di informazioni relative ai clienti, come le informazioni sulle carte di credito, le informazioni finanziarie, le informazioni sanitarie o altri dati personali possono anche sollevare rischi potenziali in termini di rivendicazioni di terzi. In riconoscimento del fatto che la sicurezza delle informazioni è una problematica crescente e composita, ma anche per tutelare i diritti civili e coinvolgere la responsabilità delle aziende, i governi dell'UE e l'Unione europea hanno stabilito leggi e regolamenti il cui rispetto è previsto da parte di tutte le organizzazioni, a prescindere dalle dimensioni o dal settore. Queste norme obbligano le società ad implementare controlli interni volti a proteggere l'azienda dai rischi informatici. Esse mirano anche a migliorare le prassi e le procedure di gestione del rischio;
- **rischi di stabilità finanziaria**. La mancanza di adeguate infrastrutture di produzione, di infrastrutture gestionali o di personale per perseguire la strategia aziendale può far sì che la società non sia in grado di conseguire gli obiettivi dichiarati e gli obiettivi finanziari in un ambiente ben gestito e controllato. Una inadeguata gestione della sicurezza delle informazioni può ricadere sui rischi relativi alla stabilità finanziaria dell'organizzazione, i quali rischi a loro volta, possono aprire la porta a frode, riciclaggio di denaro, instabilità finanziaria, ecc.
- **il rischio produttività è il rischio di riportare perdite operative** e di erogare servizi carenti alla clientela per effetto del mancato rispetto delle procedure di lavorazione di base e dei relativi controlli. Questo rischio si riferisce solitamente a tutte le attività di produzione che contribuiscono in qualche modo alla consegna complessiva di un prodotto o di un servizio. Il rischio produttività non è limitato all'uso delle tecnologie: può anche essere il risultato di attività organizzative. In questa famiglia di rischio rientrano i rischi derivanti da sistemi inadeguati o scarsamente controllati, dal software utilizzato a supporto degli operatori di sportello alle operazioni di gestione del rischio, dalla contabilità ad altre unità aziendali. Una inadeguata gestione della sicurezza delle informazioni può determinare rischi di produttività elevati, fra cui elevati costi operativi, carenze operative, debolezza delle decisioni manageriali, nonché mancanza di privacy ed interruzione del servizio alla clientela.
- **reputazione e fiducia nella clientela**. Forse il rischio più difficile da comprendere, ma anche uno dei più importanti, è il rischio di danno alla reputazione, un bene immateriale ma importante. I clienti, che hanno magari letto sul giornale che la banca dati della società, che contiene i numeri delle carte di credito, è stata aggredita dagli hacker, saranno disposti a fornire in seguito il numero della propria carta di credito? I vertici aziendali rimarranno al loro posto, in una società così danneggiata? Quale sarà la reazione degli azionisti? Qual è la prevista perdita di reddito futuro? Qual è la perdita prevista in termini di capitalizzazione di mercato?

Questi però sono i dati dell'EUROBAROMETRO[2] di una indagine su oltre 1.000 interviste a persone italiane a Marzo 2012. Questo dimostra che la sensibilità al problema sta cambiando.



1.3 Diversi livelli di attenzione

Una tipica osservazione che viene fatta dall'azienda è "**Non sono un obiettivo sensibile**" oppure "**Perché io?**".

A livello di legislazione è stato individuato, sulla base delle richieste UE, un gruppo di Aziende o Enti considerati critici su cui vien posta maggiore attenzione. In questo caso l'attività di verifica del livello di sicurezza dovrebbe essere una norma. Solitamente sono associati al concetto di infrastrutture critiche le risorse relative a:

- Produzione, trasmissione, distribuzione, dispacciamento dell'energia elettrica e di tutte le forme di energia, quali ad esempio il gas naturale
- Telecomunicazioni e telematica;
- Risorse idriche e gestione delle acque reflue;
- Agricoltura, produzione delle derrate alimentari e loro distribuzione;
- Sanità, ospedali e reti di servizi e interconnessione;

[2] http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_fact_it_it.pdf

- Trasporti aereo, navale, ferroviario, stradale e la distribuzione dei carburanti e dei prodotti di prima necessità;
- Banche e servizi finanziari;
- Sicurezza, protezione e difesa civile (forze dell'ordine, forze armate, ordine pubblico);
- Le reti a supporto del Governo, centrale e territoriale e per la gestione e delle Emergenze.

Il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) è l'unità specializzata interna al Servizio di polizia postale e delle comunicazioni dedicata alla prevenzione e repressione dei crimini informatici diretti ai danni delle infrastrutture critiche nazionali. Nel caso che una azienda appartenga a queste categorie è probabile che sia soggetta a monitorizzazione e protezione da attacchi di tipo informatico. Pertanto sarebbe necessario informare le forze dell'ordine se si intende commissionare una verifica di sicurezza.

Per rispondere al "**Perché io?**" bisogna tenere ben presente che le scansioni (normalmente non percepite) sono ripetute continuamente giorno e notte nella rete internet, a qualsiasi indirizzo pubblico ed in modo automatico, da curiosi, malintenzionati o robot (software automatizzati).

A supporto di questa tesi c'è la scarsa conoscenza di dati riconducibili ad attacchi informatici a PMI Italiane.

Ma va aggiunta una nuova forma di protesta che in questo periodo di crisi è una problematica reale. Cerchiamo di fare un rapido parallelismo fra forme di protesta tadizionali con quelle digitali.

Forma di protesta tradizionale	Forma di protesta digitale
Scritta sul muro o tazebao	Defacing del sito aziendale
Sit In	Netstrike - Tecnicamente si può definire come un attacco informatico non invasivo che consiste nel moltiplicare le connessioni contemporanee al sito-target al fine di rallentarne o impedirne le attività.
Distribuire volantini	Invio massivo di Mail
Occupazione di uno stabile in disuso	Cybersquatting - indica il fenomeno di accaparramento di nomi di dominio corrispondenti a marchi altrui o a nomi di personaggi famosi al fine di realizzare un lucro sul trasferimento del dominio a chi ne abbia interesse
Picchetto	DDoS - Si tratta di un attacco informatico in cui si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio
Attivismo	Hacktivism – Esprime la sua protesta accedendo ad un sito o ad un sistema informatico. Se questo viene fatto in modo massivo si riesce a bloccare un server per un certo periodo.

Secondo il report del Clusit 2012, le tipologie principali di attacante sono per il 41% Cybercriminali con fine di profitto e per il 29% di Hacktivist con fine di protesta. In questo ultimo caso ricordiamo gli attacchi all'Enel (25/3/2011), all' AGCOM (28/6/2011), Attacco alle banche (Banche al Sicuro 3/9/2011).

Da non dimenticare che il nostro tessuto produttivo fatto di PMI ad alto valore aggiunto in termini di know how è ipotizzabile che il Cyber Espionage farà numerose vittime arrecando un grave danno alle nostre imprese che risultano impreparate e poco sensibilizzate.

1.4 Bilanciare rischi con protezioni

Si prenda come esempio una azienda che ha come obiettivo proteggere le e-mail in transizione da sede a filiale, in modo che i dati trasmessi non siano intercettati.

Valutiamo le differenze tra un approccio analitico ed uno tempestivo in due casi di esempio, rispettivamente il caso A ed il caso B. L'esempio è una situazione ipotizzata a puro fine illustrativo.

CASO A:

Nel Caso A un approccio senza analisi, ma di intervento tempestivo tenterebbe l'implementazione di un sistema di VPN su firewall tra sede e filiale, per proteggere i dati in transizione, ed una gestione di certificati digitali, per garantire la provenienza.

Nel caso in cui il nostro interlocutore sia sfortunatamente controllato da una backdoor[3] o trojan[4], l'intero sistema di protezione sarebbe inutile, in quanto saremmo in grado di vedere il video dell'utente o ricevere i dati che scrive da tastiera.

CASO B:

Nel Caso B queste vulnerabilità sarebbero state trovate in fase di analisi. In tal caso l'implementazione sarebbe stata minore, semplicemente bloccando le porte in uscita via firewall ed installando certificati digitali in modalità crittografica.

Esempio Costi in percentuale

Caso	Analisi	Implementazione	Costo Finale
A Senza analisi	**0%**	**VPN + firewall + certificati: 100%**	**100%**
B Con analisi	**10%**	**Configurazione + certificato: 30%**	**40%**

Nel nostro esempio nel caso B pesa il costo di analisi e si riducono i costi di implementazione essendo mirati alle problematiche riscontrate. Il risultato economico questa volta è dato dalla somma dell' analisi di vulnerabilità ed implementazione delle protezioni, che, sebbene sia sempre minore rispetto al primo caso, è fortemente apprezzabile e soddisfacente dal punto di vista della sicurezza cogliendo l'obiettivo desiderato.

Un secondo problema è dato dal risultato in termini di sicurezza: il caso A ha dei risultati quasi nulli in protezione, mentre il caso B grazie all'analisi ed all'intervento mirato raggiunge una sicurezza nettamente apprezzabile.

Si stima che la spesa in ICT security sia pari al 15% delle perdite dirette e indirette generate dagli incidenti di sicurezza (Clusit 2012). Pertanto una PMI che fa un investimento di 5 mila Euro in sicurezza riesce a mitigare un rischio per l'azienda di circa 35 mila Euro.

[3] Queste "porte" possono essere intenzionalmente create dai gestori del sistema informatico (amministratori di rete e sistemisti) per permettere una più agevole opera di manutenzione dell'infrastruttura informatica da remoto, mentre più spesso da cracker intenzionati a manomettere il sistema. Possono anche essere installate autonomamente da alcuni malware (come virus, worm o trojan), in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

[4] programma che ci permette di raggiungere il client e controllarlo

1.5 Vulnerabilità di Rete

Per rete si intende tutta l'infrastruttura di comunicazione di un sistema informativo, dal cablaggio (livello 0 OSI) ad apparati concentratori (hub/switch), livello2, router firewall fino al livello dei protocolli per il trasporto (livello 4).

Con questa analisi vengono analizzate tutte le problematiche e vulnerabilità riconosciute per la rete. In modo particolare vulnerabilità a livello fisico (sniffing) e vulnerabilità ad alto livello network (attacchi a protocolli di autenticazione, attacchi per il blocco dei servizi(DOS)).

1.6 Vulnerabilità dei Sistemi

Per sistemi si intende tutto il software che controlla un apparato hardware dotato di processore e memoria. Sono sistemi i sistemi operativi dei server, i sistemi operativi dei firewall, i software di controllo router e switch, software di controllo di apparati mobili e wireless.

La tipica funzione di un sistema operativo è quella di controllare l'hardware, gestire la memoria e gestire i processi, ovvero applicazioni disegnate per quel particolare sistema.

I problemi di sicurezza sono legati al fatto che i sistemi accettano connessioni dall'esterno, o scambiano informazioni via rete.

Le relative vulnerabilità sono spesso causate da "buffer overflows", scripting o malfunzionamenti del sistema di autenticazione, che permettono accesso remoto al sistema con tecniche conosciute con il nome di "exploit".

1.7 Vulnerabilità delle Applicazioni

Per applicazione si intende tutto il software, compilato od interpretato che è funzionante su di un sistema. Un hardware può supportare uno o più sistemi operativi e, con l'avvento della virtualizzazione, un sistema può supportare più applicativi.

Si definisce "servizio" un'applicazione che renda disponibili delle informazioni via rete od in locale.

Le vulnerabilità maggiori e più pericolose sono relative ai servizi disponibili via rete, che spesso permettono di accedere al sistema.

Fanno parte della categoria applicazioni tutti i tools di posta elettronica e web, i programmi di autenticazione ed accesso ai sistemi ed applicativi gestionali, servizi web server, file server, mail server etc.

Le problematiche di Virus, Trojans, Worms sono parte di questa categoria e sono oggetto di analisi.

Le backdoor che questi software maligni possono aprire verso l'esterno, con le conseguenti problematiche, sono uno dei settori di maggiore interesse nell'analisi dei servizi attivi o processi fantasma.

Un recente esempio di vulnerabilità delle applicazioni è quello di Alitalia. Bastava andare su Alitalia.com scegliere la lingua in giapponese e prenotare. Si poteva scegliere qualsiasi volo che costasse meno di 250€ ed inserire il codice promojp. Il totale da spendere era di 0,00€. Senza bisogno di carta, bastava inserire nome, conferma e attendere la mail. In poche ore sono stati emessi biglietti verso Abu dabi a 0,38 centesimi, oppure voli "GVA-NYC-MXP a 275 euro che diventavano 25 euro". In pochi minuti la voce si è diffusa e il forum di Zingarate viene riempito da post continui e aggiornamenti che vanno avanti tutta la notte. C'è chi prende biglietti doppi, per amici e parenti. All'improvviso vengono annullati tutti i biglietti, scatenando l'ira degli utenti sulla pagina Fb dell'azienda. I clienti nel giro di poche ore ricevono una mail con su scritto:

Gentile Cliente,
grazie per aver scelto alitalia.com.
Ci spiace informarti che l'acquisto non è andato a buon fine.
L'eventuale importo addebitato ti sarà riaccreditato.
Alitalia Customer Center Team

Una volta emessi, però, i biglietti non possono essere annullati nemmeno se sono stati acquistati a prezzi stracciati, a causa di bug o errori tecnici dell'azienda. Parte una Class Action da parte del CODACONS.

2 Livelli di analisi

Spesso una non corretta interpretazione del livello di analisi che sostanzialmente è data della differenza fra un Vulnerabilty Assessment (Base) e un Penetration Test (Avanzato) crea caos nella PMI che richiede una verifica ad un fornitore. Questo è dato del confronto delle offerte e del relativo budget a disposizione.

2.1 Vulnerability Assessment

Il Vulnerability Assessment[5] costituisce il primo livello dei Servizi di Sicurezza Proattiva. Esso prevede l'esecuzione di **scansioni automatizzate e semi-automatizzate** non invasive, condotte avvalendosi di strumenti software open source (come OpenVas) e proprietari accuratamente selezionati (come Nessus 5), al fine di **rilevare la presenza di vulnerabilità note**.
Tali scansioni sono successivamente integrate da verifiche manuali eseguite da personale altamente qualificato, volte ad **eliminare i falsi positivi e negativi** eventualmente introdotti dagli strumenti di analisi automatica.
E' da valutare con attenzione lo svolgimento di un V.A. su una applicazione Web attiva in produzione poiché un test verso questo obiettivo prevede l'invio di stringhe di dati volutamente scorrette. Nel caso la stringa provochi un errore l'esito è inaspettato e comunque in grado di produrre una reazione che non è l'ambito di un V.A.

Nella valutazione di un servizio offerto è fondamentale discriminare questo limitato livello di verifica da quello più approfondito previsto nel Penetration Test

La frequenza tipica di un V.A in Italia non è definita e può variare da settore a settore. Nei paesi anglosassoni oscilla tra i 3 e i 6 mesi. La frequenza è in relazione alla frequenza delle nuove vulnerabilità note in particolare per la rete e i sistemi.

2.2 Penetration Test

Il servizio di verifica di sicurezza di tipo Penetration Test[6] prevede l'esecuzione di **test approfonditi in modalità Ethical Hacking**. Esso si basa su tecniche di attacco inferenziali finalizzate all'**identificazione delle vulnerabilità non note** o comunque non rilevabili tramite i soli strumenti di scansione ed analisi automatica.
Il P.T., che normalmente si avvale di un V.A. preliminare, consente di valutare sia le vulnerabilità riscontrate da un V.A. che altre che non lo sono e sono evidenziate dalle verifiche manuali. In aggiunta a questo (che sarebbe così solo un VA approfondito) nel P.T. si conduce un esercizio di sfruttamento delle vulnerabilità, per dimostrare le conseguenze di un ipotetico attacco. L'obiettivo è quello di evidenziare risultati non prodotti da un V.A., e può avere l'effetto di estendersi a sistemi / applicazioni ulteriori.
L'attività di verifica si avvale delle competenze e dell'esperienza di personale altamente qualificato, allo scopo di simulare nel modo più esaustivo possibile le operazioni comunemente eseguite da un agente di minaccia esterno o interno, facendo uso degli strumenti e delle **tecniche proprie di uno scenario reale**.

La frequenza tipica è minore di un V.A. ma possibilmente in coincidenza di una variazione della configurazione di rete, sistemi e applicazioni. La frequenza tipica di un P.T. in Italia non è definita e può variare da settore a settore. Nei paesi anglosassoni oscilla tra i 6 mesi e 1 anno.
A volte i revisori di bilancio sollecitano lo svolgimento della analisi al momento dell' Audit più esteso sull'azienda PMI.

[5] https://secure.wikimedia.org/wikipedia/it/wiki/Vulnerability_Assessment_and_Mitigation

[6] https://secure.wikimedia.org/wikipedia/it/wiki/Penetration_test

3 Perimetro di analisi

Per poter applicare l'analisi sui 3 livelli, rete sistemi ed applicazioni bisogna intervenire per quanto riguarda la rete ed i servizi sia nel perimetro esterno sia all'interno della rete privata. Per quanto riguarda l'analisi ad alto livello su applicazioni, processi e configurazione sistemi operativi bisogna accedere fisicamente alle macchine.

Per analizzare tutti i livelli di vulnerabilità di un sistema informativo stabiliamo tre modalità di analisi: l'analisi di sicurezza esterna (ASE) , l'analisi di sicurezza interna (ASI) e il Remediation Test (RT).

3.1 Analisi sicurezza esterna, ASE

L'analisi di sicurezza esterna è composta da una serie di processi che simulano le azioni normalmente svolte per attaccare un Sistema. Ogni azione viene svolta da una postazione remota, dove normalmente i dati o le informazioni visibili sono gli stessi per qualunque postazione o qualunque indirizzo. **Questo è il tipo di analisi che viene più spesso commissionata dalla PMI ad un fornitore**. **Erroneamente l'azienda pensa che il maggiore rischio sia proveniente dall'esterno.** Secondo recenti studi in materia di sicurezza informatica, la maggior parte delle violazioni ai sistemi IT deriva dall'errore umano, che amplifica la vulnerabilità agli attacchi cybercrime.

Proprio per definizione, i dati potrebbero non essere veritieri, ovvero i dati visibili dall'esterno potrebbero essere informazioni appositamente modificate per allontanare od imbrogliare eventuali malintenzionati. Questa tecnica, chiamata "fake system banners", è apprezzabile da un analisi di sicurezza esterna, in quanto confrontando i dati con un'analisi di sicurezza interna o con l'analisi dell'architettura di rete possiamo verificare quanto il sistema sia "prevedibile'' e protetto.

E' possibile per esempio presentare un server ftp IIS su WINDOWS come fosse un server ftp su Linux, ed in caso questo sia stato fatto volutamente, tramite questo tipo di analisi è possibile verificarne l'efficacia.

Una volta raccolto il maggior numero di informazioni è possibile verificare se il sistema soffre di possibili vulnerabilità, ovvero se vi sono dei comandi od operazioni particolari (relative ad un sistema od una applicazione) che ci permettono di violare la sicurezza, ovvero confidenzialità, disponibilità ed integrità di un sistema ed una rete.

Anche se normalmente invisibili, questo tipo di scansioni sono ripetute continuamente giorno e notte nella rete internet, a qualsiasi indirizzo pubblico ed in modo automatico, da curiosi ,malintenzionati o robot (software automatizzati).

E' quindi molto probabile essere uno dei tanti milioni di indirizzi analizzati da sistemi automatici, che avvisano in caso dei così detti 'buchi' di sicurezza.

Saranno descritte brevemente le operazioni svolte in questa analisi, effettuate manualmente o con l'ausilio di strumenti

3.1.1 Gathering Intelligence

Si immagini il seguente scenario:

Un obiettivo militare deve essere attaccato. Qual' è la prima cosa da considerare? Raccolta di informazioni,ovviamente, quello che in ambiente militare chiamano Gathering Intelligence. Per fare questo un satellite fotograferà la zona dell'obiettivo, e delle unità sorveglieranno l'area con la massima cautela per non essere identificate. Quando saranno raccolte le informazioni sui punti deboli e le vulnerabilità, i bombardieri attaccheranno gli obiettivi, compiendo la missione. Lo stesso avviene per il computer hacking. Un hacker intelligente farà molta ricerca prima di attaccare il sistema. Questa sarà proporzionale al valore della informazione recuperabile. Tipicamente la ricerca è rivolta ad identificare il punto più debole del sistema di sicurezza.

Nel mondo del computer hacking l'Intelligence gathering può essere diviso in 3 passi fondamentali:

1. Foot Printing
2. Scanning
3. Enumeration

Foot Printing

Le informazioni raccolte creano un' impronta digitale, un profilo dell'obiettivo.
Tramite queste tecniche raccogliamo dati relativi a :
1. Contatti amministrativi, tecnici e delle vendite, che includono nomi dei dipendenti, e-mail e numeri di telefono.
2. Range degli Indirizzi IP.
3. DNS Servers
4. Mail Servers.
5. Web Servers.

Si raccolgono tutte le informazioni che sono pubbliche e facilmente reperibili da Internet.

Scanning

L'attività di identificare quali sistemi sono operativi e raggiungibili via Internet,e quali servizi offrano, usando tecniche come ping sweeps, port scanners ed identificatori del sistema operativo è chiamata scanning (scansione). Si raccolgono dati relativi a:
1. Servizi TCP/UDP che girano su ogni sistema.
2. Architettura dei sistemi.
3. IP raggiungibili via internet (attraverso firewall).
4. Tipo di sistema operativo.
5. Servizi attivi.

Enumeration

Enumeration è il processo di estrarre dati e risorse da un sistema.
Le informazioni sono raccolte tramite connessioni attive e query ai sistemi. Questo tipo di procedure sono intrusive per natura, e sono ai confini della legalità e violazione del domicilio informatico.
Le tecniche dipendono dal sistema operativo, ma normalmente riguardano dati relativi a:

1. Utenti e nomi di Gruppo.
2. System Banners.
3. Services, Script & CGI exploit.
4. Vulnerabilità.

Le operazioni svolte in questa analisi includono le tre categorie, ma si focalizzano in modo particolare sullo scanning ed enumeration, per cercare le vulnerabilità del sistema.

3.2 Analisi sicurezza interna, ASI

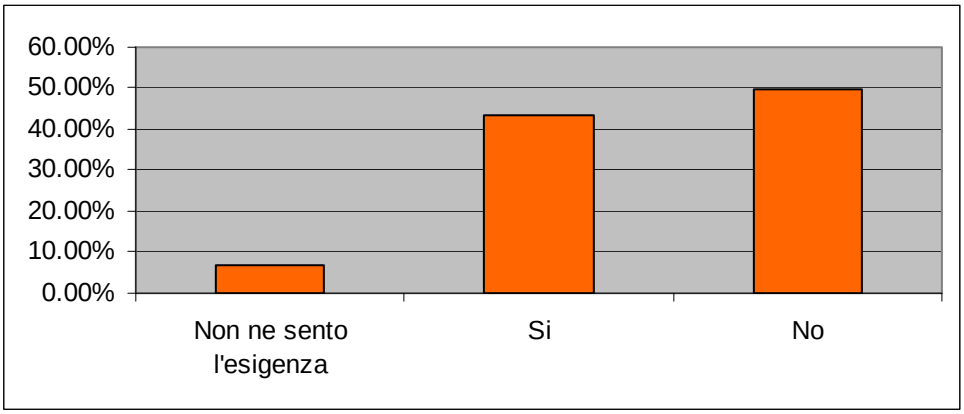
L'analisi di sicurezza Interna ASI è composta da una serie di processi che simulano le azioni normalmente svolte da un dipendente o consulente nella rete intranet. Ogni azione viene svolta da una postazione interna, dove normalmente i dati o le informazioni visibili sono gli stessi per qualunque postazione o qualunque indirizzo. Le problematiche riscontrabili da questa analisi riguardano soprattutto le problematiche di riservatezza e disponibilità.

La normativa sulla registrazione dei log per gli amministratori di sistema attualmente in vigore[7] ha voluto sensibilizzare ogni azienda sulla necessità di controllare l'operato di chi gestisce i sistemi nell'azienda. Questi super utenti hanno dei privilegi d'accesso sostanzialmente illimitati e devono essere monitorati e controllati in modo oggettivo. Il limite fra controllo lecito e violazione della privacy è di costante attualità. Una mitigazione del problema è quella di essere consapevoli delle proprie vulnerabilità interne attraverso una ASI.

Sulla base di una recente indagine svolta da ISACA VENICE CHAPTER svolto su aziende dell'area Nord Est con il seguente quesito

"Ha mai svolto delle analisi di sicurezza nel perietro interno. Dove l'analisi è composta da una serie di processi che simulano le azioni normalmente svolte da un dipendente e consulente nella rete interna".

Questo è stato il risultato.



I problemi di privacy sono legati alle informazioni della rete interna ed agli utenti che utilizzano tale rete. Spesso in una organizzazione molto grande gli utenti non sono facilmente controllabili, anche a causa di accessi ad utenti esterni.

I problemi di disponibilità sono relativi a Virus, Worm e Trojan. A seconda della tipologia di rete, dei protocolli e dei servizi una rete LAN è più o meno esposta a facili propagazioni di software anomali.

Inoltre l'unico modo per capire se nella rete abbiamo qualche software indesiderato, magari sui Client, è lo scanning di tutta la rete.

La sensibilità maggiore verso questo perimetro di analisi è evidenziata anche dalla introduzione da 9 marzo 2012 dell'obbligo secondo la nuova legge[8], di procedere con la confisca di tutti i beni e gli strumenti informatici o telematici che «risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli articoli». Se prima un dipendente si macchiava di crimine informatico utilizzando i computer dell'ufficio (con azienda ignara del crimine, ovviamente), il sequestro dei terminali non era previsto, in quanto gli strumenti informatici erano di terzi.

Spesso la somma di vulnerabilità interne può esporre ad un rischio concreto molto alto. Per esempio la presenza di un accesso Wifi con Wep su un impianto di produzione collegato alla rete aziendale. Capita spesso che i manutentori usino questo metodo per connettersi ad un macchinario per comodità. La chiave Wep è ottenibile con software specifici in circa un minuto. Sommiamo un server secondario in rete senza autenticazione ma con informazioni sensibili. La somma di questo è che una persona da un parcheggio esterno all'azienda può rapidamente trafugare le informazioni sensibili presenti su quel server con un prevedibile danno.

[7] G.U. n. 300 del 24 dicembre 2008 http://www.garanteprivacy.it/garante/doc.jsp?ID=1577499

[8] Disegno di legge N. 2271-B

Descriviamo brevemente le operazioni tipiche svolte in questa analisi, effettuate manualmente o con l'ausilio di strumenti

3.2.1 Sniffing

In una rete locale una delle tecniche più tipiche per ottenere informazioni relative al traffico è lo sniffing. Con dei tool appositi si configura la scheda di rete nella modalità promiscua, (normalmente unicast) in modo che accetti tutte le informazioni broadcast che la raggiungono. Sebbene questa tecnica sia più complessa in una switched network, è possibile analizzare tutto il traffico che passa in chiaro sulla rete, da e-mail a messaggi e documenti.

Nessun utente si può accorgere dell'avvenire di queste operazioni a meno di un analisi dei tempi di risposta di ogni IP.

In tal caso, le macchine configurate in modo promiscuo avrebbero dei ritardi enormi causati dalla saturazione della scheda di rete.

Molti tool antisniffing o di monitoraggio sono disponibili per risolvere queste problematiche.

3.2.2 Password cracking

Sempre legato allo sniffing un'altra tecnica permette di violare la privacy su reti locali: il cracking delle password.

Le informazioni che circolano criptate, come password o tunnels, possono sempre essere intercettate tramite sniffing, ma per risalire all'algoritmo che inizialmente ha cryptato le informazioni si utilizzano tecniche così dette di reverse engineering, ovvero si cerca di risalire a dei dati generati da funzioni ad una sola via alla chiave iniziale procedendo per tentativi o per confronto.

La tecnica che prova tutte le combinazioni è detta "brute forcing". Per dare un idea della lunghezza dell'operazione, decryptare oggi una password con una lunghezza di 6 caratteri alfabetici (26 caratteri) si stima che richieda 50 minuti (VASCO Data Security).

La tecnica per confronto è molto più veloce, prova delle password residenti su una lista e le confronta con quella intercettata. Trovare passwords come Admin, Love o password è un operazione di pochi millisecondi. Questo spiega la necessità di scegliere password lunghe, non appartenenti a parole di dizionari comuni e con caratteri complessi.

La scansione interna su ogni Client e Server in una rete locale è un ottimo sistema per verificare se vi sono password nulle o facilmente indovinabili.

3.2.3 Scan di Trojan Horse

Tecnica che prende il nome dalla Storia, dal cavallo di Troia. Per intercettare dati all'interno di un sistema il miglior modo è predisporre il sistema stesso a spedire le informazioni. Un Software che viene installato su un sistema operativo con lo scopo di esportare informazioni o di aprire porte verso l'esterno prende il nome di Trojan Horse.

A volte confusi come virus, I Trojan sono delle normalissime applicazioni lanciate (inconsapevolmente) dall'utente che svolgono operazioni di auditing, file browsing, keyboard sniffing, ed inviano i dati via email o aprono connessioni Socket, così dette backdoor.

Nell'ultimo caso, Software come NetBus o BackOrifice sono dei veri e propi tool di amministrazione remota di un sistema, e se installati su di una macchina remota ci permettono di accedere a tutte le risorse, webcam e memoria video comprese.

Rappresentano uno dei pericoli maggiori nell'ambito delle LAN per due motivi principali: il primo è dato dal fatto che ogni applicazione può essere un Trojan, ovvero ogni applicazione non certificata può aprire backdoor verso l'esterno, e nessun Antivirus potrebbe stabilire se le connessioni in ascolto sono legittime oppure no. Alcuni prodotti di personal firewall scaricano di fatto questa responsabilità sull'utente, che deve autorizzare le richieste di comunicazione di un'applicazione all'esterno. Di fatto si riconosce la difficoltà a gestire tecnologicamente il problema, spostandolo sull'utente, che spesso non è in grado di affrontarlo, o non lo vuole fare perchè è percepito come un fastidio all'operatività.

Il secondo problema è dato dal fatto che con il possesso della macchina si varcano tutte le barriere di protezione. Non c'è firewall, antivirus o Criptazione che blocchi la fuga di informazioni. Infatti non solo possiamo raccogliere i dati dalla fonte primaria (tastiera o video) ma possiamo anche trasmetterli all'esterno fingendoli come una normale richiesta web (Tunneling su porta 80 e masquerading tramite HTTP).

La scansione interna dei servizi presenti su ogni Client e Server in una rete locale è un ottimo sistema per verificare se vi sono Trojan inconsapevolmente in esecuzione od in ascolto sulla rete locale.

3.2.4 Social Engineering

Nell'ambito delle procedure definite dall'azienda vanno svolte delle verifiche che queste siano rispettate dal personale e va sotto il nome di ingegneria sociale[9]. Questo è un approccio di verifica, ma non è l'unico possibile. Queste sono definite internamente ma tengono conto delle leggi e le normative vigenti nel paese in cui viene svolto il PT. Questa attività è legata al fattore umano sia in caso di un errore involontario o violazione consapevolmente e richiede tipicamente un audit non tecnico anche a campione. Possono essere svolte dei tentativi di violazione delle politiche definite ma anche verificato il livello di conoscenza, comprensione ed adozione delle politiche da parte del personale.

Secondo il sondaggio svolto nel 2011 da BalaBit IT Security, il 74% del personale IT ha già violato i sistemi IT dell'azienda e avrebbe potuto perdere il lavoro se ci fosse stata una prova video a registrare il fatto. In particolare fra le maggiori attività illegali condotte dal personali IT nelle aziende emergono questi dati:

Il 48% risponde di aver creato regole eccezionali nel firewall o in altri sistemi IT per ragioni personali, per aggirare la policy delle attività IT;

Il 29% risponde di "aver portato a casa" informazioni aziendali;

Il 25% dichiara di aver visionato file riservati, archiviati nei server dell'azienda (ad esempio le buste paga dei dipendenti);

Il 16% dichiara di aver letto le email dei colleghi, senza avere il loro permesso;

Il 15% dichiara di aver cancellato o modificato file di gestione dei log, allo scopo di nascondere o distruggere le prove.

Un esempio può essere quello che può avvenire durante una verifica da parte della guardia di finanza sugli aspetti della Privacy. Una banale richiesta ad un dipendente di potersi collegare da una postazione di un collega vicino conoscendone la password genera una non conformità.

[9] http://it.wikipedia.org/wiki/Ingegneria_sociale

4 Vettori di attacco

Con il termine vettore di attacco si intende il percorso tramite il quale un agente di minaccia è potenzialmente in grado di ottenere un accesso non autorizzato ad una risorsa informatica.

Al fine di garantire una simulazione di attacco completa ed approfondita per un'ampia gamma di scenari tecnologici, sarà possibile operare attraverso differenti vettori, quali ad esempio:

- Infrastruttura: IP, VPN, Wi-Fi, SCADA, etc.
- Applicazioni: Web, Database, Client-Server, etc.
- Telefonia: PBX, RAS, APN, BlackBerry, VoIP, etc.
- Altri: Human, Physical, Videosorveglianza, Biometria, etc.

Spesso esistono dei preconcetti sulla vulnerabilità dei vettori d'attacco. Un esempio è considerare una linea MPLS sicura, la rete di produzione e la rete degli uffici isolate, un tablet incapace di infettare. Senza scivolare nella banalità è impensabile di non avere vulnerabilità ma è importante concentrarsi su quelle più macroscopiche. E fra queste è da porre massima attenzione a quelle che coinvolgono sistemi importanti per il business dell'azienda. Sostanzialmente se l'azienda diventa un obiettivo sarà sicuramente violata per cui è necessario convivere con una dose di rischio. Molto spesso con tattiche di social engineering si riescono a violare i sistemi complessi perché questo è l'anello più debole nella catena della sicurezza. In questo ambito (legato alla persona) si può includere la violazione di Tablet e Smart Phone aziendali. L'estensione a questi device va considerato perché le statistiche indicano una maggiore facilità degli utenti a cadere in attacchi tipo "Man in the middle[10]" (per intercettare le informazioni in chiaro) se veicolati su device mobili rispetto ai laptop. Questo vale specialmente per l'italia che ha il maggior rapporto utenti/cellulari nel mondo.

[10] è un tipo di attacco nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte, ovvero appunto un attaccante. L'attaccante deve essere in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime.

5 Strumenti

Per lo svolgimento delle attività vengono comunemente impiegati strumenti di attacco standard di pubblico dominio o che possono essere sviluppati dal fornitore. Tali strumenti appartengono alle seguenti categorie:

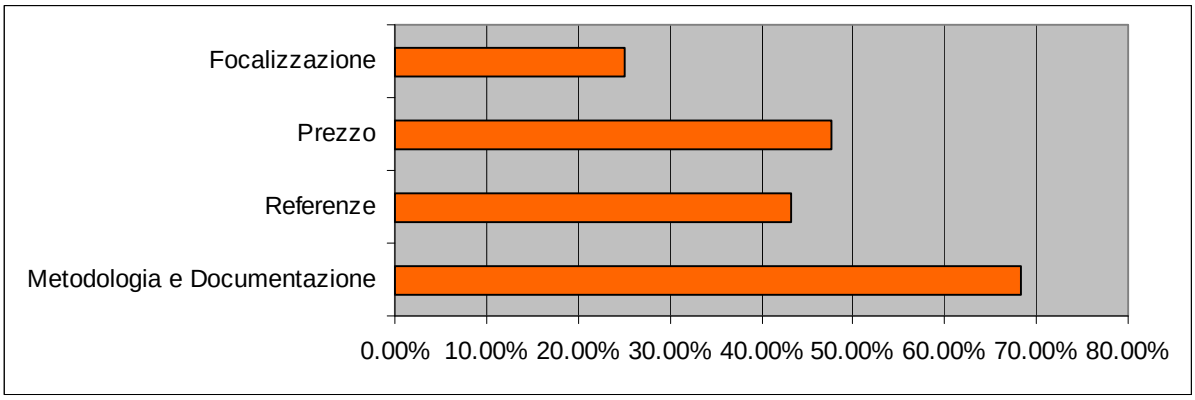
- Vulnerability Scanning (nessus, nexpose, openvas, etc.)
- Network Scanning (nmap, unicornscan, singsing, arp-scan, ike-scan, p0f, etc.)
- Web Testing (burp suite, zed attack proxy, w3af, skipfish, nikto, etc.)
- Wireless Testing (aircrack-ng, kismet, karmetasploit, etc.)
- Phone Testing (minicom, warvox, ward, thc-scan, etc.)
- Packet Forging (hping, scapy, voiphopper, yersinia, isic, netcat, etc.)
- Network Sniffing (wireshark, cain & abel, ettercap, etc.)
- Password Cracking (john, rcrack, fgdump, thc-hydra, medusa, etc.)
- Exploitation (metasploit framework, exploit-db, private exploits, etc.)

Gli strumenti sopra menzionati vengono tipicamente utilizzati per lo svolgimento di Vulnerability Assessment (VA) o nella fase iniziale di un Penetretion Test (PT).

Esistono alcuni soluzioni commerciali come Core Impact Professional focalizzati alla gestione del ciclo di vita delle vulnerabilità. Anche se sulla base di una recente indagine svolta da ISACA VENICE CHAPTER aspetti come la ripetitibilità sono considerati erroneamente poco importanti nella PMI.

6 Metodologie standard

Al fine di garantire una valutazione di sicurezza indipendente, oggettiva e ripetibile, tutte le attività previste devono essere condotte in conformità con le metodologie più accreditate, nel rispetto delle norme internazionali di riferimento. Sulla base di una recente indagine svolta da ISACA VENICE CHAPTER Metodolgia e Documentazione risultano le caratteristiche più importanti su cui viene scelto il fornitore a discapito della focalizzazione. Questa infatti risulta essere la caratteristica meno importante.



Esito del quesito sottoposto alle aziende campione: "**Su quale base sceglie il fornitore**".

In particolare possono essere considerati i seguenti riferimenti normativi e metodologici:

- ISO/IEC 19011:2011 – Guidelines for quality and/or environmental management;
- ISO/IEC 27002:2005 – Code of practice for information security management;
- ISO/IEC 27001:2005 – Information security management systems – Requirements;
- ISO/IEC 27004:2009 – Information security management – Measurement;
- ISO/IEC 20000-1:2011 – Service management – Part 1: Specification;
- ISO/IEC 27005:2011 – Information security risk management;
- BS25999-2:2007 – Business continuity management – Specification;
- BS25777:2008 – Information and communication technology continuity management;
- COBIT v5 – Control Objectives for Information and related Technologies;
- OSSTMM v3 – Open Source Security Testing Methodology Manual;
- OWASP Testing Guide v3 – Open Web Application Security Project Testing Guide;
- OWASP Guide 2010 – Open Web Application Security Project Development Guide;
- WASC Threat Classification v2.0 – Web Application Security Consortium Classification;
- CVSS v2.0 – Common Vulnerability Scoring System;
- CC v3.1 – Common Criteria;
- CEM v3.1 – Common Methodology for Information Technology Security Evaluation;
- ITIL v3 – Information Technology Infrastructure Library;
- PCI-DSS v2.0 – Payment Card Industry Data Security Standard;
- SOX of 2002 – Public Company Accounting Reform and Investor Protection Act;

- Basilea3 – International Convergence of Capital Measurement and Capital Standards;
- D.Lgs 196/2003 – Codice in materia di protezione dei dati personali;
- D.Lgs 231/2001 – Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica;
- D.Lgs 262/2005 – Tutela del risparmio e disciplina dei mercati finanziari;
- D.Lgs 81/2008 – Tutela della salute e della sicurezza nei luoghi di lavoro.

7 Metodologia OSSTMM

L'Open Source Security Testing Methodology Manual (OSSTMM[11]), è lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza, sviluppato da ISECOM tramite il modello peer review.

ISECOM (Institute for Security and Open Methodologies) è un'organizzazione internazionale di ricerca senza scopo di lucro, fondata nel 2001 al fine di sviluppare e condividere metodologie aperte nel campo della sicurezza delle informazioni. ISECOM è inoltre un'autorità di certificazione sostenuta da partner istituzionali.

OSSTMM è una metodologia scientifica che definisce esattamente quali elementi devono essere verificati, che cosa occorre fare prima, durante e dopo i test di sicurezza e come misurare i risultati ottenuti. Consente pertanto di valutare sul campo in modo consistente e ripetibile la superficie di attacco relativa al contesto oggetto di analisi.

La metodologia OSSTMM ha introdotto numerosi nuovi concetti nella disciplina della Sicurezza Proattiva, quali: OPSEC e controlli, Competitive Intelligence (CI), metriche per misurare la superficie di attacco (RAV), reportistica certificata (STAR). Una verifica di sicurezza conforme allo standard OSSTMM assicura:

- Esaustività e profondità dei test, con riduzione sostanziale dei falsi positivi e negativi.
- Conclusioni oggettivamente derivate dai risultati dei test stessi, tramite applicazione del metodo scientifico.
- Rispetto di politiche, normative e leggi vigenti applicabili al contesto oggetto di analisi.
- Risultati consistenti e ripetibili.
- Risultati misurabili e quantificabili secondo precise regole.
- La reportistica certificata costituisce la prova di un test basato sui fatti e rende gli analisti responsabili dell'audit.

Tramite il calcolo del RAV e l'emissione di reportistica STAR certificata, OSSTMM consente alla azienda di ottenere le risposte alle seguenti domande fondamentali:

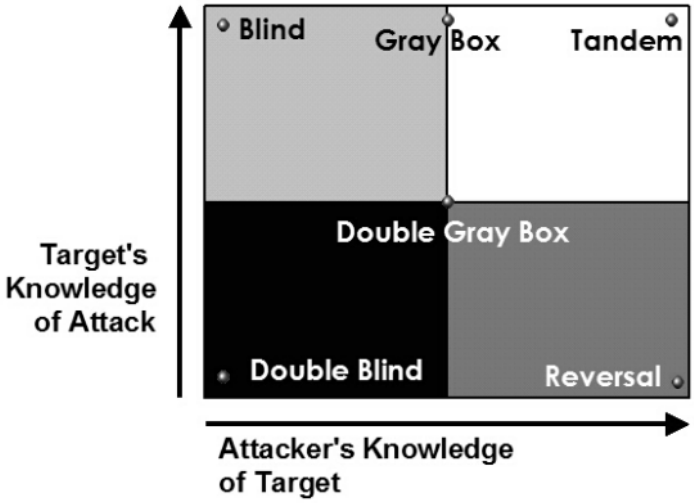
- Quanto dobbiamo investire nella sicurezza?
- Su quali aspetti dobbiamo concentrarci in modo prioritario?
- Di quali soluzioni di sicurezza abbiamo bisogno?
- Quanto migliora il livello di sicurezza a seguito dell'adozione di specifiche contromisure?
- Come possiamo misurare i risultati dei piani correttivi?
- Come possiamo sapere se stiamo riducendo l'esposizione alle minacce?
- Quanto è resistente un determinato componente?
- Come possiamo ottenere conformità e sicurezza?

L'obiettivo finale di una verifica conforme allo standard OSSTMM, pertanto, è fornire un processo concreto per essere funzionalmente sicuri.

[11] http://www.isecom.org/osstmm/.

Inoltre definisce quelli che devono essere i punti di attenzione per l'azienda nel commissionare un PT.

7.1 Tipi di Penetration Test secondo OSSTMM



BLIND: quando l'attaccante non conosce minimamente il sistema da analizzare. E' conosiuto solamente il target (Indirizzi IP o URL)

DOUBLE BLIND: simile a quello precedente con la differenza che alcune persone del committente sono al corrente del test. Viene tipicamente usato per verificare se il personale interno dedicato alla sicurezza è "vigile" e svolge con diligenza il proprio lavoro.

GRAY BOX: sia l'attaccante che l'attacco sono pienamente a conoscenza sia del sistema informatico da analizzare che delle modalità di attacco. Viene utilizzato quando si analizza il proprio sistema interno.

DOUBLE GRAY BOX: è un gray box che prevede la conoscenza delle credenziali di accesso. Viene usato per testare l'accesso ad informazioni più riservate rispetto al suo livello da parte di un utente.

TANDEM: analisi del codice. Chi verifica e chi crea il codice collaborano

REVERSAL: test a uso interno. Il tester ha una grande quantità di informazione il committente non sa i tempi e le metodologie con cui verrà attaccato.

7.2 Le fasi secondo OSSTMM

La metodologia OSSTMM segue quattro fasi fondamentali ben precise che permettono di svolgere al meglio l'analisi di sicurezza ed è applicabile a qualsiasi tipologia di test di sicurezza. Ogni singola fase ha una diversa profondità sull'analisi ma tutte hanno la stessa importanza in termini di sicurezza.

Le quattro fasi sono:

- Induction Phase
- Interaction Phase
- Inquest Phase
- Intervention Phase

7.2.1 Induction Phase

Induction Phase è il primo step dell'analisi. Durante questa fase l'analista inizia con la raccolta dei requisiti di audit, definendo la portata e le limitazioni del test. In questa fase viene coinvolto il committente e quindi definita la tipologia di test da svolgere. La fase di induzione di suddivide a sua volta in tre momenti:

- Posture Review: identificare le normative, regole, norme e politiche associate al target da analizzare. Ad esempio, nel caso di una multinazionale, le normative in termini di privacy possono essere diverse a seconda dello stato in cui risiede il sistema da analizzare.
- Logistics: analizzare i possibili errori e limitazioni quali distanza, velocità, fallibilità. Tutto questo per ridurre al minimo la possibile fallibilità del test.
- Active Detection Verification: identificare i possibili limiti dei test interattivi verso il target.

7.2.2 Interactive Phase

Per svolgere un test di sicurezza bisogna definire lo scope associato al target da analizzare. Questa fase è suddivisa in quattro moduli:

- Visibility audit: determinare gli obiettivi da testare. E' considerata “visibility” la presenza e non solamente la visibilità. Se un sistema non risponde non vuol dire che questo non esiste.
- Access Verification: definire i punti di interattività (punti di accesso) e misurare la robustezza ed efficacia delle richieste di autenticazione.
- Trust Verification: verificare l'affidabilità e sicurezza delle relazioni tra e verso i target da analizzare. Vi è una relazione di trust ogni qualvolta il target accetta interazione.
- Control Verification: vengono fatti i controlli definiti di classe B:
    - non ripudio (tracciabilità delle informazioni)
    - confidenzialità (informazioni scambiate in sicurezza)
    - privacy (le informazioni sono scambiate in riservatezza)
    - integrity (controllo integrità delle informazioni scambiate)

7.2.3 Inquest Phase

Molti dei test di sicurezza svolti vengono fatti secondo le informazioni reperite dall'analista. I test infatti vengono creati “su misura” (come un vestito) a seconda delle caratteristiche del sistema da analizzare. Questa fase è suddivisa in 6 moduli.

- Process Verification: identificare e comprendere i processi informatici del committente
- Configuration Verification / Training Verification: identificare il normale stato di funzionamento dei sistemi per rilevarne eventuali problemi di fondo quando questi sono soggetti a stress test di sicurezza.
- Property Validation: verificare lo stato dei diritti di proprietà (licenze, software abusivi, ecc)

- Segregation Review: verificare se il sistema informatico rispetta le leggi vigenti nello stato in cui risiede il sistema, ad esempio la legge sulla privacy.
- Exposure Verification: rilevare se esistono informazioni dichiarate riservate che invece risultano visibili
- Competitive Intelligence Scouting: ricercare informazioni liberamente disponibili e pubbliche che potrebbero danneggiare o compromettere il sistema.

7.2.4 Intervention Phase - Fase finale

- Quarantine Verification: verificare come il sistema di “quarantena” funzioni adeguatamente (virus, black list, ecc)
- Privileges Audit: controllo della robustezza delle credenziali di accesso, politiche applicate o non autorizzate “privilege escalation”.
- Survivability Validation / Service Continuity: misurare la resistenza del sistema in caso di sovraccarico (DOS). Il controllo viene fatto solo su esplicita richiesta e autorizzazione scritta.
- Alert and Log Review / End Survey: verificare come e se il sistema ha tracciato e identificato l'attacco informatico.

8 Metodologia OWASP

Quando la verifica comprende applicazioni pubblicate via WEB si adotta la metodologia OWASP Testing Guide per svolgere le attività di analisi. Questo è lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza applicative, sviluppato da OWASP tramite il modello peer review.

OWASP (Open Web Application Security Project) è una comunità internazionale di ricerca senza scopo di lucro, fondata nel 2001 al fine di aumentare la robustezza del software applicativo, promuovendo lo sviluppo ed il mantenimento di applicazioni web sicure.

Nonostante numerose aziende del settore abbiano aderito ad OWASP, la comunità non supporta o raccomanda prodotti o servizi commerciali, ma rimane vendor-independent al fine di assicurare la massima imparzialità. Tutto il materiale documentale ed il software prodotto nell'ambito dei progetti promossi da OWASP è distribuito gratuitamente sotto licenza aperta.

La OWASP Testing Guide è un framework di verifica che descrive nel dettaglio come rilevare le problematiche di sicurezza associate al software applicativo. In particolare, essa fornisce gli strumenti metodologici per comprendere quando ed in che modo analizzare le applicazioni web.

Una verifica di sicurezza conforme alle linee guida OWASP consente di rilevare le classi di problematiche. Qui elenchiamo le più importanti:

- Injection (in particolare SQL Injection)
- Cross-Site Scripting (XSS)
- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

9 Proceduralizzare le verifiche

Le aziende PMI nel commissionare un PT come valore aggiunto, dovrebbero iniziare a sviluppare una procedura di valutazione della sicurezza IT. Questo permetterebbe di fornire gli obiettivi e le linee guida per le esecuzioni di PT anche per il futuro. Questa politica dovrebbe individuare i requisiti, e definire quegli individui che hanno la responsabilità di garantire che le valutazioni siano conformi ai requisiti. Una più ampia procedura di gestione del rischio informatico nella PMI[12] prevede:

- identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità, ovvero le carenze di protezione relativamente a una determinata minaccia.
- individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse
- individuazione dei danni che possono derivare dal concretizzarsi delle minacce
- identificazione delle possibili contromisure
- effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure
- definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare
- documentazione e accettazione del rischio residuo

[12] Per approfondimenti si veda IL RISCHIO INFORMATICO - NOVEMBRE 2004 - CONVENZIONE INTERBANCARIA PER I PROBLEMI DELL'AUTOMAZIONE
Per approfondimenti sulla gestione del rischio nella PMI si veda https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/information-package-for-smes-1/at_download/fullReport

10 Requisiti per commissionare un Penetration Test

Se una Azienda commissiona questa attività per la prima volta ad un fornitore esterno, il valore aggiunto è quello di verificare oggettivamente le barriere difensive verso l'esterno. Se invece l'attività è già stata svolta devo avere come obiettivo quello di standardizzare il processo in modo da creare un percorso di miglioramento delle difese. La finalità in entrambi i casi è quello di ridurre il rischio descritto nei paragrafi precedenti.

Se il fornitore è qualificato e competente sarà anche in grado di fornire delle indicazioni sui miglioramenti alla infrastruttura di sicurezza. Questo non è lo scopo del PT che è una analisi oggettiva, ma può essere un servizio aggiuntivo che posso chiedere al fornitore.

Non esiste una soglia nella dimensione di azienda che è obbligata a svolgere un PT e l'ottica deve essere quella di un aiuto alla riduzione del rischio. Molti titolari di PMI pensano di non essere a rischio, in virtù della ridotta dimensione della propria azienda e del patrimonio informativo. La maggior parte ritiene che soltanto le grandi società, quelle che hanno un patrimonio di grande rilievo, siano a rischio. Questo non è vero. In primo luogo, la sensitività delle informazioni si applica alla qualità e non alla quantità delle informazioni. In secondo luogo, le PMI non dispongono delle risorse o del personale necessari per affrontare la sicurezza in maniera intensiva, come fanno le grandi società: sono pertanto più esposte.

Di fatto, le nuove tecnologie consentono alle piccole aziende di utilizzare una buona parte dei medesimi sistemi informativi utilizzati dalle grandi imprese. Nel fare questo, le piccole aziende si espongono a molte delle minacce che tradizionalmente si associano alle grandi società. Sfortunatamente, una percentuale non irrilevante delle aziende colpite da inconvenienti che hanno messo fuori uso i computer non riesce a recuperare il danno e l'azienda stessa è costretta a chiudere.

Affinché il successo sia continuativo, è imperativo pertanto che i titolari ed i responsabili decisionali delle PMI ammettano queste insidie e prendano misure atte ad affrontare le questioni relative alla sicurezza delle informazioni.

Questi sono i requisiti che serve definire per commissionare un PT:

- Definire se si appartiene alle infrastrutture critiche[13]
- Definire quali sono i beni aziendali coinvolti in ordine di priorità[14] classificandoli in un livello da 1 a 3.
- Definire i meccanismi di protezione attuali per tali beni.
- Definire fra questi beni ciò che si desidera analizzare, il suo stato di verifica e la frequenza di analisi. A volte per esigenze di budget si procede a verifiche specifiche a rotazione.

Qui formalizziamo una possibile tabella dei beni con valori ipotetici utile a creare un piano di rischio:

Codice	Bene	Attuale meccanismo di protezione	Priorità	Stato di verifica	Frequenza di analisi	Responsabile
001	Firewall	Aggiornamento delle patch, Salvataggio delle configurazione, registro delle modifiche di configurazione, ecc…	Alta (divisa in 3 livelli)	13/08/2012	Mensile	Network Manager

[13] vedi capitolo precedente "Diversi livelli di attenzione"

[14] FIPS PUB 199, Prevede norme per la determinazione della categoria di sicurezza dei sistemi informativi di un'organizzazione che possono essere utili nello sviluppo di una graduatoria di priorità di tali sistemi per scopi di test. FIPS PUB 199 è disponibile per il download http://csrc.nist.gov/publications/PubsFIPS.html

- Definire il tipo di PT (Intrusivo o meno, Decadimento accettabile, Blind/Gray Box…)
- Definire il perimetro
- Definire il vettore di attacco
- Definire il periodo (durata, periodo, sistemi Online). In caso si voglia definire una procedura operativa va definita anche una frequenza.
- Definire chi sono le persone chiave in azienda che devono essere informate del test e chi sono i contatti per il fornitore in caso di problemi durante il test.
- Definire di chi è il compito di correggere le vulnerabilità identificate.

La valutazione non deve avvenire durante gli aggiornamenti, l'integrazione di nuove tecnologie, o se il sistema di sicurezza è alterabile in fase di verifica.

Nel caso il PT riguardi anche le applicazioni web pubblicate si può scegliere di fornire al fornitore un account di prova per verificare l'atomicità del profilo utente e l'impossibilità di fare escalation dei diritti.

Il cliente dovrà fornire una dichiarazione firmata che prevede l'autorizzazione all'esecuzione del test, che dispensa il fornitore dalla responsabilità di un eventuale sconfinamento nel campo d'applicazione. Questo è un esempio di testo da compilare su carta intestata e rilasciare al fornitore quale autorizzazione all'esecuzione del test.

… AUTORIZZO

La società ….. alla raccolta di dati ed informazioni circolanti sulla nostra rete LAN aziendale attraverso una serie di attività atte a valutare e testare il livello di sicurezza della nostra rete informatica, attraverso il servizio indicato come "Analisi di sicurezza esterna".

Dichiaro di essere consapevole e di autorizzare fin d'ora che da una postazione remota via internet o direttamente in sede aziendale, il Sig. ….. in qualità di tecnico della società ….. effettui nelle date concordate, le verifiche tecniche sullo stato della nostra rete informatica aziendale, sui servizi e protocolli attivi, valutando conseguentemente le possibili vulnerabilità dei nostri sistemi informatici aziendali con diversi strumenti e tecniche di analisi manuale e/o automatiche.

Le analisi di sicurezza verificano i sistemi di protezione informatica ed i server pubblici. Tali test possono risultare in saturazione della banda e delle risorse dei sistemi. La società …. Non sarà responsabile di eventuali disservizi che si potranno verificare durante il periodo di esecuzione del test.

I dati e le informazioni raccolte dagli strumenti di analisi manuale e/o automatica saranno elaborati dal personale della società …. Come documentazione confidenziale riservata, considerabile come dati sensibili e trattati secondo il rispetto del "codice in materia di protezione dei dati personali" D.lgs 196/2003. La società ….. si impegna altresì a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici e cartacei tali dati alla conclusione dell'incarico conferito.

Le date previste per l'intervento tecnico di attuazione del test/verifiche sono: dalle ore …. Alle ore …. Nei giorni compresi fra … e ….

Gli indirizzi IP del cliente sui quali verranno effettuati i test/verifiche sono: …..

Firma

Data

11 Schema di un contratto tipo

Di seguito viene proposto uno schema di contratto utile alle parti per definire in modo preciso obblighi e responsabilità reciproche. Lo schema proposto discende da due criteri diversi ma entrambi legati alla tipologia di servizio in questione.

Il primo criterio è riferito ai contratti di servizio tout court. Ricadono in questa categoria i contratti relativi a servizi che solitamente sono di carattere continuativo(manutenzione, assistenza, ecc).

Il secondo criterio è relativo alle attività specifiche legate ad un progetto. Ricadono in questa categoria, ad esempio, i contratti di sviluppo software e di manutenzione software.

Nel nostro caso (penetration test) si tratta di un servizio fornito in modo occasionale e non continuativo, ritagliato sulle specifiche esigenze del cliente e non definito attraverso una licenza d'uso, per cui riassume entrambi i criteri su citati.

Quella che segue è una traccia di struttura contrattuale che le parti possono utilizzare prevedendo integrazioni e modifiche. Il testo, quindi, non è esaustivo e va inteso solo come traccia per il contratto. Si ritiene che solo l'intervento di un professionista potrà consentire la predisposizione di un contratto che tenga conto di tutte le effettive esigenze delle parti. Nel testo che segue si fa l'ipotesi che le parti siano entrambe italiane essendo il testo redatto secondo la legge nazionale. Nel caso di un contratto fra parti di nazionalità diverse l'intervento del professionista sarà ancora più importante.

E' raccomandabile che prima della stesura del contratto il cliente affidi al fornitore uno studio di fattibilità a pagamento. Sempre in fase pre contrattuale è raccomandata la stesura di specifiche inerenti le modalità di conduzione dell'attività e che queste vengano condivise fra le parti.

I commenti al testo sono espressi in carattere corsivo.

Tra XXX (Fornitore) e YYY (Cliente), in seguito collettivamente definiti "le Parti", si conviene:

11.1 Oggetto

Con questo accordo (Contratto) il Fornitore si impegna ad eseguire per il Cliente i servizi descritti di seguito secondo le modalità previste nell'allegato A ai termini e condizioni concordate (Servizi).

Servizi:

qui il fornitore descrive la sequenza dei servizi ad esempio:

. Verifica dei servizi disponibili sulla rete;

. Determinazione delle vulnerabilità dei sistemi;

. Verifica dei diritti di proprietà del software installato;

. Verifica di conformità alla legge 196/2003;

. Verifica della reale riservatezza delle informazioni dichiarate riservate;

. Verifica delle credenziali di accesso;

. Verifiche aggiornamenti sistemi per tutti i nodi della rete;

. Test di penetrazione con le tecniche e gli strumenti indicati nell'allegato A;

.

.

. Consegna del rapporto di test come descritto nell'allegato A;

….

11.2 Dichiarazione del Fornitore

Il Fornitore dichiara di aver ricevuto dal Cliente informazioni sufficienti in merito all'ambiente informatico esistente dal Cliente ed alle condizioni di erogazione dei Servizi.

E' la conseguenza dello studio di fattibilità.

11.3 Struttura del Contratto

Il Contratto è composto da questo documento, dall'allegato A (Modalità di esecuzione del servizio, attività pianificate e strumenti adottati), dall'allegato B (Tabella costi del materiale e degli strumenti utilizzati), allegato C (Rischi associati ai test di sicurezza) che ne fanno parte integrante. Le Parti potranno modificare o integrare il Contratto solo tramite documento sottoscritto da entrambe e con espresso riferimento al Contratto.

11.4 Esecuzione del Contratto da parte di terzi

Il Fornitore non affiderà a terzi l'esecuzione di alcuna parte del Contratto senza il preventivo consenso del Cliente. Il Fornitore non sarà sollevato da alcuna delle obbligazioni nei confronti del Cliente per l'esecuzione del Contratto per il fatto di averle affidate a terzi.

11.5 Pagamenti e spese

Versione 1: Prezzo fisso

Il prezzo convenuto fra le Parti a fronte delle attività del Fornitore di cui all'art.1 è di XXX.

Il prezzo sarà pagato come segue:

yyy alla firma dell'accordo a titolo di anticipo;

zzz alla consegna del rapporto di test;

hhh alla data di accettazione.

I pagamenti avverranno a XX giorni dalla data della fattura.

In caso di ritardato pagamento il Cliente dovrà corrispondere gli interessi moratori nella misura dell'x% per ogni settimana di ritardo. Se il ritardo nei pagamenti è superiore a xx settimane, il contratto si intenderà risolto di diritto, previa notifica del Fornitore al Cliente, da comunicarsi per iscritto con un mezzo di trasmissione che assicuri la prova e la data di ricevimento della comunicazione stessa (es. lettera raccomandata con avviso di ricevimento, corriere, ecc).

E' importante prestare attenzione al tasso applicato, verificando che non sia in contrasto con la legge sull'usura.

Versione 2: Time and Material

- Il Cliente pagherà il Fornitore per il tempo speso per l'esecuzione del Contratto (che non includerà il tempo di viaggio) e per il materiale (e costo della strumentazione) utilizzati dal Fornitore fino ad un costo massimo di XXX.

- La tariffa oraria applicata sarà di YYY (15).

- I costi del materiale e dell'utilizzo della strumentazione utilizzata saranno calcolati sulla base delle tabelle dell'allegato B.

- Il Fornitore manterrà aggiornata documentazione del tempo e dei materiali utilizzati, che terrà a disposizione del Cliente su richiesta.

- Il prezzo sarà pagato come segue:

15 Le tariffe potranno essere differenziate a seconda della figura professionale coinvolta.

yyy alla firma dell'accordo a titolo di anticipo;

x% del totale – yyy alla consegna del rapporto di test (16)

la quota rimanente alla data di accettazione.

- I pagamenti avverranno a XX giorni dalla data della fattura.

In caso di ritardato pagamento il Cliente dovrà corrispondere gli interessi moratori nella misura dell'x% per ogni settimana di ritardo. Se il ritardo nei pagamenti è superiore a xx settimane, il contratto si intenderà risolto di diritto, previa notifica del Fornitore al Cliente.

11.6 Responsabilità del Cliente

Il Cliente metterà a disposizione del Fornitore le informazioni richieste per l'esecuzione del Contratto e si assicurerà che i suoi collaboratori siano disponibili per il Fornitore, con gli strumenti e gli spazi necessari per l'esecuzione del Contratto.

Il Cliente dichiara di avere preso atto dei rischi connessi all'attività di test di sicurezza elencati nell'allegato C in rapporto alle attività che saranno messe in cantiere ed elencate nell'allegato A.

11.7 Personale del Fornitore

Il Fornitore dovrà assicurarsi che il personale incaricato dell'attività abbia un adeguato livello di preparazione e specializzazione (e sia gradito al cliente).

Il Fornitore si impegna ad assicurare la presenza delle seguenti figure professionali per ognuna delle attività elencate nell'allegato A:

attività 1: figura 1;

attività 2: figura 2, figura 3;

.

Il Fornitore garantisce che le proprie prestazioni saranno eseguite da personale regolarmente assunto, idoneo e di comprovata capacità tecnica. Il personale del Fornitore agirà sotto l'esclusiva responsabilità, direzione tecnica, organizzativa del Fornitore.

Se il personale del Fornitore dovrà eseguire la propria prestazione presso la sede del Cliente, sarà riconoscibile come appartenente all'impresa del Fornitore e sarà tenuto a rispettare le regole di sicurezza e di comportamento che il Cliente richiede di osservare ai propri dipendenti. Il fornitore farà in modo che il proprio personale rispetti queste obbligazioni.

11.8 Accettazione

Il Cliente effettuerà l'accettazione formale del rapporto di test entro e non oltre xx giorni dalla consegna; entro quel periodo potrà eventualmente richiedere i chiarimenti necessari oppure indire una specifica riunione di presentazione dei risultati conseguiti.

Trascorsi xx giorni dalla consegna del rapporto di test senza nessuna comunicazione o richiesta del Cliente il rapporto si intenderà accettato.

11.9 Informazioni riservate

Ciascuna delle Parti tratterrà come riservate le informazioni ricevute dall'altra ai fini del contratto, salvo quelle di pubblico dominio, e non le divulgherà a terzi senza il consenso dell'altra.

16 Per la modalità Time and Material non si ritiene di applicare la fatturazione tipica di questo tipo di prestazione, ovvero fatturazione periodica, perché la si ritiene non consona per un'attività, il penetration test, che si presume non si estenda oltre un congruo numero di giornate di attività. La classica modalità (fatturazione su avanzamento mensile) è pportuna quando l'attività si estende su un periodo di diversi mesi.

Le Parti informeranno i propri dipendenti dell'obbligo di riservatezza contenuto in questo articolo e si assicureranno che venga rispettato anche ai sensi dell'art. 1381 del Codice civile.

Se il Fornitore si rivolgerà a terzi per l'esecuzione del Contratto, dovrà ottenere da questi il medesimo impegno di riservatezza.

L'obbligo di riservatezza di cui al presente articolo si estenderà oltre la durata del Contratto.

Il Fornitore prenderà le misure necessarie per la custodia delle informazioni riservate del Cliente in suo possesso.

11.10 Assicurazione

Il Fornitore conferma di avere stipulato una polizza assicurativa per la copertura contro i rischi della responsabilità civile e professionale per l'attività da lui svolta.

Tale copertura assicurativa prevede un massimale pari al corrispettivo complessivo del Contratto e comunque non inferiore a xxx per sinistro assicurato.

I massimali non potranno essere ridotti senza il consenso scritto del Cliente.

11.11 Trattamento dei dati personali da parte del Fornitore

Il Cliente è Titolare dei dati personali a cui avrà accesso il Fornitore per l'esecuzione del Contratto e nomina il Fornitore Responsabile per la durata del Contratto in quanto soggetto competente anche in virtù della propria attività professionale.

Il Fornitore si impegna a rispettare tutte le leggi e i regolamenti in materia di protezione di dati personali nonchè le istruzioni del Cliente in proposito.

Il Fornitore si impegna a rispettarne la riservatezza, ad adottare tutte le misure prescritte ed utili per rispettarne la riservatezza e l'integrità.

Le Parti concorderanno le modalità necessarie per la designazione scritta dei relativi incaricati al trattamento, all'interno dell'organizzazione del Responsabile.

Il Fornitore si impegna inoltre ad utilizzare i dati esclusivamente al fine dell'esecuzione del Contratto e per l'adempimento degli obblighi normativi ove necessario.

Il Fornitore metterà a disposizione del Cliente, su semplice richiesta, il supporto e i dati necessari per garantire agli interessati l'effettivo esercizio dei propri diritti.

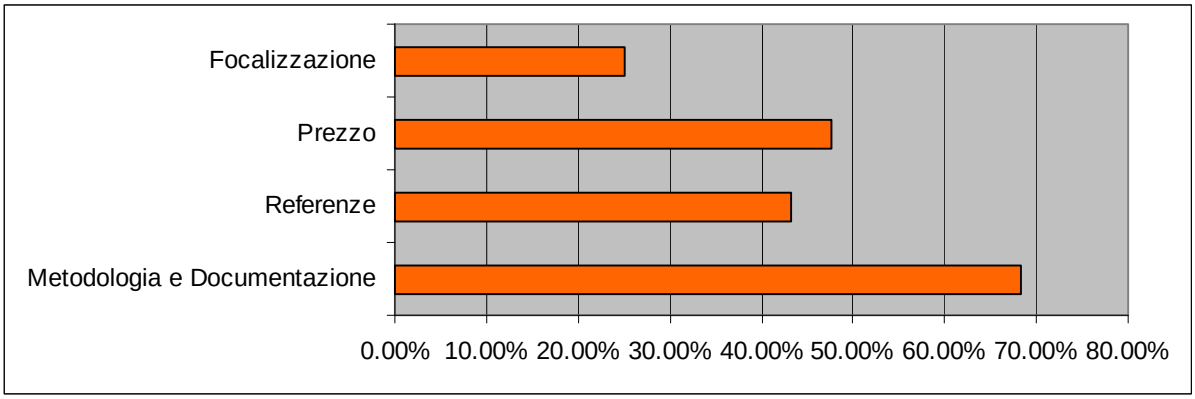
Nota finale:

Per la specificità del contratto in questione (eseguibile in tempi relativamente ristretti) non sono state inserite specifiche clausole relative ai ritardi nell'esecuzione del contratto sia per il Fornitore e sia per il Cliente. Idem per forza maggiore e per risoluzione in caso di mancato adempimento contrattuale.

12 Come orientarsi nella selezione del fornitore

Le organizzazioni dovrebbero fare attenzione nella scelta del fornitore accreditato, perché scegliere valutatori adeguatamente controllati, abili, esperti riduce i rischi legati alle prove di sicurezza. Non esiste una figura riconosciuta per legge di fornitore accreditato ma citiamo all'interno del c.d. Codice Privacy, o meglio, nel disciplinare tecnico dedicato alle misure minime di sicurezza "Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico" (cfr Art. 25 dell'Allegato B al D.Lgs. 196/03). Ad oggi non esiste una procedura ottimale nella qualificazione del fornitore, ma elenchiamo alcune regole di "due diligence" per una corretta scelta traendo spunti dalla metodologia OSSTMM sulla qualifica del fornitore[17] o dal documentazione del SANS Institute[18]. Sulla base delle informazioni acquisite sui fornitori creare una lista ristretta di quelli che si intendono coinvolgere nella quotazione del progetto. L'aspetto economico in questa attività in base all'indagine svolta risulta secondario.

Partiamo dall'esito del quesito sottoposto alle aziende campione "Su quale base sceglie il fornitore"



12.1 Prevendita

Il terrore psicologico, l'incertezza, il dubbio, e l'inganno non possono essere utilizzati nelle vendite e nelle presentazioni marketing, siti web, illustrazione di test di sicurezza con l'obiettivo di vendere PT. Per cui ricevere risultati di verifiche precedenti o vulnerabilità individuate non anonimizzati è da considerare un fattore negativo. Se il fornitore chiede un permesso scritto di citare l'azienda è un indice di serietà. Con o senza un accordo di non divulgazione (NDA) il fornitore è tenuto in ogni caso a garantire la riservatezza e a non divulgare informazioni sui clienti e sui risultati dei test.

12.2 Verifica indiretta

E' necessario acquisire informazioni sul fornitore. Sapere chi è, quali referenze ha, devo verificare la presenza o meno di certificazioni di qualità, devo informarmi su chi sono le persone che svolgeranno i lavori. Nelle certificazioni vanno privilegiate quelle neutre come CISA, CISM, GIAC Certified Incident Handler (GCIH), Certified Ethical Hacker (CEH) o OSSTMM Professional Security Tester (OPST). Queste certificazioni non garantiscono la qualità, ma forniscono un certo livello di garanzia che il personale tecnico del fornitore sia stato addestrato per questo tipo di impegni. Fare attenzione anche che il PT sia svolto dal Team di esperti presentato e non svolto da personale non qualificato.

Le certificazioni rilasciate dai fornitori sono esclusivamente indice di competenza sugli elementi di sicurezza coinvolti (Es. certificazione su una marca di firewall o di antivirus).

[17] Capitolo 2.4 OSSTMM v3 - Rules Of Engagement

[18] Penetration Testing: The Third Party Hacker - SANS Institute 2006

E’ consuetudine chiedere le referenze da parte dei clienti precedenti. E' però possibile che il fornitore non sia in grado di soddisfare questa richiesta a causa di accordi di riservatezza con gli altri suoi clienti. L’azienda può chiedere al fornitore di fornire un elenco di clienti che hanno dato il loro esplicito consenso ad essere utilizzati come riferimento. Se possibile, contattare tali riferimenti per verificare le loro esperienze con il fornitore.

A volte il fornitore che non utilizza solo gli scanner, può aver identificato delle vulnerabilità non note usando tecniche manuali. Pertanto è lecito chiedere al fornitore se questo è mai avvenuto e se esiste una pubblicazione o un riferimento.

12.3 Gestione del rischio

Il PT è ovviamente, altamente insicuro e instabile. Per cui la mancanza di una pianificazione concordata fra cliente e fornitore anche in forma scritta è potenzialmente rischiosa. I contratti devono spiegare chiaramente i limiti e i pericoli del test di sicurezza come parte della dichiarazione del lavoro.

Per evitare potenziali disservizi sui sistemi e sui servizi applicativi in produzione, nel corso delle attività tipicamente non viene verificata l’applicabilità degli attacchi invasivi di tipo Denial of Service (DoS), a meno di una esplicita richiesta del Cliente.

Tutti i fornitori di servizi di PT devono avere un'assicurazione di responsabilità civile sufficiente per coprire i costi associati con il rischio di perdere informazioni di proprietà di un cliente e qualsiasi perdita potenziale di entrate che potrebbero derivare da downtime causati imprevisti dalla loro attività. I contratti devono comunque limitare la responsabilità al costo del lavoro, a meno che il dolo sia stato dimostrato. Va comunque posta attenzione nel contratto a come il fornitore si assume la responsabilità e se esiste una procedura documentata e consultabile di gestione degli incidenti e se questa viene attivata e verificata prima dell’inizio delle attività.

Una particolare garanzia per il cliente da parte dell’esecutore del test è una assicurazione che si chiama RCT Professionale, tipicamente stipulata con validità internazionale con i LLoyds di Londra. Questa garanzia a tutela del cliente prevede massimali per:

- responsabilità civile professionale:
- danneggiamento siti internet:
- responsabilità civile
- responsabilità sul prodotto
- responsabilità per danni da inquinamento
- tutela del marchio
- spese legali
- fedeltà dei dipendenti

12.4 Metodologia

E' importante non svolgere PT improvvisati che non possono fornire un approccio dettagliato di collaudo. Il fornitore dovrebbe fare uso di un metodo comunemente accettato, come OSSTMM. Richiedendo dei report di test è possibile verificare la qualità delle relazioni che vengono fornite. Per prima cosa devo notare che siano anonimizzate. Tipicamente una buona relazione include una sintesi per la direzione comprensibile e non tecnica, i dettagli tecnici delle vulnerabilità identificate compresi screenshot di riferimento, una valutazione del rischio di base, e un dettaglio completo delle azioni intraprese nel corso del PT.

12.5 Reperibilità

Durante gli incontri iniziali il responsabile del cliente PMI dovrebbe prestare molta attenzione al Project leader del fornitore per vedere se chiede e fornisce un unico punto di contatto. Entrambe le persone devono essere completamente consapevoli di come il test viene condotto, il periodo di tempo per il test e quanto approfondite saranno le prove. Il SPOC (Single Point Of Contact) sul lato cliente deve avere la autorità di intervenire durante la prova, sia per risparmiare tempo su domande che sorgessero come per fermare l'attività se si verificasse un rischio inaccettabile per il cliente. Nel caso di test remoto, il contratto deve comprendere l'origine delle analisi per indirizzo, numero di telefono o l'indirizzo IP. I contratti devono contenere i nomi dei contatti e numeri telefonici di emergenza.

12.6 Oggettività

Una delle cose che capita spesso nella PMI è che sia affidata l'esecuzione del PT al fornitore di sicurezza abituale dell'azienda. Questo è chiaramente un conflitto di interesse ma può in linea di massima essere ragionevole se ci si limita ad un Vulnerability Assessment (si veda nei capitoli precedenti la differenza fra VA e PT). Mentre in caso di PT non ha senso che il fornitore abituale faccia una autovalutazione, in quanto è implicito che adotti quelli che per lui sono i migliori standard di sicurezza. Per la correzione delle vulnerabilità l'azienda le può fare in autonomia o fornire le informazioni sulle vulnerabilità da correggere al fornitore abituale. In ogni caso è bene procedere ad una fase di Remediation Test a seguito della correzione delle vulnerabilità riscontrate dal PT.

I file di log che sono stati utilizzati dal fornitore (anche se estesi) sono l'unico modo per verificare l'attività di analisi del fornitore. Questi log devono essere consegnati dal fornitore al cliente.

12.7 Competenza

La competenza del fornitore è riscontrabile nella consulenza che viene fornita. Il compito del fornitore è quello di suggerire e concordare le specifiche tecniche per l'ambiente, le procedure applicative, l'organizzazione e le modalità esecutive del test del cliente. Spesso un buon fornitore fornisce una prima valutazione sui problemi macroscopici. Ma deve essere anche visto come una entità in grado di contribuire al raffinamento della procedura che l'azienda ha per l'esecuzione di un PT. Se il fornitore ha le certificazioni tecniche sugli elementi che costituiscono la mia infrastruttura di sicurezza questo mi assicura che possa meglio comprenderla. Se le certificazioni sono su piattaforme diverse mi manca questa assicurazione.

Anche gli elementi da valutare in un PT sono in evoluzione e impostazioni di analisi svolte nel passato possono non essere più attuali. Nell'ambito delle verifiche di sicurezza l'evoluzione è molto rapida e come testimoniato anche dal Rapporto OAI 2011[19] attualmente l'attacco più temuto, con il 76%, è il ricatto sulla continuità operativa e sull'integrità dei dati del sistema informativo, che nel 2010 risultava ultimo con un 15% sul totale dei rispondenti. Questo significa che un PT commissionato anni fa non includeva aspetti attuali come l'analisi sui device mobili o l'ambito della produzione.

12.8 Rotazione

Buona norma, adottata da molte aziende è una rotazione sul fornitore che esegue il PT. Questo garantisce una individuazione più ampia delle vulnerabilità nel tempo.

12.9 Uso dei dati del cliente

Durante un PT, le informazioni sensibili potranno essere comunicate al fornitore.

[19] Osservatorio Attacchi Informatici in Italia 2011
http://www.malaboadvisoring.it/index.php?option=com_docman&task=doc_download&gid=107

Queste informazioni possono includere i dettagli di infrastruttura, le informazioni critiche del cliente, l'attività, il Know-How e le informazioni personali dei dipendenti. La divulgazione non intenzionale di queste informazioni potrebbe avere un impatto sull'immagine dell'azienda. Per questo il fornitore deve essere disponibile a sottoscrivere un accordo di non divulgazione (NDA). Il fornitore può chiedere al cliente il suo esplicito consenso ad essere utilizzato come riferimento.

Si può chiedere al fornitore come e dove archivia le informazioni ottenute nel corso di un PT. Per garantire la riservatezza delle informazioni, al fornitore dovrebbe essere richiesto di salvare in modo sicuro crittografato solo le informazioni sensibili e di togliere o proteggere tutte le informazioni della attività che sono memorizzate su dischi condivisi.

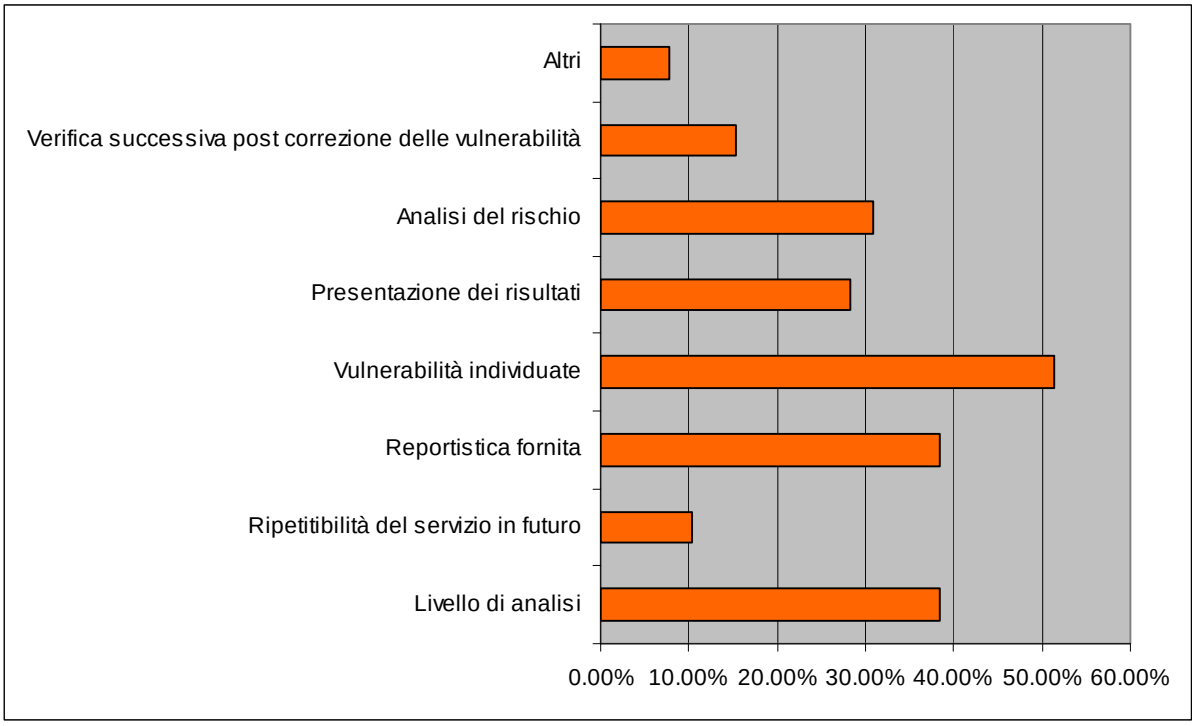
12.10 Pianificazione

Prima che il fornitore possa fare una proposta adeguata, la portata del test e gli obiettivi dovrebbero essere chiaramente definiti. In caso contrario, il fornitore deve chiedere al cliente di fornire l'obiettivo e la portata del PT per creare una proposta che sia in grado di soddisfare i requisiti. Se questo non viene fatto si rischia di limitare il campo di applicazione ad un numero ridotto di sistemi. Una mancata richiesta di informazioni è un indice di bassa professionalità del fornitore.

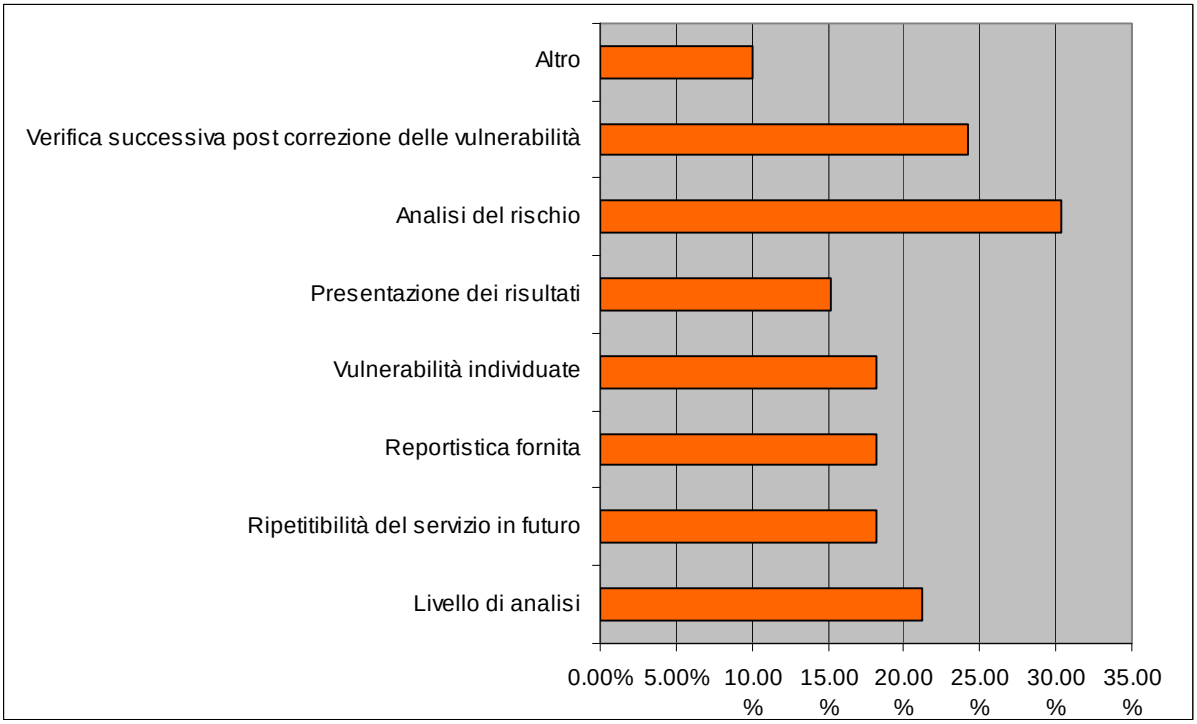
L'esecuzione di un PT deve essere eseguita sulla base di una pianificazione concordata. Questo può includere alcune restrizioni, come l'esecuzione di PT con un forte impatto al di fuori delle ore di ufficio. Per cui è necessario assicurarsi che il fornitore proponga un programma dettagliato. Compito del cliente sarà di verificare se le attività seguono questa pianificazione.

12.11 L'opinione del cliente

A controprova che questi aspetti sono tenuti in considerazione dal cliente è da valutare l'esito del quesito sottoposto al campione "Quale sono gli aspetti per le attività svolte in passato di cui sono stato **PIU'** soddisfatto"



Mentre questo è l'esito del quesito su "Quale sono gli aspetti per le attività svolte in passato di cui sono stato **MENO** soddisfatto"



13 Esito del test

L'obiettivo del documento è anche quello di stimolare la PMI nel creare una metodologia standard per registrare le verifiche di sicurezza. Sulla base della tabella definita nei requisiti per ogni bene verrà creato uno storico delle vulnerabilità individuate. Questo è un esempio di un registro delle vulnerabilità sui beni aziendali.

Codice bene	Verifica	Descrizione Vulnerabilità	Gravità	Falso positivo	Data mitigazione	Mitigazione adottata	Responsabile	Verificata
001	13/08/2012 Società xxx	Password di amministrazione debole	Alta	No	13/09/2012	Sostituzione PWD	Network Manager	Si

Nello storicizzare le vulnerabilità è importante ottenere una verifica ripetibile base di partenza di un successivo PT. Una metodologia standardizzata permette di ottenere dei test ripetibili anche se svolti da fornitori diversi permettendo un punto di partenza condiviso. Poiché le informazioni sulla valutazione della sicurezza richiedono risorse quali tempo, personale, hardware e software, la disponibilità delle risorse è spesso un fattore limitante per il tipo e la frequenza delle valutazioni di sicurezza.

Come detto nel capitolo precedente l'importanza di procedurizzare l'esecuzione di un PT dà all'organizzazione la possibilità di riutilizzare le risorse prestabilite, come personale qualificato a colloquiare con un protocollo comune al fornitore; piattaforme di prova standardizzate e requisiti concordati; con la diminuzione del tempo necessario per effettuare la valutazione si riducono i costi complessivi di valutazione.

I risultati ottenuti con gli strumenti automatici di analisi hanno spesso bisogno di essere convalidati per isolare i falsi positivi. I fornitori possono verificare le vulnerabilità manualmente esaminando il sistema coinvolto o utilizzando un secondo strumento automatizzato e confrontando i risultati. Anche se questa controprova è rapida, questo strumento di confronto, spesso produce risultati simili. L'esame manuale di una vulnerabilità fornisce in genere risultati più accurati, ma ha anche l'impatto negativo di richiedere molto tempo per cui un aumento dei costi. Spesso le cause di errore sono legate a false supposizioni sul reale stato del bene analizzato. E' però più pericoloso un falso negativo poiché sbaglia nell'identificare come sicuro ciò che non lo è, e per questo non viene corretto.

Qui la competenza del fornitore è il valore aggiunto che giustifica costi più alti a fronte di una riduzione del numero dei Falsi positivi.

Per un semplice calcolo dell'analisi del rischio questa può essere fatta mettendo in relazione il livello di vulnerabilità con la priorità che abbiamo associato alla risorsa utilizziamo la seguente tabella:

Priorità/Vulnerabilità	Bassa			Media			Alta		
Bassa	1	2	3	1	4	6	3	6	9
Media	2	4	6	4	8	12	6	12	18
Alta	3	6	9	6	12	18	9	18	27

Livello di rischio per ogni bene.

Priorità/Vulnerabilità	punteggio
Basso	1-8
Medio	9-17
Alto	18-27

Come regola generale è che il livello di rischio più elevato da il livello di rischio generale dell'azienda.

14 Documentazione prevista

Prendiamo spunto dallo standard definito dal SANS Institute[20]. Al termine dei lavori, il fornitore provvede alla stesura della reportistica di dettaglio in lingua italiana, che costituisce la documentazione formale delle differenti sessioni di verifica. Informazioni sono strettamente riservate agli incaricati designati perciò deve essere classificato come “Riservato” secondo le metodologia di classificazione del cliente.

Deve essere definito il numero di copie e il loro formato con una indicazione precisa dei destinatari. Potrebbe essere necessario trasmettere i dati di valutazione, come configurazioni di sistema o delle vulnerabilità individuate, attraverso la rete o Internet, ed è importante per garantire la sicurezza dei dati che vengono trasmessi in modo criptato per proteggerle da un accesso indesiderato.

Nel dettaglio, saranno prodotti due livelli di documentazione distinti:

14.1 Sintesi per la direzione

Questo documento è destinato allo staff dirigenziale del Cliente, che fornirà indicazioni strategiche e di facile lettura sullo stato complessivo della sicurezza riscontrato a seguito delle attività di analisi, in riferimento ai benchmark ed agli standard di mercato. Saranno in particolare evidenziati i livelli di rischio economico e di immagine, i danni potenziali derivanti, la facilità di sfruttamento delle problematiche rilevate, i rischi legali, le contromisure organizzative e tecnologiche da adottare nel piano correttivo di rientro. Una analisi costi/benefici può anche fornire ai manager una valutazione quantitativa dei maggiori risparmi da realizzare attuando la correzione alla vulnerabilità.

Il documento presenterà un riepilogo numerico delle problematiche riscontrate divise per livello di gravità.

Il documento presenterà una sintesi delle raccomandazioni che sono dettagliate nel report tecnico.

14.2 Report Tecnico

Questo documento riporterà in modo particolareggiato i risultati emersi dalle attività svolte ed i relativi dettagli tecnici, descrivendo le vulnerabilità rilevate in ordine di importanza e fornendo le relative raccomandazioni in forma di requisiti per la stesura del piano correttivo di rientro. Esso conterrà inoltre le evidenze più significative reperite nel corso delle verifiche (screenshot, output di comandi, dati di business, etc.) e le procedure seguite per acquisirle (URL, attacchi o exploit, etc.).

Esistono diversi livelli di attenzione sulle problematiche individuate ma la più ragionevole è a 3 livelli per la PMI. La valutazione deve essere oggettiva ed evitare considerazioni soggettive del fornitore.

Questi 3 livelli coincidono con valori da 1 a 3.

- **Alta**: Il sistema è o sembra vulnerabile ad un particolare attacco oppure ha delle limitazioni di sicurezza che possono compromettere l’affidabilità, confidenzialità o integrità del sistema. E’ necessario verificare se tale vulnerabilità esiste ed in tal caso trovare una soluzione.
- **Media**: Il sistema sembra in pericolo di possibile vulnerabilità. Per esempio tramite servizi e versioni conosciute come vulnerabili o servizi che potrebbero essere inutili o pericolosi. Verificare se i servizi sono necessari e se presentano delle vulnerabilità.
- **Bassa**: Informazioni relative alla sicurezza del sistema che potrebbero non essere conosciute dagli amministratori, e che potrebbero essere utilizzate da eventuali attaccanti per ottenere informazioni sul sistema.

[20] Writing a Penetration Testing Report. Alharabi 2010

Nel report tecnico la descrizione della vulnerabilità deve specificare i beni/sistemi coinvolti. La Vulnerabilità deve essere descritta e comprendere la violazione che potrebbe avvenire e il suo impatto sul bene/sistema. Se la vulnerabilità è nota va segnalata poiché significa che esiste un exploit scaricabile facilmente da internet.

La mitigazione deve essere valida e applicabile e deve essere possibile per il cliente avere le istruzioni per correggerla in autonomia.

Se possibile è necessario che sia presente un link di riferimento dove poter trovare maggiori informazioni sulla vulnerabilità.

Es di Vulnerabilità tipo

HOST	IP xxx.xxx.xxx.xxx
IMPORTANZA BENE	ALTA
VULNERABILTA'	ALTA
DESCRIZIONE	Dal software di back up presente sul server è possibile ottenere numerose informazioni pericolose. Il software in questione è yyyy, gestito dalla xxxx Srl. Si possono ottenere le seguenti informazioni: Metodo backup utilizzato: dat Percorso sorgente: //(boot etc var root) Percorso destinazione: /dev/hst3 File esclusi dal backup: Versione yyyy: 0.6.2 – 20031004 Assistenza tecnica: xxxx Srl support@xxxx.it inizio backup : 15 giugno 2012 - 23:00:01 Fine backup: 15 giugno 2012 - 23:09:23 Tempo totale: Tempo backup: 00:09:22 dati transfer: Copia di 'boot etc var root': -= OK =- (Informazioni: Byte totali scritti: 1604832960 (1.5GB, 2.5MB/s)) (Durata: 00:09:22) Esito del Backup: Es: OK Informazioni sul filesystem: Filesystem Tipoblocchi di 1M Usati Disponib. Uso% Montato su xxxxxxxxx Tali informazioni sono pericolose e possono essere usate da un attaccante per attività di "Social Engineering" (come chiedere informazioni via email alla società che gestisce il database dando i dati dell'ultimo report). Inoltre, ogni informazione ulteriore non necessaria (come i dati sulle partizioni) non deve esse disponibile pubblicamente, per evitare di facilitare operazioni di "Gathering Intelligence" (raccolta dati) del sistema e della sua sicurezza.
Mitigazione	Proteggere la directory con password o limitare l'accesso al server via firewall solo agli addetti al sistema.
Riferimenti	

15 Remediation test

Prima di essere messo in produzione, le patch o mitigazioni dovrebbero essere installate su sistemi analoghi in ambiente di test per determinare se ci sono implicazioni negative. Tali prove riducono significativamente, ma non eliminano, il rischio che un sistema reagisca negativamente alla modifica tecnica introdotta.

E' necessario tenere traccia della approvazione delle azioni di mitigazione previste prima della loro attuazione.

Questi aspetti si devono inserire in un più ampio controllo delle fasi di test e accettazione in produzione dei sistemi in generale che la PMI adotta. Le procedure di controllo devono essere particolarmente accurate al fine di garantire che vengano realizzate, e funzionino correttamente, tutte le funzionalità previste, incluse quelle concernenti le misure di sicurezza.

Deve quindi essere formalizzata ed eseguita una procedura formale di accettazione e messa in produzione.

È responsabilità dell'utente proprietario assicurare che la procedura applicativa soddisfi tutti i criteri dell'accettazione in ambiente di produzione, ivi inclusa l'accettazione dei rischi residui, e che i livelli di responsabilità del sistema siano ben documentati e consegnati alla struttura di gestione competente.

A seguito della analisi e della correzione può essere riproposta una verifica da parte del fornitore sulle correzioni apportate. Anche se limitato alle vulnerabilità individuate, il rifacimento dell'analisi comporta dei vantaggi in termini di definizione delle varie debolezze del sistema, in quanto a volte i tools utilizzati trovano vulnerabilità diverse al variare della banda disponibile e della percentuale di utilizzo del server. Inoltre le correzioni apportate ad un sistema possono introdurre nuove vulnerabilità.

Prima di effettuare questo Remediation Test, i tools utilizzati vengono aggiornati con le ultime vulnerabilità scoperte, in modo da fornire la massima scrupolosità. Questa analisi non è un nuovo Penetration Test ma si limita a verificare la correzione delle vulnerabilità riscontrate durante l'analisi iniziale.

16 Conclusioni

Il documento ha voluto analizzare l'aspetto della esecuzione di una analisi di sicurezza da parte di un fornitore esterno. Il punto di vista è stato quello dell'utente (PMI) e in particolare del committente preposto (CIO, CISO….). E' stato suggerito in che modo dare valore aggiunto alla esecuzione di una verifica di sicurezza a prescidere dall'esito. Sono state analizzate le motivazioni che dovrebbe avere la PMI nello svolgere il servizio al fine della riduzione del rischio. E' stata proposta una metodologia di gestione del processo che prevede anche una registrazione degli esiti di una analisi per riuscire ad ottimizzare l'attività ed arrivare ad una riduzione dei costi.

E' stato definito come si configura il servizio nelle sue caratteristiche di mercato, illustrando tipi, perimetro, risorse coinvolte e tutte quelle caratteristiche necessarie ad una sua valorizzazione. Nel fare questo sono state analizzate le metodologie standard, linee guida, i requisiti e le best practice esistenti ma calate sulla realtà della PMI.

Sono poi stati affrontati i punti di attenzione nel commissionare un PT e nel qualificare il fornitore analizzando anche i risultati di una indagine svolta su un campione di PMI.

17 Riferimenti

Security Through Effective Penetration Testing	ISACA JOURNAL	VOLUME 2, 2012
EUROBAROMETRO Cybersicurezza	Commissione Europea	Marzo 2012
Valutazione e gestione del rischio per due PMI	European Network and Information Security Agency	Febbraio 2007
Guidelines for Developing Penetration Rules of Behavior	SANS Institute	2001
How to choose the right vendor	Netragard Inc	2012
Network Perimeter Security Audit/Assurance Program	ISACA	2009
Technical Guide to Information Security Testing and Assessment Special Publication 800-115	National Institute of Standards and Technology	Settembre 2008
OSSTMM 3 – The Open Source Security Testing Methodology Manual	ISECOM	Dicembre 2010
OWASP Web Application Penetration Checklist	Fondazione OWASP	Luglio 2004
SECURITY ASSESSMENT– PENETRATION TESTING AND VULNERABILITY ANALYSIS DOCUMENT P8	ISACA	Luglio 2004
Penetration 101 - Introduction to becoming a Penetration Tester	SANS Institute	2002
Penetration Studies - A Technical Overview	SANS Institute	Dicembre 2001
Penetration Testing: Assessing Your Overall Security Before Attackers do	SANS ANALYST PROGRAM	Giugno 2006
Penetration Testing: The Third Party Hacker	SANS Institute	2006
Penetration Testing - Is it right for you?	SANS Institute	2002
The Impact of Cybercrime on Business	Ponemon Institute© Research Report	Maggio 2012
Il valore del Penetration Test dal punto di vista dell'auditor - -	GRUPPO DI RICERCA AIEA Roma	2005
Global Risks 2012 - Seventh Edition	World Economic Forum	2012
Rapporto Clusit 2012 sulla sicurezza ICT	Associazione Italiana per la Sicurezza Informatica	Giugno 2012
OSSERVATORIO ATTACCHI INFORMATICI IN ITALIA	Soiel International srl	Novembre 2011
IL RISCHIO INFORMATICO	CONVENZIONE INTERBANCARIA PER I PROBLEMI DELL'AUTOMAZIONE (CIPA)	Novembre 2004

Writing a Penetration Testing Report	SANS Institute	Aprile 2010
Modelli di contratto ad oggetto informatico: spunti per la negoziazione e redazione	Unindustria Treviso a cura di Cristina Franchi.	2008

ISACA VENICE Chapter
mail: info@isacavenice.org
sito: www.isacavenice.org

DOCUMENTO RISERVATO

ISACA VENICE CHAPTER

Sponsor e Sostenitori di ISACA VENICE Chapter

Sostenitore Platinum

Sponsor Platinum

Sostenitore Platinum

con il patrocinio di

ISACA – Information Systems Audit & Control Association

E' una associazione internazionale, indipendente e senza scopo di lucro. Con oltre 100.000 associati in più di 160 Paesi, ISACA (www.isaca.org) è leader mondiale nello sviluppo delle competenze certificate, nella promozione di community professionali e nella formazione nei settori dell'assurance e sicurezza, del governo dell'impresa, della gestione dell'IT e dei rischi e della compliance in ambito IT.

Fondata nel 1969, ISACA organizza conferenze internazionali, pubblica l'*ISACA Control Journal*, sviluppa standard internazionali di audit e per il controllo dei sistemi IT, che contribuiscono a facilitare il perseguimento dell'affidabilità e a trarre valore dai sistemi informativi. ISACA attesta l'acquisizione delle competenze e delle conoscenze IT mediante certificazioni riconosciute a livello internazionale quali: CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems Control).

ISACA aggiorna continuamente il frame work COBIT che assiste i professionisti dell'IT e i manager delle imprese nel far fronte alle proprie responsabilità per quanto attiene l'IT governance e la gestione manageriale, in particolare nell'ambito di assurance, sicurezza, rischio e controllo e a fornire valore al business.

ISACA Venice Chapter

E' un'associazione non profit costituita in Venezia nel novembre 2011 da un gruppo di professionisti del Triveneto che operano nel settore della Gestione e del Controllo dei Sistemi Informativi: è il terzo capitolo italiano di ISACA.

Riunisce coloro che nell'Italia del Nord Est svolgono attività di Governance, Auditing e Controllo dei Sistemi Informativi promuovendo le competenze e le certificazioni professionali sviluppate da ISACA.

L'associazione favorisce lo scambio di esperienze, promuove un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo sia di affidabilità dell'organizzazione sia di sicurezza dei sistemi.

Vantaggi per chi si associa ad ISACA Venice

Iscrivendosi ad ISACA Venice automaticamente si è soci di ISACA, e si ottiene:

accesso gratuito:
- ai meeting di ISACA Venice
- alle pubblicazioni riservate ai soci di ISACA eLibrary
- al framework COBIT©
- ai webcasts e agli e-Simposium organizzati da ISACA

sconti:
- sulle pubblicazioni ISACA (Bookstore)
- sulle quote d'iscrizione e sulle pubblicazioni di preparazione agli esami CISA, CISM, CGEIT, CRISC

partecipare ai corsi professionali organizzati da ISACA Venice proposti a costi favorevoli

ricevere gratuitamente l'ISACA Journal

ISACA VENICE Chapter

Quaderni

Vulnerability Assessment e Penetration Test

Linee guida per l'utente di verifiche di terze parti sulla sicurezza ICT