Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Vulnerability assessment e penetration test: Case study ICAR-CNR e Sicur Control System

Danilo Cistaro, Agostino Forestiero,
Antonio Francesco Gentile e
Francesco Monteleone

RT-ICAR-CS-15-01 **Gennaio 2015**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 41C, 87036 Rende, Italy, URL: *www.icar.cnr.it*
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: *www.na.icar.cnr.it*
– Sezione di Palermo, Viale delle Scienze, 90128 Palermo, URL: *www.pa.icar.cnr.it*

1. Introduzione

Nel presente elaborato si vogliono presentare i risultati ottenuti dall'esecuzione dei test per la valutazione della sicurezza della rete dell'ICAR-CNR effettuati dalla Sicur Control System, società afferente al polo di innovazione ICT-SUD, di cui fa parte anche l'istituto. 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.

L'adozione di specifiche misure di sicurezza logica costituisce in sempre più numerosi settori un obbligo normativo previsto dalla legge o dai regolamenti di settore. Per il settore dell'informatica e telecomunicazioni 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.

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.

Tutto ciò 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 delle società per le quali la continuità operativa e/o la protezione delle informazioni e della proprietà intellettuale 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.

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.

2. La Sicurezza

Il problema della sicurezza informatica all'interno delle aziende viene spesso sottovalutato in quanto comporta una spesa iniziale senza un immediato beneficio, anche se la legge italiana prevede l'adagiamento alle misure minime di sicurezza (D.Lgs. 30/06/2003, n. 106) per imprese, pubblica amministrazione ed enti pubblici, o chiunque utilizzi sistemi informatici per scopi economicamente rilevanti, anche se non a scopo di lucro. Garantire la sicurezza di un sistema informatico consiste nell'assicurarne la non violabilità da parte di persone non autorizzate, al fine di garantire ***confidenzialità***, ***integrità*** e ***disponibilità*** dei dati. La ***confidenzialità*** di un dato è la capacità di un sistema di garantire che solamente gli utenti autorizzati possano accedere a quel dato, caso tipo l'accesso alla posta elettronica privata. L'***Integrità*** è la proprietà che garantisce che il dato possa essere modificato **solamente** da utenti autorizzati. Un dato è integro se nell'esecuzione dell'applicazione che lo contiene, viene modificato esclusivamente dall'applicazione stessa.

Infine, la ***Disponibilità*** invece riguarda la possibilità degli utenti **autorizzati** di avere sempre accesso ad un certo dato o risorsa. Anche se questo concetto può sembrare ovvio in sistemi complessi può essere messo in secondo piano senza essere implementato e controllato da solide policy.

I concetti di ***autenticazione*** e ***autorizzazione*** spesso vengono confusi se non equiparati, è quindi importante sottolinearne le differenze. L'***autenticazione*** è il processo attraverso il quale un sistema determina l'identità di un utente. L'***autorizzazione*** è il processo attraverso il quale un sistema garantisce o meno l'accesso a una risorsa da parte di un utente.

Con il termine di ***auditing*** indichiamo la valutazione effettuata su un generico sistema, progetto o prodotto, è ha come scopo ad accertarne l'affidabilità.

Si definisce invece ***Vulnerability Assessment*** l'analisi di un'applicazione software mirata alla ricerca di errori o bug che, se opportunatamente sfruttate, possono costituire delle vulnerabilità per la sicurezza dell'applicazione stessa. Con ***Penetration Test*** si intende invece l'attività attraverso al quale un esperto di sicurezza informatica verifica la robustezza di un sistema informatico contro tentativi di attacco e/o accesso non autorizzato.

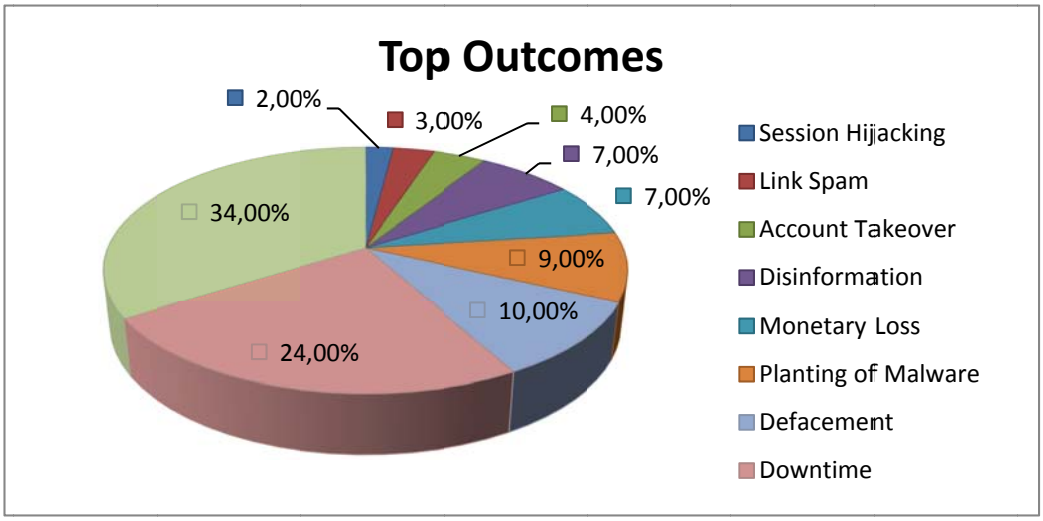
Solitamente è sempre opportuno iniziare con l'attività di vulnerability assessment e poi eventualmente proseguire con la penetration test, tenendo sempre presente che la sicurezza non è una scienza perfetta ma un processo a tendere, è quindi importante valutare sempre il costo del rischio e il costo della difesa applicando il "*principio del minimo rischio (o costo)*".

La ***vulnerabilità*** o ***falla*** di un sistema informatico è una caratteristica di un suo componente per cui risulta suscettibile a particolari situazioni che portano al guasto, spesso improvviso, del componente stesso o di un particolare ad esso direttamente correlato.

La ***minaccia*** è la causa che *scatena la falla* di cui sopra, generalmente non dipende da problemi strettamente implementativi, ma da comportamenti anomali degli utenti, fra questi è opportuno fare delle distinzioni fra: gli *hacker*, tester esperti della materia che tentano di stressare il sistema al fine di migliorarlo oppure di aumentare il loro grado di conoscenza; i *cracker*, che sfruttano le stesse tecniche e gli stessi strumenti degli hacker ma con fini differenti e spesso illegali, fra cui non mancano le frodi; i *phreaker* invece raramente esperti, utilizzano tool freeware e tutorial reperibili nella rete per divertimento personale.

Negli ultimi anni si sta diffondendo una distinzione fra "**Hacking for Profit**" e "**No-Profit Hacking**", mentre quest'ultimo è effettuato quasi esclusivamente per motivi ideologici o di divertimento, i primi "Hacking for Profit" sono realizzate da cyber-criminali professionisti, che

sono continuamente alla ricerca di nuove vie attraverso le quali attuare gli attacchi informati che consentono di realizzare falici guadagni: in questo scenario, le applicazioni web costituiscono certamente il bersaglio principale.
L'obiettivo primario degli attacchi è il furto d'informazioni, e ciò è facilmente spiegabile: vengono portati attacchi ai siti di e-commerce allo scopo di rubare i dati sensibili dei clienti, questi dati vengono poi venduti sul mercato nero, a cui interessano per mettere in atto ulteriori attività fraudolente.
Il grafico di seguito mostra i principali obiettivi relativi all' hacking for profit [https://www.trustwave.com/].



Il ***rischio*** diventa elevato nel momento in cui il sistema, affetto da vulnerabilità, diventa oggetto di attenzione da parte di soggetti portatori di una minaccia (ad esempio un cyber-criminal). Il livello di rischi sarà proporzionale al numero di falle ed al numero di attacchi. Possiamo quindi ipotizzare che maggiore sarà il valore dei dai da proteggere, maggiori saranno gli sforzi che una attaccante sarà disposto a compiere per trovare la vulnerabilità. Il rischio è tanto più elevato quanto più è elevato il valore dei dati da proteggere. Possiamo quindi scrivere:

vulnerabilità x minaccia = rischio

3. La continuità operativa

In caso di evento che determini l'interruzione dell'operatività ordinaria, assume particolare importanza la presenza in azienda di un *business continuity plan* che contempli tutte le attività volte ad assicurare la prosecuzione dei processi di business considerati critici. Esso è costituito dall'insieme dei piani di continuità sviluppati per ogni singola funzione interessata e prevede processi organizzativi di ripristino differenziati in funzione della gravità degli eventi presi in considerazione e del grado di importanza/essenzialità dei processi.
Nell'ambito di tale piano specifico rilievo rivestono le misure di *disaster recovery* tese a consentire, nell'ipotesi di evento disastroso, una ripartenza dei sistemi informatici nel più breve tempo possibile, attraverso, ad esempio, la definizione di piani organizzativi di intervento e il sistematico salvataggio dei dati presso la propria sede e presso una sede alternativa, opportunamente individuata, dotata di apparecchiature elaborative in grado di prendere in carico l'attività primaria dell'azienda.

Policy aziendale "aspetti sulla sicurezza IT"

Nell'ambito di un sistema informatico "*sicuro*" vanno tenuti ben presenti i rischi connessi con le attività di implementazione e gestione di applicazioni, sistemi operativi e reti. In quest'ambito possono rinvenirsi delle vulnerabilità in grado di generare minacce alla riservatezza, all'integrità e alla disponibilità delle informazioni aziendali, come ad esempio:

- la presenza di errori involontari commessi in fase di progettazione e/o implementazione che possono consentire a utenti non autorizzati l'esecuzione di operazioni e programmi riservati a altre categorie di utenti;
- la presenza di un codice malizioso inserito volontariamente dai programmatori del sistema o dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate (rientrano in queste categorie di minacce i virus, i *trojan horse*, le *backdoor*, ecc.)

Esaminiamo adesso nel dettaglio, le attività da porre in essere al fine di far fronte a tali minacce, tenendo presente che, per poter definire sicuro un sistema o un'applicazione occorre che siano soddisfatti non soltanto i requisiti di ***riservatezza, integrità e disponibilità***, ma anche quelli di:

- autenticità – ovvero che sia possibile accertarsi che l'applicazione/sistema con cui si sta interagendo sia proprio quello atteso;
- tracciabilità - ovvero che rimanga traccia dei dettagli di ogni operazione effettuata in modo da consentirne l'eventuale ricostruzione;
- non ripudiabilità - ovvero che né il mittente né il destinatario di uno scambio informativo possano negare di avere inviato/ricevuto i dati in questione.

La sicurezza nello sviluppo e nella manutenzione delle applicazioni

Per sviluppo e manutenzione delle applicazioni si intende l'insieme delle attività di realizzazione, installazione e aggiornamento dei prodotti software sviluppati per il fabbisogno aziendale, sia che siano prodotti internamente, sia che vengano acquisiti all'esterno come pacchetti ed eventualmente personalizzati per le proprie esigenze.

Nella catena dello sviluppo e della distribuzione del software (analisi, stesura delle specifiche, sviluppo, test, rilascio), come anche nel processo di manutenzione, si possono facilmente evidenziare talune vulnerabilità, dovute anche al coinvolgimento di risorse sia interne sia esterne.

I test effettuati per l'accettazione dell'applicazione, benché ampi, possono non evidenziare tutti gli errori e non danno certezza assoluta che l'applicazione esegua correttamente tutto e solo quanto dichiarato.

Eventuali malfunzionamenti rappresentano pertanto un potenziale rischio per la sicurezza aziendale poiché:

- possono compromettere la disponibilità, la riservatezza e l'integrità di una parte più o meno critica del sistema informativo;
- possono essere rilevati tardivamente; è quindi sempre possibile che errori avvenuti nella realizzazione di un'applicazione si presentino durante l'utilizzo nell'ambiente aziendale, anche parecchio tempo dopo il rilascio in esercizio.

A fronte dei predetti rischi possono essere adottate specifiche contromisure quali:

- utilizzo dei soli software acquisiti o sviluppati lecitamente, secondo procedure verificate dalle strutture aziendali preposte;
- gestione costante di un inventario del software e delle relative licenze, al fine di verificare la lecita installazione di ciascun prodotto; a tal fine è utile disporre di uno strumento di *asset management* che correli il software al relativo hardware;
- adozione di un processo interno di "certificazione/validazione" della produzione del software, che garantisca la qualità dei test, l'originalità e l'integrità del codice. Per tale ultimo aspetto potrà essere utilizzato un codice di validazione o una firma elettronica;
- disponibilità di ambienti separati per il test, il collaudo e la produzione, evitando di mettere in produzione qualsiasi software senza prima averne verificato la funzionalità e la compatibilità con il resto del sistema;
- fissazione di norme specifiche per lo sviluppo, la modifica, la copia e la cancellazione dei programmi;
- formalizzazione di procedure autorizzative per l'inserimento/variazione dei programmi nel sistema;
- adozione di procedure di *change management* per tutte le modifiche in modo da poter tenere traccia di tutte le variazioni apportate;
- classificazione dei programmi;
- contrattualizzazione con i fornitori del rispetto delle *policy* di sicurezza e verifica della loro osservanza;
- divieto di utilizzo di programmi e/o applicazioni prelevati da Internet o forniti da terze parti e non formalmente autorizzati dall'azienda;

- attivazione di meccanismi di *back-up* e *recovery* che permettano di avere sempre a disposizione il salvataggio di precedenti versioni di programmi e/o dati per eventuali ripristini;
- identificazione del responsabile del passaggio in produzione di ciascun programma;
- protezione adeguata, anche tramite strumenti crittografici, delle basi dati di sicurezza (con l'utilizzo, ad esempio, di chiavi di autenticazione o di crittografia);
- eliminazione periodica di tutto il software obsoleto per evitare utilizzi non consentiti e/o inutili oneri di manutenzione;
- previsione, per l'espletamento di operatività particolarmente critiche, dell'intervento contemporaneo di più persone (*four eyes principle*);
- definizione delle regole di trasferimento a terzi del software o dell'hardware su cui il software è installato (ad esempio in caso di outsourcing);
- redazione e aggiornamento di tutta la documentazione a supporto delle varie fasi del ciclo di vita del software.

Un altro aspetto importante che va attentamente curato riguarda lo sviluppo dei presidi di sicurezza nelle applicazioni.
A livello di studio di fattibilità o di documenti di *start-up* di un progetto, l'utente deve fornire una chiara rappresentazione del livello di sicurezza richiesto in termini di disponibilità, riservatezza e integrità. Tale attività può essere svolta attraverso la compilazione di *check-list* che costituiranno la documentazione da allegare agli studi di fattibilità o agli analoghi documenti che costituiscono lo *start-up* del progetto.
Una volta identificata la tipologia di presidi da applicare al progetto, è necessario precisarne le fasi di sviluppo, che possono articolarsi come segue:

- definizione dei requisiti di sicurezza utente e analisi dei rischi;
- definizione delle specifiche di dettaglio dei requisiti di sicurezza;
- definizione del piano di test di sicurezza e dei criteri di accettazione;
- analisi degli impatti di sicurezza connessi con specifiche esigenze dell'architettura applicativa e/o tecnologica (es. utilizzo di pacchetti software di mercato; necessità di supporto remoto da parte della casa costruttrice; ricorso all'esterno per la gestione del sistema);
- scelta e acquisizione delle soluzioni tecniche di sicurezza, avendo presenti fattori quali: la coerenza con gli standard aziendali; la possibilità di attivare le funzionalità di sicurezza in modo trasparente all'utente; la facilità di utilizzo; l'informativa all'utente circa l'attivazione delle funzionalità di sicurezza; la robustezza delle funzionalità fornite;
- predisposizione delle procedure tecnico–organizzative che descrivano in dettaglio gli adempimenti tecnici e procedurali per l'applicazione dei presidi in linea con gli standard aziendali;
- collaudo e accettazione dei presidi di sicurezza.

La sicurezza nella gestione dei sistemi operativi

Il sistema operativo costituisce la base su cui poggiano tutte le applicazioni dell'utente.

Pertanto, particolare cura deve essere posta nelle fasi di installazione, messa in opera ed evoluzione del sistema, con particolare riferimento agli aggiornamenti resi disponibili dal fornitore, soprattutto se finalizzati a rimuovere problemi di sicurezza.

Tali attività richiedono elevate competenze tecnico-specialistiche per ciascun tipo di ambiente/software e spesso devono essere effettuate operando con privilegi di sicurezza elevati e prevedono di norma il coinvolgimento di risorse interne ed esterne.

Una volta progettati in modo sicuro, i sistemi devono essere gestiti in modo altrettanto sicuro: è opportuno pertanto progettare anche la sicurezza di gestione. Tra le varie attività da prevedere rilevano, in particolare:

- il controllo degli accessi ai sistemi;
- la definizione dei principi da seguire nella fase di configurazione dei sistemi;
- l'applicazione di *policy* di *change management* che rispettino l'architettura di sicurezza progettata;
- la definizione di procedure di gestione dei malfunzionamenti;
- l'applicazione di misure di prevenzione da utilizzare in caso di malfunzionamenti, come i *back-up*;
- l'applicazione di regole di segregazione (delle responsabilità, delle mansioni, degli ambienti operativi, delle funzioni) per tutte le risorse;
- l'uso di particolari software di *utility* e l'applicazione delle *fix* che pongono riparo ai *bug* di sicurezza rilevati;
- il monitoraggio dei sistemi di sicurezza posti a protezione dei sistemi operativi.

Controllo degli accessi ai sistemi

Tutti i sistemi, inclusi quelli di gestione, devono prevedere meccanismi di identificazione e autenticazione. L'accesso alle risorse deve essere sottoposto a sistemi di controllo degli accessi che verifichino i profili del soggetto e delle entità che richiedono l'accesso, registrino ed eventualmente rifiutino quegli accessi che non rientrano nei profili autorizzati e anche quelli che non seguono percorsi prestabiliti.

Tutti i terminali e gli apparati devono essere univocamente identificati, tramite opportune convenzioni di nomenclatura, e non deve essere permesso l'accesso ai servizi e ai sistemi da parte di apparati non riconosciuti. I terminali devono essere anche provvisti di meccanismi di autenticazione del terminale stesso, in modo da garantire la sicurezza di specifiche transazioni od operazioni (che possono, in questo modo, essere eseguite in modo vincolato a una specifica postazione o a uno specifico utente).

I principi per la configurazione dei sistemi

Particolare cura va posta nella fase di configurazione dei sistemi, al fine di contrastare le possibili minacce connesse con l'eventualità di indebiti accessi al software di base e di attacchi esterni.

In particolare deve essere attuata una politica di *hardening*: con tale termine, riferito a un prodotto software (es. un sistema operativo), si intende quella attività di configurazione che si basa sul principio che "quello che non c'è non può essere sfruttato per condurre attacchi", il che porta a eliminare dal software le parti/servizi/funzioni non strettamente necessari.

Change management

I processi di *change management* (es. gli aggiornamenti del sistema operativo) devono essere eseguiti nel rispetto di regole predefinite, quali:

- la separazione delle librerie: ove possibile le partizioni riservate al sistema operativo devono contenere solo codice eseguibile;
- per l'accesso alle librerie relative alle componenti di base deve essere applicato il principio del "minimo privilegio";
- il rilascio di componenti di base deve essere:
    - consentito unicamente a personale o a processi espressamente autorizzati dal corretto livello manageriale;
    - autorizzato esclusivamente in presenza della documentazione che attesti il superamento di test di accettazione;
    - effettuato previa predisposizione di un piano di ripristino della situazione precedente in caso di problemi.
- la registrazione di tutti gli aggiornamenti e le variazioni apportate ai sistemi e la protezione di queste registrazioni;
- il costante allineamento della documentazione di supporto al sistema sia per l'operatività corrente sia per utilizzo in caso di emergenze;
- la conservazione delle versioni precedenti;
- l'effettuazione di test di accettazione documentati del sistema prima del passaggio in produzione;
- l'attivazione in produzione del sistema a seguito di un'autorizzazione formale.

Gestione dei malfunzionamenti

Tutti i malfunzionamenti relativi ai sistemi devono essere registrati e devono formare una base di conoscenza per la valutazione dei parametri di affidabilità dei sistemi. Dovrebbero essere oggetto di valutazione statistiche relative, ad esempio, al tempo medio tra due successivi guasti -MTBF (*mean time between failures*), al tempo medio di ripristino - RMT (*recovery mean time*), al tempo medio di rimozione della causa che ha generato l'incidente -MTTR (*mean time to repair*).

La gestione dei malfunzionamenti consiste nella rapida presa di conoscenza dell'evento, nell'analisi di primo ed eventualmente secondo livello del problema che è stato generato, nella approvazione delle soluzioni proposte (eventualmente coinvolgendo anche i proprietari delle applicazioni), nell'attuazione di queste soluzioni e nella documentazione della soluzione adottata.

Back-up
Le *policy* di *back-up* devono essere definite a livello aziendale in funzione della criticità dei dati elaborati dai sistemi e devono prevedere:

- un livello minimo di *back-up*12;
- le modalità di conservazione dei *back-up*;
- le regole e i profili di accesso ai *back-up*;
- il tempo di *retention* per le informazioni essenziali e le regole relative al *back-up* di informazioni che devono essere conservate indefinitamente (è essenziale in questi casi assicurare la "bontà" del *back-up* anche a fini legali);
- le modalità di distruzione dei *back-up* obsoleti.

Particolare attenzione deve essere posta, infine, alla verifica e alla documentazione delle procedure di ripristino: devono essere in particolare stabiliti e testati i tempi di ripristino che hanno impatto sui livelli di servizio.

Regole di segregazione
Si tratta di regole che disciplinano la separazione delle applicazioni e dei sistemi con l'obiettivo di ridurre la concentrazione di criticità e consentire l'adeguata applicazione dei presidi di sicurezza su un numero limitato di elementi proteggendoli da interazioni e effetti determinati, anche involontariamente, da altri sistemi e applicazioni. Tale misura permette anche di mettere in pratica il principio del "minimo privilegio".

Software di utility e applicazione di fix
L'uso dei software di *utility* e l'applicazione di *fix* ai sistemi sono funzioni critiche che occorre monitorare strettamente perché tramite esse è possibile compromettere l'integrità e la disponibilità (nonché la riservatezza) del sistema e delle applicazioni. Occorre pertanto: controllare che tali funzioni siano effettuate nel rispetto dei privilegi di accesso, verificarne la funzionalità, inibirne l'utilizzo durante i processi critici, registrarne l'utilizzo (log).

Monitoraggio
I processi di monitoraggio dei sistemi di seguito indicati hanno lo scopo di verificare i livelli di efficacia ed efficienza prefissati ed eventualmente anche contrattualizzati:

- *capacity planning*: devono essere previste e pianificate, a livello aziendale, le necessità future in termini di capacità operativa al fine di evitare pericolosi "colli di bottiglia" nei processi di implementazione o di *upgrading* dei sistemi;
- monitoraggio dell'uso dei sistemi e di particolari eventi; deve essere prevista una registrazione per le seguenti aree:
    - accessi autorizzati effettuati e tentativi di accesso non autorizzato;
    - operazioni con privilegi particolari (fra cui le modifiche alle *policy* di audit e di *accounting*, la gestione di utenze/gruppi/ecc.);
    - *shut down/restart* dei sistemi;
    - allarmi o incidenti del sistema.

L'analisi degli eventi prevede l'esame di grandi masse di dati utilizzando sistemi automatici (es. *Intrusion Detection System*, analizzatori di log) coerentemente con le *policy* stabilite.

La sicurezza nella gestione delle reti

La sicurezza nella gestione delle reti e dei servizi resi attraverso le reti stesse si avvale di una articolata serie di presidi: fondamentale è innanzitutto l'adozione di misure di controllo degli accessi e di monitoraggio analoghe a quelle previste per i sistemi operativi; rilevano poi misure specifiche, quali ad esempio:

- autenticazione delle connessioni esterne e autenticazione dei nodi: poiché l'accesso dall'esterno rappresenta una fonte potenziale di rischio per l'organizzazione, è estremamente importante che il processo di presentazione sia oggetto di autenticazione. Anche in questo caso il livello di autenticazione deve essere proporzionale al livello di rischio. Occorre valutare in particolare il livello di sicurezza offerto da soluzioni che prevedono l'uso di tecniche di autenticazione forte, quali *token hardware*, protocolli "a sfida", procedure di *callback*, ecc. L'autenticazione dei nodi può essere complementare all'autenticazione di gruppi di utenti remoti connessi a sistemi sicuri;
- protezione delle porte di diagnostica remota: le porte di diagnostica remota e quelle utilizzate per la gestione degli apparati devono essere disabilitate o controllate da dispositivi fisici e procedure di abilitazione esplicite e formalizzate che impediscano di intervenire sul sistema senza controllo;
- regole sulle limitazioni di utilizzo delle connessioni di rete: è importante che siano attivati meccanismi e procedure che limitino la possibilità per un utente di connettersi alle risorse di rete in modo non controllato. È consigliabile in questo senso l'utilizzo di tavole e regole che filtrino il traffico in base a *policy* generali di controllo accessi, esigenze di business e requisiti delle applicazioni. Devono in particolare essere regolate le seguenti funzioni: la posta elettronica, i meccanismi di *file transfer*, gli accessi interattivi;
- politiche di *routing*: per la gestione sicura delle reti è necessario prevedere la definizione di precise regole di instradamento, sia per ottimizzare il bilanciamento dei carichi, sia per garantire la separazione dei flussi critici e quindi la possibilità che apparati divengano *single point of failure*;
- politiche di gestione degli *sniffer*, ovvero delle apparecchiature che possono essere collocate sulla rete per rilevare ai fini della sicurezza il tipo di traffico in transito; la definizione di tali *policy* è critica, considerato che tramite *sniffer* possono essere anche condotti attacchi alla sicurezza informatica (cfr. oltre);
- percorsi obbligati: la flessibilità e la condivisione di un gran numero di risorse, richiesta implicitamente dai requisiti di interconnessione, rappresenta una debolezza in termini di controllo e facilita anche la possibilità per i malintenzionati di produrre danni all'organizzazione che si avvale sempre più dei servizi di rete. La misura principale per ridurre questi rischi è quella di forzare il percorso tra l'utente di rete e le risorse accedute limitando le opzioni di instradamento.

Aspetti di sicurezza connessi con l'utilizzo di nuove tecnologie

Poiché l'utilizzo delle nuove tecnologie informatiche può esporre l'azienda a molteplici rischi, non sempre adeguatamente percepiti e valutati (es. patrimoniali, legali, di immagine, di sicurezza), è necessario fornire al personale idonee indicazioni e istruzioni sull'utilizzo delle stesse, al fine di evitare comportamenti, anche inconsapevoli, non corretti.

Nei paragrafi che seguono il tema della sicurezza informatica è trattato in relazione al mondo Internet (inteso non solo come accesso al *World Wide Web* ma anche come tecnologia al servizio dello sviluppo applicativo), alla gestione della posta elettronica e all'utilizzo di dispositivi di *mobile computing*; sono infine descritte le nuove tipologie di attacco – e le relative contromisure – che vanno diffondendosi in relazione all'utilizzo di tali tecnologie.

4. Utilizzo di Internet in ambito aziendale

Accesso al World Wide Web

I principali rischi connessi con l'accesso ai siti web sono quelli derivanti dalla possibilità che l'utente, anche in modo inconsapevole, installi sul proprio posto di lavoro (e veicoli nella rete aziendale alla quale esso è connesso) del codice potenzialmente "dannoso" (virus e *trojan horse*), progettato, ad esempio, per alterare o catturare dati, spedire documenti all'esterno, generare un traffico elevatissimo in rete, aprire "varchi" sul computer per consentire il controllo remoto del sistema da parte di soggetti malintenzionati. Tramite i varchi anzidetti eventuali *hacker* possono presentarsi nelle LAN come un utente interno, una volta superate le difese perimetrali; tale possibilità non deve essere trascurata quando si progettano le contromisure.

Vanno altresì tenuti in considerazione i costi e le inefficienze connessi con il tempo impiegato dai dipendenti nella consultazione di pagine web non strettamente correlate all'attività aziendale.

Pur avendo presente che la scelta delle modalità per garantire l'accesso sicuro alla rete Internet in ambito aziendale deve essere effettuata dalle singole aziende secondo approcci funzionali agli specifici obiettivi perseguiti, si forniscono di seguito alcune indicazioni di massima sulle possibili contromisure da attivare in relazione ai predetti rischi:

- tempestivo aggiornamento dei software di base e delle configurazioni dei prodotti tramite *patch* o *service pack* fornite dal produttore;
- accesso a Internet tramite stazioni di lavoro dedicate, isolate dalla rete aziendale, oppure realizzando un disaccoppiamento logico tra le stazioni di lavoro e la navigazione mediante l'utilizzo di strumenti di emulazione di terminale;
- separazione degli ambienti e delle reti utilizzando la separazione fisica o logica per creare "domini di sicurezza" a protezione degli *asset* ritenuti più importanti;
- utilizzo di software che impediscono l'accesso a determinati siti contenuti in una *black list* o che rispondano a determinati requisiti, fissati dall'azienda, e valutati di volta in volta da un sistema esperto che ne analizza il contenuto15; in alternativa, può essere consentito l'accesso soltanto a determinati siti contenuti in una *white list*; dette liste possono essere gestite direttamente dall'azienda oppure dal fornitore;

- accesso al mondo esterno via *proxy server*, ai quali spetta anche la verifica dell'abilitazione all'accesso dei dipendenti;
- utilizzo di *firewall* sulla rete aziendale e di *personal firewall* anche sui computer portatili;
- utilizzo di un prodotto antivirus su tutti i computer (*server* e *client*), sistematicamente e tempestivamente aggiornato;
- importazione controllata dei file mediante scansione dei flussi, privando i file stessi di ogni contenuto attivo (eseguibili, macro, ecc.);
- ricorso a sistemi di *intrusion detection*;
- uso di tecniche VPN per accessi "in remoto";
- duplicazione delle risorse critiche;
- predisposizione di appositi piani di *contingency* per poter contrastare le diverse eventuali tipologie di attacco, prevedendo anche azioni drastiche quali la disconnessione di taluni sistemi o addirittura l'interruzione dei servizi di rete;
- adeguamento costante delle infrastrutture tecnologiche a fronte dei nuovi rischi e delle nuove vulnerabilità;
- creazione di una struttura di intervento da contattare in caso di sospetto attacco informatico;
- definizione di una *policy* per l'utilizzo di Internet, inserita nelle *policy* di sicurezza e portata a conoscenza di tutto il personale.

Particolare attenzione va posta inoltre alla scelta dell'ISP (*Internet Service Provider*) e alla relativa contrattualizzazione dei livelli di servizio, ivi inclusi i presidi di sicurezza ritenuti più adeguati al livello di protezione che l'azienda intende conseguire.
Problemi analoghi a quelli appena descritti si possono porre nell'utilizzo delle **intranet aziendali**: infatti, in relazione alla caratteristica di accesso a diffusione capillare, tali infrastrutture sono spesso utilizzate dai virus per la diffusione di codice malevolo all'interno dell'azienda.

La sicurezza delle applicazioni web-based
Nello sviluppo di applicazioni basate su tecnologia web, va rivolta particolare attenzione ai rischi che l'utilizzo di detta tecnologia può presentare e vanno tenute in considerazione le principali contromisure a oggi note.
Se da una parte l'impiego del *browser* consente di realizzare applicazioni più snelle, dall'altra va considerato che in quest'area lo sviluppo applicativo presenta alcuni peculiari aspetti critici, connessi da una parte con scelte orientate alle funzionalità più che alla sicurezza e, dall'altra, con la necessità di prevedere collaudi specifici, coerenti con le vulnerabilità proprie del mondo web, e sistematici test di vulnerabilità e di intrusione sui *server* e sui *client.*
La pericolosità delle applicazioni *web-based* deriva dalla diffusione di tecnologie di *scripting* (Active X, ASP, ecc.) che spesso sono in grado di superare la sicurezza del sistema e/o suscettibili di veicolare codice malevolo. In particolare possono presentarsi le seguenti minacce dirette a *web application server*: accessi non controllati ai servizi di rete, vulnerabilità di sicurezza del sistema operativo e del sofware applicativo, sfruttamento della configurazione aperta del sistema operativo e del software web, disponibilità di software non necessario, disponibilità di funzionalità pericolose,

errori di scrittura del codice, interazione con i *client*, attacchi diretti ai controlli formali (dati di input, URL, informazioni utili, ecc.), esecuzione remota di software.
Le principali contromisure relative alle minacce citate sono basate sull'adozione di log e strumenti di controllo, su un'attenzione massima in fase di disegno dell'applicazione, sulla definizione di un'architettura applicativa che preveda un *client* il più possibile *light* - cioè scarico da funzionalità applicative -, sull'utilizzo di un'appropriata metodologia di sviluppo del codice sicuro.
Risulta infine indispensabile per le applicazioni che nascono o che vengono "tradotte" in tecnologia web effettuare, prima della consegna in ambiente di produzione, un *application vulnerability assessment*, basato sull'analisi del codice applicativo e volto essenzialmente a individuare eventuali errori di programmazione e/o vulnerabilità dell'architettura, avvalendosi di appositi strumenti di test.

Posta elettronica
La rapida diffusione della posta elettronica nelle aziende, favorita dalle sue caratteristiche di semplicità d'uso e di standardizzazione, non sempre è stata accompagnata da una piena consapevolezza dei rischi insiti nel suo utilizzo, quali ad esempio:

- attacchi tramite virus/*trojan horse*, che possono diffondersi a tutti i sistemi elaborativi aziendali;
- intercettazione e modifica dei messaggi durante la trasmissione (attacco definito "*the man in the middle*");
- indisponibilità del servizio per la mancanza di connessione o al *server* di posta o alla rete;
- identificazione non certa del mittente;
- non certezza della consegna al destinatario;
- accesso non autorizzato al contenuto delle caselle di posta.

Alla mancata adozione di misure di sicurezza nella posta elettronica è altresì associata l'esposizione a rischi di tipo legale; tra questi rilevano, ad esempio, quelli connessi con l'inosservanza delle prescrizioni normative di cui al D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) ovvero quelli derivanti da un'eventuale integrazione della fattispecie di reato di cui all'art. 615 quinquies del codice penale, che punisce la diffusione di programmi che provochino il danneggiamento, l'interruzione o l'alterazione del funzionamento di un sistema informatico o telematico.
Non bisogna poi dimenticare particolari fenomeni che possono presentare profili di illegalità come, ad esempio, il cosiddetto *spamming*, volontario o involontario.
Un'ulteriore delicata problematica è quella relativa all'utilizzo della posta elettronica da parte dei dipendenti per finalità non correlate all'attività aziendale (analoga questione si pone per la consultazione dei siti Internet); si tratta di una pratica che può esporre l'azienda a rischi di natura economica, per i costi sostenuti e per la possibile perdita di produttività del personale, oltre che a rischi legali e di immagine. Nell'adozione delle necessarie contromisure , l'azienda dovrà peraltro tenere conto dell'esigenza di operare un corretto bilanciamento tra gli interessi aziendali e i diritti dei lavoratori, in materia ad esempio di tutela della riservatezza.
A fronte delle diverse tipologie di rischio sopra descritte l'azienda può quindi adottare varie contromisure, tecnologiche e organizzative, quali ad esempio:

- utilizzare più antivirus in sequenza - di produttori diversi - per analizzare i flussi di posta;
- applicare filtri sugli allegati mediante *black-list* o *white-list*;
- configurare in sicurezza i *client* di posta elettronica;
- non consentire l'invio di posta da parte di utenti non autenticati sulla rete aziendale;
- bloccare comunque le e-mail rilevate infette, disattivando la funzione di bonifica, in modo da evitare di esportare informazioni, anche inconsapevolmente.

È poi necessario emanare *policy* dirette agli utenti interni che prevedano:

- istruzioni per l'utilizzo della posta elettronica aziendale, che deve essere limitato alle sole finalità aziendali;
- indicazioni sulle modalità per l'eventuale consultazione del sistema di posta elettronica aziendale dall'esterno dell'azienda;
- limitazioni dell'uso e della tipologia degli allegati ai messaggi di posta, in particolare per quanto riguarda la ricezione /spedizione di file di tipo eseguibile;
- regole per l'iscrizione a *mailing list* degli utenti interni;
- regole per l'invio di risposte automatiche;
- modalità per una corretta gestione delle e-mail, attraverso prescrizioni quali ad esempio:
    - cancellare la posta ricevuta da mittenti sconosciuti;
    - cancellare le e-mail ricevute con oggetti /messaggi seducenti;

Mobile computing

Molteplici sono i dispositivi utilizzati per il *mobile computing*: personal computer portatili (*desktop*, *laptop*, ecc.), palmari (*workpads*, *personal digital assistant*, *palm pilots*, ecc.) e telefoni cellulari con funzioni multimediali.

Per l'utilizzo di dispositivi mobili, da parte di personale interno o esterno, è opportuno adottare una logica di sicurezza delle basi dati con requisiti di protezione elevati, dove sono negati tutti i privilegi non esplicitamente autorizzati.

Assume quindi particolare importanza, soprattutto con riguardo alla salvaguardia della rete interna, la redazione di appropriate *policy* che regolamentino le procedure e le modalità di accesso, il riconoscimento dell'utente e il tipo di utilizzo consentito di dati e informazioni.

Inoltre, nonostante si tratti di apparecchiature di norma mantenute sotto il controllo diretto dell'assegnatario, per la salvaguardia dei dati in esse contenuti è raccomandabile l'utilizzo, ove possibile, di strumenti di controllo degli accessi che garantiscano alti livelli di sicurezza, nonché specifiche modalità di protezione dei dati, al fine di evitare che l'eventuale furto di un *mobile computer* infici la sicurezza aziendale.

Per la connessione dall'esterno alla rete aziendale è opportuno adottare:

- sistemi di autenticazione forte dell'utente (es. *token* o *smart card*) e di autorizzazione all'accesso sulle risorse, di tipo RADIUS (Remote Dial-in User Service, protocollo sviluppato per i servizi di autenticazione e di gestione degli *account* su *server* di accesso alla rete), Terminal Access Controller Control System (protocollo di autenticazione, autorizzazione e gestione degli *account* largamente utilizzato per le connessioni telefoniche dirette), KERBEROS (protocollo di autenticazione a chiave segreta), ecc.;

- tecniche di restrizione dell'accesso quali RPN (Remote Private Network), VPN (Virtual Private Network), CUG (Closed User Group), *call-back*, ecc.;
- sistemi di protezione e di anti-intrusione (quali *firewall*, *proxy*, traslazione degli indirizzi privati, ecc.);
- sistemi di autenticazione dei nodi;
- sistemi di *logging* per la verifica degli accessi, degli eventi e delle violazioni;
- crittografia dei dati critici archiviati e trasmessi.

Anche nel caso in cui i dispositivi si connettano alla rete aziendale dall'interno, devono essere adottati, oltre ai consueti sistemi di autenticazione dell'utente, *logging* e crittografia dei dati critici, anche tecniche di restrizione dell'accesso quali VLAN (Virtual Local Area Network), identificazione dei MAC Address (Medium Access Control Address), ecc.
Si sottolinea comunque che tale tipologia di connessione deve essere attuata con estrema prudenza, soprattutto nel caso in cui gli apparati non siano configurati preventivamente dall'azienda che ne mantiene il controllo (es. personal computer di personale esterno).
Per le particolari caratteristiche di tali dispositivi, dotati di modem interno o aventi la possibilità di comunicazione con apparecchi di telefonia mobile, risulta facilitata la possibilità di connessione a sistemi e reti esterne all'azienda, incluso Internet.
Nel caso in cui tali apparecchiature siano utilizzate per la connessione a Internet, e quindi soggette al rischio di infezioni virali e di acquisizione inconsapevoli di *malicious code*, è opportuno che siano dotate di *personal firewall* opportunamente configurati e che siano in grado di effettuare l'aggiornamento automatico delle impronte dell'antivirus a ogni connessione a Internet. È inoltre buona norma prevedere che, prima di ogni accesso a Internet effettuato al di fuori di una infrastruttura di protezione aziendale, la stazione di lavoro venga disconnessa dalla rete interna.
Un fattore di rischio nell'utilizzo di dispositivi mobili risiede anche nell'architettura di tipo *client/server* delle relative applicazioni18: al riguardo è raccomandato l'utilizzo di protocolli di comunicazione sicuri (es. protocollo SSL3, VPN, ecc.) tra le componenti applicative *client* e *server*.

5. Nuove modalità di attacco informatico e relative contromisure

Di seguito si illustrano alcune delle nuove tipologie di attacco - finalizzate a ledere le attività e gli interessi economici dell'azienda - che vanno diffondendosi in connessione con lo sviluppo dell'offerta di nuovi servizi informatici e con l'utilizzo di tecnologie innovative.

Social engineering

Tra le forme di attacco sta assumendo sempre maggiore rilevanza nel contesto informatico la c.d. *social engineering*, che consiste in una particolare tecnica psicologica che sfrutta l'inesperienza e, nella maggior parte dei casi, la buona fede degli utenti per carpire informazioni utili a portare successivi attacchi tecnologici ai sistemi.

Al di là dell'accezione apparentemente positiva della denominazione, il *social engineering* è una delle tecniche di attacco potenzialmente più dannose per la vittima.

Questo attacco ha di solito lo scopo di acquisire informazioni al fine di compiere azioni non consentite dai sistemi di controllo (quali avere accesso a locali o a dati riservati di pertinenza dell'azienda della vittima).

L'attacco è di solito condotto mediante un'impersonificazione, ovvero una sostituzione di identità o, nelle forme più sofisticate, con una pseudo-impersonificazione. In sostanza il soggetto che attacca si presenta, ad esempio mediante contatto telefonico, alla vittima prescelta - che ha accesso a informazioni utili all'attaccante o che svolge attività di controllo – e adotta, con finalità diverse, i seguenti comportamenti o atteggiamenti:

- assertivi: l'attaccante si finge un'altra persona in possesso dell'autorità necessaria a poter derogare alle regole (impersonificazione) e porta il suo attacco usando come elemento di coercizione la minaccia implicita di danni che potrebbero derivare alla vittima o alla società se non viene soddisfatta la propria richiesta;
- empatici e spesso allusivi: l'attaccante induce la vittima ad attribuirgli un'identità o un'autorità che in realtà non è quella corretta (pseudo-impersonificazione);
- esplicitamente complici: l'attaccante induce la vittima a violare le regole di controllo nella convinzione che sia bene farlo (manipolazione);
- candidamente corruttivi: l'attaccante propone scambi tra quanto a lui interessa e benefici per la vittima.

Le prime tre modalità hanno in comune il fatto che l'attaccante costruisce situazioni nelle quali la vittima percepisce come lecita o conforme alle regole aziendali l'azione che è indotto a eseguire. Pertanto, questa tipologia di attacco ha buone probabilità di avere successo, considerata anche la frequente presenza di ulteriori circostanze favorevoli all'attaccante:

- scarsa conoscenza da parte della vittima delle responsabilità e dei ruoli aziendali, delle regole e delle prassi operative soprattutto in condizioni non ordinarie o di emergenza;
- scarsa preparazione della vittima in tema di gestione della comunicazione (in modo particolare delle fasi conflittuali e delle interviste);
- sottovalutazione da parte della vittima delle conseguenze delle violazioni.

Contromisure
La possibile difesa da questa tipologia di attacco consiste nell'adozione di sistemi di formalizzazione delle richieste secondo gli standard aziendali e di controllo dell'autenticità dell'interlocutore.
Considerato, inoltre, che gran parte dei danni è spesso causata dalla superficialità e da comportamenti non accorti all'interno dell'azienda, al fine di contenere i rischi di questo tipo di attacco può essere utile effettuare alcuni interventi, quali:

- stabilire norme volte a prevenire l'indebita pubblicizzazione, comunicazione o diffusione di dati e informazioni inerenti all'azienda, sia sul posto di lavoro, sia al di fuori dello stesso, anche in contesti non lavorativi;
- prevedere l'obbligo di segnalare qualsiasi contatto dall'esterno di natura sospetta;
- attuare un piano di formazione nei confronti di tutti i dipendenti e dei collaboratori esterni in merito a questo tipo di attacco, alle sue possibili conseguenze e alle relative contromisure;
- svolgere una specifica attività di formazione nei confronti della struttura di *helpdesk/customer–care*.

6. Tecniche varie per l'acquisizione di informazioni

Sono molteplici le tecniche utilizzate dall'attaccante per acquisire informazioni utili. Le più diffuse sono le seguenti:

sniffing
Consiste in una operazione di intercettazione passiva delle comunicazioni per la cattura di dati; l'attaccante può riuscire a intercettare informazioni e dati di varia natura (password, messaggi di posta elettronica, ecc.). Normalmente questa attività di intercettazione illecita viene effettuata con l'ausilio di strumenti informatici denominati *sniffer* – talora posizionati illecitamente su un sistema di proprietà di un utente inconsapevole – che catturano le informazioni in transito nel punto in cui sono stati installati: si tratta in sostanza di hardware o software - legali e reperibili normalmente in commercio - analizzatori, in grado di intercettare, selezionare per protocollo, tradurre, visualizzare e memorizzare tutti i tipi di pacchetti in transito sulla rete.

Contromisure
Riconoscere la presenza di tali tipologie di strumenti non è sempre facile. Un rilevamento specifico può essere effettuato mediante:

- il controllo locale dello stato dell'interfaccia di rete dei singoli sistemi o la verifica della presenza di schede di rete configurate in modalità promiscua;
- l'utilizzo di software specializzati;
- l'analisi delle segnalazioni delle eventuali "sonde" utilizzate. Per impedire un attacco della specie, si hanno a disposizione diverse possibilità:
- realizzazione di una topologia di rete sicura adottando tecniche di segmentazione;
- applicazione di funzioni crittografiche per rendere i dati intelligibili al solo legittimo destinatario;
- adozione di sistemi di autenticazione forte;
- preclusione della possibilità di configurare le interfacce di rete in modalità promiscua.

connection hijacking
È un metodo di attacco che riguarda principalmente le transazioni o, comunque, i flussi di dati che transitano da un computer all'altro. Con tale violazione l'intrusore, dopo averne analizzato il flusso, si inserisce materialmente nella transazione alterandone il contenuto e riuscendo a operare con le credenziali di chi legittimamente ha iniziato la sessione.

Contromisure
Si basano generalmente sull'adozione di tecniche crittografiche, utilizzate sia per gestire la cifratura delle informazioni in transito, sia per l'autenticazione dei poli terminali della transazione.

network scanning
È il tentativo di rilevare indirizzi IP o porte TCP al fine di individuare quali servizi o sistemi siano presenti e attivi, per poter successivamente procedere a un tentativo di intrusione.

Contromisure
Adottare *firewall* di rete, *personal firewall* sulle stazioni di lavoro e strumenti di *intrusion detection* che consentano l'attivazione delle forme di reazione più appropriate.

Spoofing
Lo *spoofing* non rappresenta un attacco nel senso stretto del termine, ma piuttosto una tecnica complementare a vari tipi di attacco. Consiste nel falsificare l'origine della connessione in modo tale da far credere di essere un soggetto/sistema diverso da quello reale.
Le principali tipologie di *spoofing* sono:

- **User account spoofing**: consiste nell'utilizzo della userid e della password di un altro utente senza averne il diritto. Può essere attuato sfruttando comportamenti non corretti degli utenti o utilizzando strumenti quali *sniffing* e *password crackers*.
- **DNS spoofing**: è il sostituirsi a un *server* DNS21 lecito nei confronti di un *client* che ha effettuato una richiesta a un *Name Server*.
- **IP Address spoofing**: è l'attacco più diffuso. Si basa sul fatto che la maggior parte dei *routers* all'interno di una rete utilizzano solo l'indirizzo IP di destinazione e non quello di origine.

Questo fa sì che un attaccante possa inviare dei pacchetti a un sistema bersaglio utilizzando *source* IP fittizi in maniera che le risposte siano inviate al falso IP indicato dall'attaccante.

Contromisure
La principale contromisura è costituita dall'utilizzo di tecniche crittografiche finalizzate all'autenticazione forte dei soggetti/sistemi coinvolti.
L'IP Address *spoofing* può essere limitato inserendo dei filtri sull'indirizzo IP sorgente a livello di *routers* e *firewall*.

Sfruttamento di servizi non autenticati
L'acquisizione indebita di informazioni o l'attacco di tipo *spoofing* possono essere più agevolmente condotti nei confronti di servizi di rete che non utilizzano tecniche di autenticazione, quali ad esempio:

- **TFTP** (*Trivial Files Transfer Protocol*): è un protocollo che si basa solo sulla gestione degli accessi a livello del *file-system* e può essere sfruttato per acquisire *file* sensibili del sistema;
- **SMTP** (*Simple Mail Transfer Protocol*): si tratta di un diffuso protocollo che non effettua i controlli sulla vera identità degli utenti; pertanto i servizi che si basano su di esso sono soggetti più di altri ad attacchi di tipo *spoofing*;
- **DNS** (*Domain Name Server*): è il sistema che, nel caso sia oggetto di attacco di tipo *spoofing*, può fornire agli utenti richiedenti indirizzi errati.

Contromisure
La migliore contromisura consiste nel disabilitare i servizi che non vengono utilizzati o limitarne l'accesso a soggetti identificati e autenticati. Per quanto riguarda in particolare l'SMTP è raccomandabile l'utilizzo di funzioni crittografiche oltre a quelle di autenticazione.

Malicious code
Questo termine, che ha come sinonimi "*malware"* e "*MMC (Malicious Mobile Code*)", si riferisce a quella famiglia di software che ha come obiettivo il danneggiamento, totale o parziale, o l'alterazione del funzionamento di un sistema informatico/telematico.
Alcune forme di codice malevolo, quali virus, *worm*, *trojan horse*, *mass mailing* e *mixed mmc*, sono in grado di autoinstallarsi, di autoriprodursi, di diffondersi, di determinare alterazioni del corretto funzionamento del sistema e anche di esportare i dati o di prendere il controllo del sistema stesso, spesso sfruttando vulnerabilità presenti nei software di sistema e/o applicativi.

Contromisure
Si richiamano di seguito le principali cautele da adottare per contrastare eventuali infezioni da *malicious code*:

- utilizzare solo software "certificato";
- assegnare al software solo i privilegi minimi necessari;
- innalzare e mantenere elevato il livello di sicurezza delle stazioni di lavoro;
- aggiornare tempestivamente i software anti-virus;
- applicare tempestivamente al software le correzioni (*patch*) rilasciate dai produttori;
- utilizzare specifici software antivirus in grado di rilevare i *malicious code* analizzando i flussi informativi in transito o sui sistemi;
- sensibilizzare tutto il personale con riferimento ai rischi inerenti all'introduzione di software estraneo sulle postazioni di lavoro.

Denial of Service (DoS)
È una tipologia di attacco che ha come obiettivo la riduzione o l'annullamento della capacità di utilizzo di una risorsa e agisce attraverso la produzione di un sovraccarico dell'impegno della risorsa stessa; tale attacco si può realizzare, ad esempio, attraverso l'invio di un flusso massiccio di dati verso uno o più sistemi con l'obiettivo finale di mandarli in *crash* o di rendere talmente lenti i tempi di risposta da bloccare di fatto qualsiasi operazione. Gli attacchi diretti a un determinato sistema possono essere attivati localmente oppure tramite rete da sistemi esterni. Inoltre, si possono distinguere due tipologie di DoS:

- **esaurimento di banda:** la tecnica consiste nel sovraccaricare la rete bersaglio in modo da consumarne tutta l'ampiezza di banda;
- **esaurimento delle risorse elaborative:** consiste nel colpire direttamente un sistema, attraverso un consumo straordinario delle risorse della macchina (cicli CPU, memoria).

Va rilevato come sono oggi disponibili software particolarmente aggressivi in grado di automatizzare i processi di attacco, con la conseguenza che anche un dilettante può portare un attacco DoS anche senza capirne il funzionamento o rendersi conto di cosa stia esattamente facendo.

Contromisure
Oltre alle contromisure già indicate, si possono indicare le seguenti:

- adozione di sistemi di monitoraggio sull'utilizzo delle risorse per rilevare prontamente gli scostamenti da valori medi;
- adozione di sistemi di *intrusion detection*;
- utilizzo di *proxy* e *firewall* a protezione delle connessioni con l'esterno.

Defacement
Il *defacement* di un sito web è un tipo di attacco che consiste nella modifica della *home page* mediante la sostituzione delle immagini e/o dei testi originali. Attraverso questa tecnica si possono perseguire due diversi obiettivi: danneggiare l'immagine di un determinato sito web; trarre in inganno il navigatore facendogli trovare su un sito web informazioni diverse da quelle ricercate.

Contromisure
La prevenzione di tale forma di intrusione può essere realizzata adottando le contromisure già previste per il *Denial of Service*.

Gestione degli incidenti di sicurezza
Oltre all'attivazione delle specifiche contromisure preventive appena descritte, l'azienda deve dotarsi di un adeguato apparato di reazione, pronto a intervenire secondo schemi predefiniti che contemplino in modo dettagliato la tipologia dei possibili incidenti, le conseguenti azioni da intraprendere e le funzioni aziendali che devono essere coinvolte.

È necessario innanzi tutto costituire un *Incident Response Team* (IRT), composto da elementi puntualmente individuati in grado di intervenire all'occorrenza, ben addestrati e agevolmente reperibili anche al di fuori dell'orario di lavoro. Tali elementi devono possedere, tra le proprie caratteristiche personali, anche la capacità di operare con efficacia in condizioni difficili, in un clima di stretta collaborazione con gli altri soggetti coinvolti. Particolare attenzione deve essere riservata all'individuazione della figura del coordinatore dell'IRT, che assume la responsabilità della conduzione del lavoro e che è tenuto a curare anche il *reporting* finale dell'incidente.
La gestione degli incidenti di sicurezza va comunque attuata secondo un piano di azione che deve essere preventivamente formalizzato, adeguatamente testato e manutenuto. Tale piano deve prevedere almeno le seguenti fasi:

- rilevazione dell'incidente, utilizzando idonei strumenti, tecnici e organizzativi; è importante che in questa fase siano considerati incidenti anche quegli avvenimenti che potrebbero poi non rivelarsi tali; è infatti preferibile gestire un falso allarme che ignorare un reale incidente;
- attivazione della figura individuata come responsabile dell'IRT;
- accertamento della natura e dell'entità dell'incidente e coinvolgimento dei diversi comparti aziendali interessati e degli opportuni livelli decisionali e, laddove sussistano gli estremi di un possibile reato, segnalazione alle Autorità competenti, in particolare al Servizio di Polizia Postale e delle Comunicazioni ;
- documentazione dei dettagli dell'evento, attivazione delle misure di contrasto e ripristino delle condizioni di funzionamento normale ovvero degradato, prospettando in quest'ultimo caso tempi e modi per il completo ripristino;
- dichiarazione della fine dell'emergenza e redazione del rapporto finale.

Al termine del processo, è opportuno verificare l'eventuale necessità di effettuare interventi organizzativi e tecnologici in modo da ridurre la possibilità che l'incidente si ripeta.

7. Livelli di sicurezza

L'obiettivo di un responsabile della sicurezza è proteggere le informazioni gestite dal sistema informatico, rendendole accessibili solo ed esclusivamente da un gruppo definito e limitato di utenti.
Scomponendo il sistema informatico aziendale in un albero funzionale possiamo individuare tre livelli di vulnerabilità:

1. **Livello di rete**, i server DNS costituiscono uno dei bersagli preferiti degli attacchi, esistono in rete numerosi tools anche open source come port-scanner che permettono di rilevare le vulnerabilità note.
2. **Livello di sistema operativo**, l'attacco a questo livello segue una dinamica be definita:
    1. Accesso al sistema attraverso l'esecuzione di exploit[(1)], la cattura o l'intercettazione del file delle password, gli attacchi a forza bruta.
    2. Scalata dei privilegi e/o impersonificazione degli utenti con previlegi amministrativi attraverso il crack delle password e/o l'esecuzione di exploit successivi;
    3. Occultamento delle tracce attraverso la cancellazione dei logs, l'uso di rootkits[(2)] e lo sfruttamento di particolari caratteristiche del sistema operativo;
    4. Installazione di backdoors, programmi nascosti che aprono all'aggressione delle porte senza restrizioni con la possibilità di controllare il sistema in qualsiasi momento.

    Il sistema operativo può avere un miglioramento significativo nella predisposizione e nel mantenimento dei giusti livelli di sicurezza se:
    1. Assenza di vulnerabilità note nei confronti di tipologie conosciute di attacco;
    2. Capacità di limitare determinati tipi di attività soltanto ad alcuni utenti;
    3. Abilità nel rimuovere e disabilitare servizi e risorse non necessari;
    4. Abilità nel controllare l'uso e l'accesso alle risorse e nel registrare le attività degli utenti;

- **Livello applicativo,** rappresenta il livello più alto del sistema, composto da tutti quei software utilizzati durante le proprie attività produttive. Una volta messi in sicurezza i livelli più bassi del sistema è necessaria un'analisi dei rischi effettivi di questo livello.

Possiamo quindi affermare *che non è possibile applicare una politica di sicurezza generale* ma siamo costretti a progettare ed implementare un checkpoint ad-hoc per ogni livello del sistema informatico.

[(1)]Un exploit è un termine usato in informatica per identificare un codice che, sfruttando un bug o una vulnerabilità, porta all'acquisizione di privilegi (wikipedia)
[(2)]In informatica un rootkit, letteralmente equipaggiamento da amministratore (in ambiente Unix per "root" access si intende accesso di livello amministrativo), è un programma software prodotto per avere il controllo sul sistema senza bisogno di autorizzazione da parte di un utente o di un amministratore.

8. Vulnerability assessment e penetration test

Vulnerability assessment e penetration test hanno come obiettivo di fornire una conoscenza dettagliata sullo stato di sicurezza di sistemi informatici presi in esame.
Si differenziano tra loro sia per i risultati che permettono di raggiungere quanto per le risorse necessarie alla loro conduzione.
L'attività di vulnerability assessment (VA) permette di avere una fotografia dettagliata dello stato di esposizione dei propri sistemi a tutte le vulnerabilità note. A questo scopo vengono utilizzati alcuni tool automatici i quali, effettuando una lunga serie di controlli su ogni singolo sistema, servizio o applicazione, permettono di conoscere dettagli riguardanti la loro configurazione e l'eventuale presenza di vulnerabilità.
Il penetration test (PT) è un test con il quale è possibile testare la sicurezza di un sistema informatico attaccandolo attivamente alla ricerca di falle di sicurezza. Durante un penetration test vengono simulate delle intrusioni, ipotizzando diversi scenari di attacco e combinando tecniche manuali all'utilizzo degli strumenti automatici. In questo modo è possibile analizzare non solo l'esposizione a vulnerabilità non verificabili dai software automatici.
Il motivo principale della loro diffusione sta nel fatto che, oggigiorno, i costi derivanti da un "incidente informatico" possono essere elevati, sia da un punto di vista economico che a livello d'immagine. La perdita di dati confidenziali comporta, oltre alle perdite per costi diretti, danni derivanti dalla perdita di fiducia da parte di consumatori ed investitori; può inoltre comportare conseguenze legali e sanzioni da parte delle autorità, qualora sussistano inadempienze alle norme in materia di sicurezza di dati informatizzati. E' facile dunque capire perché con il passare degli anni sempre maggiori risorse vengano impiegate in materia di Sicurezza.
L'Open Source Security Testing Methodology Manual (OSSTMM) [http://www.isecom.org/osstmm/], 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.
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(metriche per misurare la superficie di attacco) e l'emissione di reportistica STAR (reportistica 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.

Quando la verifica comprende applicazioni pubblicate via WEB esiste 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.
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.

Di seguito elenchiamo alcune di queste classi:

- 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. Sicur control system roadmap

La verifica per la gestione del rischio informatico prevede le seguenti fasi:

Fasi dell'attività

1. **Audit:** identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità, ovvero le carenze di protezione relativamente a una determinata minaccia.
2. **Verifica:** individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse
3. **Report:** individuazione dei danni che possono derivare dal concretizzarsi delle minacce
4. **Correzione:** identificazione delle possibili contromisure e analisi costi/benefici degli investimenti per l'adozione delle contromisure
5. **Prevenzione:** definizione di un piano di azioni preventive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare
6. **Monitoraggio:** dello stato del sistema nel tempo

10.Valutazione del Rischio nell'ICAR-CNR

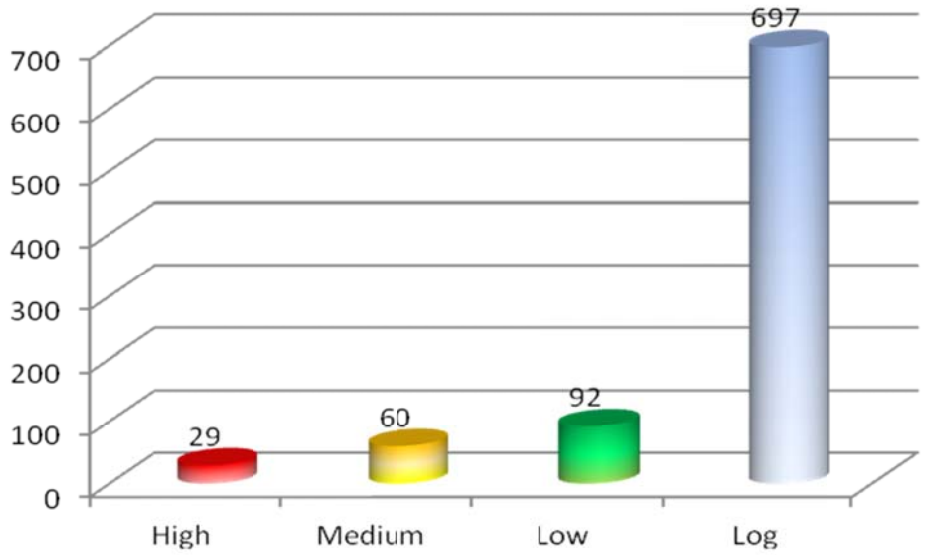
L'esecuzione dell'attività di Vulnerability Assessment sulla network dell'ICAR-CNR ha prodotto una serie di risultati sui quali si è basata la successiva attività di valutazione del rischio. La "***matrice di valutazione***" rappresenta graficamente la mappatura di valutazione.

I risultati ottenuti con gli strumenti automatici di analisi hanno spesso bisogno di essere convalidati per isolare i falsi positivi, la verifica può essere 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.

Le vulnerabilità individuate verranno mappate all'interno della "*matrice di tracciabilità"*, con lo scopo di monitorarne l'evoluzione ed e la loro mitigazione.

E' necessario anche definire una metodologia standardizzata che permetta di effettuare dei test il più possibilmente ripetibili quindi misurabili, in modo da poter confrontare i risultati ottenuti.

Il grafico successivo definisce, in modo complessivo l'assessment aziendale, è importante notare anche se il numero delle vulnerabilità alte rappresentano una piccola percentuale di quelle complessive, esse afferiscono a host con priorità alta pertanto necessitano di una mitigazione in tempi brevi.



Di seguito l'overview dell'assessment effettuato sui sistemi di ICAR (gli indirizzi IP sono stati oscurati per motivi di privacy) :

HOST	Most Severe Result	High	Medium	Low	Log	False Positives
a.b.c.1	L	0	0	0	15	0
a.b.c.2	H	3	2	2	18	0
a.b.c.3	M	0	1	4	24	0
a.b.c.4	H	4	5	15	64	0
a.b.c.5	H	1	7	12	67	0
a.b.c.6	H	4	5	6	32	0
a.b.c.7	M	0	2	1	41	0
a.b.c.8	M	0	3	5	49	0
a.b.c.13	M	0	2	2	25	0
a.b.c.17	L	0	0	1	14	0
a.b.c.25	L	0	0	2	25	0
a.b.c.26	M	0	1	1	25	0
a.b.c.58	H	2	2	10	50	0
a.b.c.60	H	3	9	10	53	0
a.b.c.109	M	0	1	4	32	0
a.b.c.161	H	11	12	6	54	0
a.b.c.180	H	1	1	9	26	0
a.b.c.205	M	0	1	1	26	0
a.b.c.209	M	0	5	0	23	0
a.b.c.254	M	0	1	1	34	0
Total:	**20**	**29**	**60**	**92**	**697**	**0**

Dalla tabella dell'overview è possibile definisce in modo analitico una misura valutativa delle vulnerabilità riscontrate, in particolare per ogni host analizzato vengono definiti una serie di indicatori:

HOST	∑p Vulnerability	% Priority	#Port	Result	Note
a.b.c.1	0,0	100%	7	0	
a.b.c.2	8,5	100%	15	128	
a.b.c.3	2,0	100%	13	26	
a.b.c.4	16,8	80%	45	603	
a.b.c.5	12,0	100%	34	408	
a.b.c.6	14,5	100%	16	232	
a.b.c.7	2,3	90%	16	32	
a.b.c.8	4,3	90%	19	73	
a.b.c.13	2,5	100%	18	45	
a.b.c.17	0,3	70%	8	1	
a.b.c.25	0,5	70%	9	3	
a.b.c.26	1,3	100%	11	14	
a.b.c.58	8,5	70%	27	161	
a.b.c.60	17,5	90%	28	441	
a.b.c.109	2,0	50%	12	12	
a.b.c.161	35,5	80%	30	852	
a.b.c.180	5,3	80%	12	50	
a.b.c.205	1,3	80%	10	10	
a.b.c.209	5,0	80%	11	44	
a.b.c.254	1,3	70%	11	10	

Ogni indicatore è stato calcolato analiticamente nel seguente modo:

Indicatore	Metrica adottata	Descrizione
∑p Vulnerability	∑H*2+∑M+∑L/5-∑FP	Sommatoria delle vulnerabilità pesate
% Priority	%	Priorità assegnata ad ogni host
#Port	∑Porte	Numero di porte potenzialmente vulnerabili
Result	π(∑p Vulnerability,% Priority,#Port)	Valutazione finale pesato

dove
H = Vulnerabilità di livello alto
M = Vulnerabilità di livello medio
L = Vulnerabilità di livello basso
FP = Falsi positivi

E’ possibile quindi estrarre la seguente tabella di valutazione::

Host	Assessment
a.b.c.1	0
a.b.c.2	128
a.b.c.3	26
a.b.c.4	603
a.b.c.5	408
a.b.c.6	232
a.b.c.7	32
a.b.c.8	73
a.b.c.13	45
a.b.c.17	1
a.b.c.25	3
a.b.c.26	14
a.b.c.58	161
a.b.c.60	441
a.b.c.109	12
a.b.c.161	852
a.b.c.180	50
a.b.c.205	10
a.b.c.209	44
a.b.c.254	10

Priority	Value
Low	0-50
Medium	51-200
High	201-500
Critical	>500

Tab. 1 – Tabella di valutazione

Dalla Tab. 1 si evince in modo chiaro, la necessità di un’attività di mitigazione sugli host a.b.c.4, a.b.c.5, a.b.c.6, a.b.c.160 e in particolare sull’host a.b.c.161.
E’ da sottolineare anche che questi risultati non tengono conto di eventuali falsi positivi (non ancora individuati), che potrebbero modificare la valutazione del rischio degli host in esame, e dal coefficiente “%Priority” che definisce l’importanza del bene all’interno dell’istituto.

Matrice di tracciabilità

HOST	Data Verifica	Tipologia Vulnerabilità	Gravità	Falso Positivo	Data Mitigazione	Mitigazione Adottata	Responsabile	Verificata	Report
a.b.c.2	05/03/2014	NTP mode 7 MODE PRIVATE Packet Remote Denial of Service Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.2	05/03/2014	NTP 'ntpd' Autokey Stack Overow Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.2	05/03/2014	NTP Stack Buffer Overow Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.2	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.2	05/03/2014	openssh-server Forced Command Handling Information Disclosure Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.3	05/03/2014	TCP timestamps	M	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	http TRACE XSS attack	H	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	H	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	Microsoft RDP Server Private Key Information Disclosure Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	DCE Services Enumeration	M	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	LDAP allows null bases	M	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	Use LDAP search request to retrieve information from NT Directory Services	M	Verificare					report-LanIcar.pdf
a.b.c.4	05/03/2014	openssh-server Forced Command Handling Information Disclosure Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	http TRACE XSS attack	H	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	Squid HTCP Packets Processing Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf

a.b.c.5	05/03/2014	Squid Header-Only Packets Remote Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	Check for SSL Weak Ciphers	M	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	Check if Mailserver answer to VRFY and EXPN requests	M	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	openssh-server Forced Command Handling Information Disclosure Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.5	05/03/2014	Check if Mailserver answer to VRFY and EXPN requests	M	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	PHP version smaller than 5.3.3	H	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	Joomla! Prior to 1.6.1 Multiple Security Vulnerabilities	H	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	PHP version 5.3< 5.3.6	H	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	PHP version smaller than 5.3.4	H	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	Joomla! Multiple Cross-site Scripting Vulnerabilities	M	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	TCP timestamps	M	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	Samba Multiple Remote Denial of Service Vulnerabilities	M	Verificare					report-LanIcar.pdf
a.b.c.6	05/03/2014	openssh-server Forced Command Handling Information Disclosure Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.7	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.7	05/03/2014	Check for SSL Weak Ciphers	M	Verificare					report-LanIcar.pdf
a.b.c.8	05/03/2014	Check for SSL Weak Ciphers	M	Verificare					report-LanIcar.pdf
a.b.c.13	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service	M	Verificare					report-LanIcar.pdf

		Vulnerability							
a.b.c.13	05/03/2014	TCP timestamps	M	Verificare					report-LanIcar.pdf
a.b.c.26	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.58	05/03/2014	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	H	Verificare					report-LanIcar.pdf
a.b.c.58	05/03/2014	Microsoft RDP Server Private Key Information Disclosure Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.58	05/03/2014	Fingerprint web server with favicon.ico	M	Verificare					report-LanIcar.pdf
a.b.c.58	05/03/2014	SSL Certificate Expiry	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	http TRACE XSS attack	H	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Microsoft RDP Server Private Key Information Disclosure Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Apache Tomcat Session Fixation Vulnerability (Windows)	H	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Apache Tomcat HTTP NIO Denial Of Service Vulnerability (Windows)	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Apache Tomcat Denial Of Service Vulnerability (Windows)	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Check for SSL Weak Ciphers	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	DCE Services Enumeration	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	TCP timestamps	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	LDAP allows null bases	M	Verificare					report-LanIcar.pdf
a.b.c.60	05/03/2014	Use LDAP search request to retrieve information from NT Directory Services	M	Verificare					report-LanIcar.pdf
a.b.c.109	05/03/2014	Check for SSL Weak Ciphers	M	Verificare					report-LanIcar.pdf

a.b.c.161	05/03/2014	JBoss Enterprise Application Platform Multiple Remote Vulnerabilities	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat Windows Installer Privilege Escalation Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat 'Transfer-Encoding' Information Disclosure and Denial Of Service Vulnerabilities	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat Multiple Vulnerabilities January 2010	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL 5.x Unspecifed Buffer Overow Vulnerability	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL 'sql parse.cc' Multiple Format String Vulnerabilities	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL Denial Of Service and Spofing Vulnerabilities	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL Multiple Vulnerabilities	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL Authenticated Access Restrictions Bypass Vulnerability (Linux)	H	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	JBoss Enterprise Application Platform Multiple Vulnerabilities	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat Multiple Vulnerabilities June-09	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat Multiple Security Bypass Vulnerabilities (Windows)	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat cal2.jsp Cross Site Scripting Vulnerability	M	Verificare					report-LanIcar.pdf

a.b.c.161	05/03/2014	Apache Tomcat Authentication Header Realm Name Information Disclosure Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Apache Tomcat Security bypass vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL multiple Vulnerabilities	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL MyISAM Table Privileges Secuity Bypass Vulnerability	M	Verificare					report-LanIcar.pdf
a.b.c.161	05/03/2014	Oracle MySQL 'TEMPORARY InnoDB' Tables Denial Of Service Vulnerability	M						report-LanIcar.pdf
a.b.c.161	05/03/2014	Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities	M						report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL Empty Bit-String Literal Denial of Service Vulnerability	M						report-LanIcar.pdf
a.b.c.161	05/03/2014	MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability	M						report-LanIcar.pdf
a.b.c.180	05/03/2014	Microsoft RDP Server Private Key Information Disclosure Vulnerability	H						report-LanIcar.pdf
a.b.c.180	05/03/2014	Check for SSL Weak Ciphers	M						report-LanIcar.pdf
a.b.c.205	05/03/2014	Check for SSL Weak Ciphers	M						report-LanIcar.pdf
a.b.c.209	05/03/2014	TCP Sequence Number Approximation Reset Denial of Service Vulnerability	M						report-LanIcar.pdf
a.b.c.209	05/03/2014	TCP timestamps	M						report-LanIcar.pdf
a.b.c.209	05/03/2014	Check for SSL Weak Ciphers	M						report-LanIcar.pdf
a.b.c.209	05/03/2014	Check for SSL Weak Ciphers	M						report-LanIcar.pdf
a.b.c.209	05/03/2014	penssh-server Forced Command Handling Information Disclosure Vulnerability	M						report-LanIcar.pdf
a.b.c.254	05/03/2014	Check for SSL Weak Ciphers	M						report-LanIcar.pdf

La matrice di permette di abbattere il rischio di attacchi o perdite di dati è l'obiettivo principale di qualsiasi ICT manager, pertanto la matrice deve far parte in modo integrante dei documenti di policy aziendale, assegnargli un responsabile e pianificandone delle verifiche periodiche.

11.Correzioni apportate dall'area IT dell'ICAR-CNR

A seguito dell'analisi di rischio sottopostaci, ove possibile sono state applicate tutte le patchfix richieste,

- provvedendo al patch manuale nel caso di sistemi in cui erano presenti misconfigurazioni
- sostituendo o aggiornando le versioni con vulnerabilità dei servizi preinstallati
- isolando in una LAN apposita i servizi di cui per motivi di compatibilità con software di terze parti non era possibile fare l'upgrade
- eliminando i server con servizi obsoleti che non erano più di utilità (previo backup immagine del sistema)

Tutte le macchine che presentano vulnerabilità sono isolate comunque via FIREWALL per non fornire accessi dall'esterno.
Oltre ciò esistono due firewall che consentono la rapida ripresa del servizio di connessione/protezione di rete in caso di malfunzionamenti hardware.
Dopo questi step, la situazione aggiornata dei report di penetration testing è disponibile nei report sotto indicati disponibili nell'archivio di istituto.

- *report-027ac2cd-8e2c-42ff-9011-f752eae759db.pdf* del 22 gennaio 2015
- *report-37318111-0ae0-4381-b6c6-b8bb6e770a88.pdf* del 22 gennaio 2015
-*LanIcar.pdf* del 5 marzo 2014

NOTA: L'attività di aggiornamento all'epoca del pentest era già iniziata, prova ne sia che i firewall, le prime due macchine aggiornate, risultano essere con zero vulnerabilità almeno di livello medio/alto, inoltre è stato installato un servizio DNS master/slave precedentemente non esistente.

Priority	Value
Low	0-50
Medium	51-200
High	201-500
Critical	>500

Host	Assessment
a.b.c.1	0
a.b.c.2	128
a.b.c.3	26
a.b.c.4	603
a.b.c.5	408
a.b.c.6	232
a.b.c.7	32
a.b.c.8	73
a.b.c.13	45
a.b.c.17	1
a.b.c.25	3
a.b.c.26	14
a.b.c.58	161
a.b.c.60	441
a.b.c.109	12
a.b.c.161	852
a.b.c.180	50
a.b.c.205	10
a.b.c.209	44
a.b.c.254	10

(1)

Host	Assessment
a.b.c.1	0
a.b.c.2	1 (SOSTITUITO)
a.b.c.3	26
a.b.c.4	603 (isolato in LAN)
a.b.c.5	7 (In sostituzione con nuovo server mail)
a.b.c.6	232 (In sostituzione col 23)
a.b.c.7	32
a.b.c.8	3 (INSOLATO IN LAN)
a.b.c.9	1 (NUOVO SETUP)
a.b.c.13	45
a.b.c.17	0
a.b.c.23	1
a.b.c.25	3
a.b.c.26	14
a.b.c.58	161 (DISMESSO)
~~a.b.c.60~~	~~441 (DISMESSO)~~
a.b.c.109	10
~~a.b.c.161~~	~~852 (DISMESSO)~~
a.b.c.180	50 (IN DISMISSIONE)
a.b.c.205	10
a.b.c.209	32
a.b.c.254	10

(2)

Tab. 2 – Tabelle di valutazione. La tabella (2) mostra le correzioni apportate dal reparto IT per ovviare alle problematiche emerse dai test e riportate in (1).

Grafico riassuntivo delle correzioni apportate.