

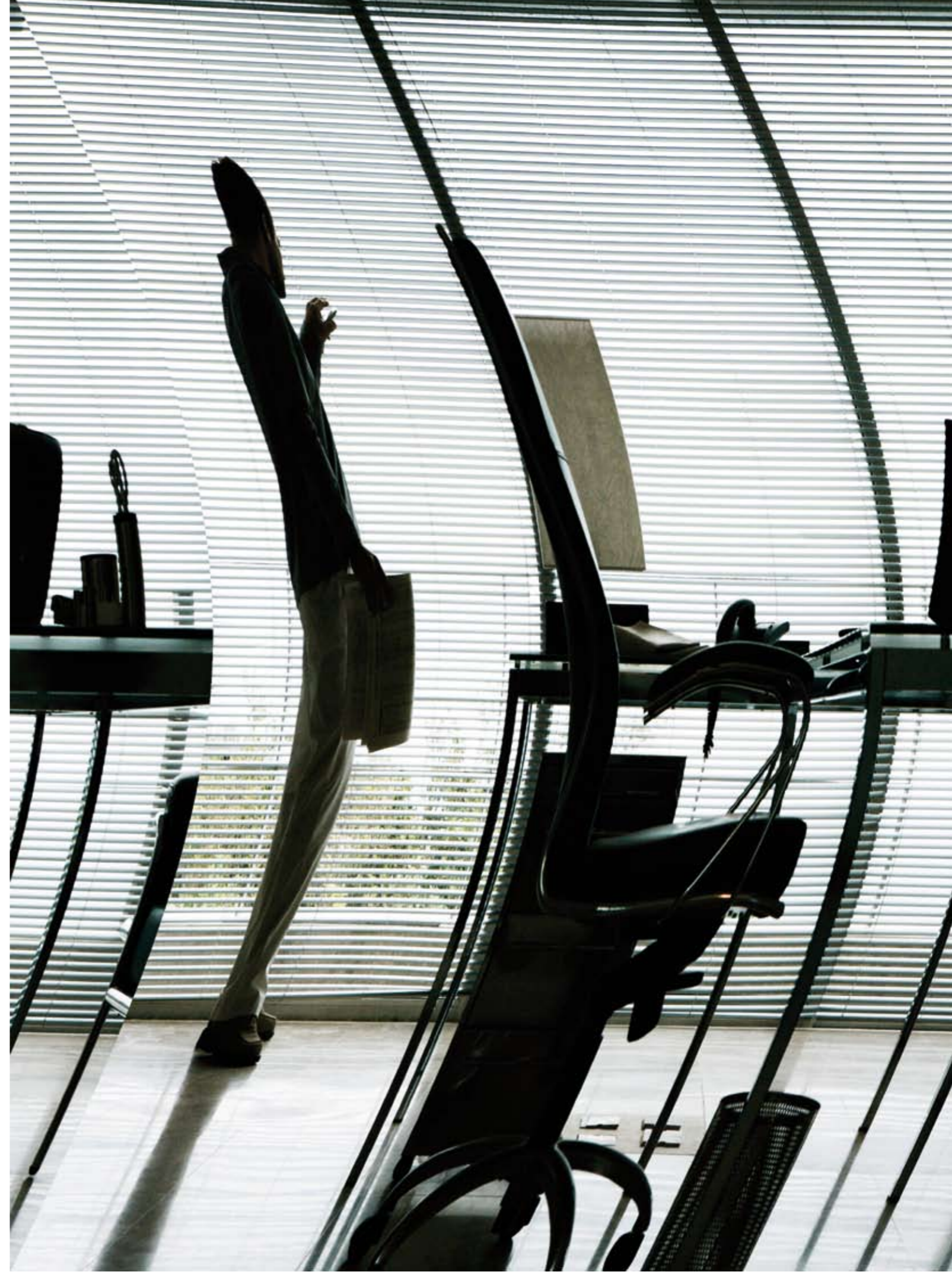
# Il security audit

Quanto contano efficacia e sicurezza dei sistemi informativi per il successo di un'azienda?

Qualunque sia la risposta, l'audit periodico di sicurezza è uno degli strumenti a disposizione del management per localizzare i sistemi più esposti ai pericoli e adottare le contromisure più efficaci per garantire continuità al business

di Giuseppe Badalucco

**B**isogna cominciare col piede giusto. Definire con precisione l'obiettivo dell'audit di sicurezza, stabilire cioè quali informazioni dovrà produrre l'attività di analisi e disporre di policy di sicurezza chiare è già un buon punto di partenza sia per l'azienda sia per l'auditor. Per esempio si potrebbe sottoporre a verifica l'adeguatezza delle policy a fronte delle reali esigenze dell'azienda; oppure fissarsi come obiettivo basilare, ma non per questo meno importante, quello di verificare la corretta applicazione delle policy esistenti. E i risultati potrebbero anche essere distonici rispetto alle aspettative. Tuttavia l'analisi sarebbe perfettamente legittima, gli obiettivi calibrati e coerenti e, allo stesso tempo, correttamente posizionati a debita distanza da quell'enfasi (velleitarismo?) che talvolta permea certi obiettivi assegnati all'audit di sicurezza. Senza dubbio questo servizio rappresenta il primo passo da compiere sulla strada della pro-



tezione globale della rete da attacchi e/o tentativi di intrusione non autorizzati; esso raffigura quella sorta di esame di maturità per l'azienda che vuole mettere alla prova la sicurezza dei propri sistemi e la maturità di collaboratori e partner. Ma non dovrebbe trasformarsi, come qualche volta si tende a

rappresentare, in un evento straordinario gravido di aspettative esorbitanti. L'azienda dovrà arrivarci per gradi, siamo d'accordo, ma alcuni passi in questa direzione dovrebbero essere stati fatti in precedenza, saranno stati fatti in precedenza; non dimentichiamo che tutte le organizzazioni qualunque sia il loro grado di consapevolezza dispongono di un sistema di gestione che, con maggiore o minore competenza, si oppone alle criticità insite nei propri processi operativi. Altri invece descrivono l'audit di sicurezza come l'appendice del più ampio processo di risk management, termine oggi alquanto abusato e spesso agitato come una clava per minacciare le aziende che ancora non si sono attrezzate per pianificarne il varo e alle quali è negato per definizione l'accesso al nirvana della gestione aziendale perfetta. Rimaniamo con i piedi per terra e diamo per assodato che siano verificati e dimostrabili gli assunti di partenza e che l'azienda disponga di uno storico (baseline), vale a dire di dati sufficienti per permettere di valutare l'efficacia delle contromisure implementate nel corso del tempo e di valutare i trend evolutivi nel contrasto delle minacce, e che il security audit sarà parte di un più ampio processo già pianificato e verificato e non un diletteantistico e disarticolato tentativo di scimmiettare il comportamento di aziende famose; soddisfatte queste condizioni l'audit di sicurezza può acquistare un enorme valore per l'azienda.



**Ombretta Comi**  
marketing manager  
di McAfee Italia



**Alberto Prandini**  
regional director Italy,  
Greece and Cyprus  
di Radware



**Antonio Forzieri**  
principal consultant  
Symantec Professional  
Services

## L'audit parte da una mappatura delle risorse da verificare, con la valutazione dei rischi e delle minacce

### IDENTIFICARE I PUNTI CRITICI

In genere l'audit parte da una preliminare mappatura delle risorse da verificare, formalizzata attraverso la valutazione in termini di rischi e minacce degli oggetti che compongono l'ambiente aziendale, che porti l'auditor a comprendere come si svolge una certa attività in termini di business, di organizzazione e di tecnologie utilizzate. L'obiettivo della mappatura è di ricondurre a un modello logico la complessità delle architetture, dei processi e delle procedure di elaborazione dei dati, individuando le componenti critiche su cui procedere con le opportune verifiche. Partendo dagli obiettivi di sicurezza sarà importante identificare gli ambiti operativi, le applicazioni, i dati, che per l'azienda rappresentano i punti più critici e sensibili del proprio business. Per capire quali siano i processi e gli asset critici di un'azienda occorre un'analisi molto attenta che richiede tempo, energie e risorse. «Quando si effettua un assessment della rete, vanno prima individuati gli asset critici e poi procedere nella selezione di quelli che verranno

messi in sicurezza, assegnando le priorità e tenendo conto degli aspetti legati alla compliance», ci conferma **Ombretta Comi, marketing manager di McAfee Italia** ([www.mcafee.com/it](http://www.mcafee.com/it)). Solo dopo questa fase si sarà in grado di stabilire cosa deve essere difeso, con quali priorità e in quale modo. «Man-

cando un'analisi critica della situazione operativa, il rischio è quello di intervenire in modo non efficace o poco tempestivo», mette in guardia **Alberto Prandini, regional director Italy, Greece and Cyprus di Radware** ([www.radware.com](http://www.radware.com)). Ritornando all'importanza di regole chiare dalle quali partire retoricamente ci si chiede in che modo senza questa base di partenza l'auditor potrebbe eseguire le proprie verifiche. «Gli auditor seguono un paradigma che può essere semplificato con l'acronimo Rce ovvero "regole, controlli ed evidenze"», ci dice **Antonio Forzieri, principal consultant Symantec Professional Services** ([www.symantec.com/it](http://www.symantec.com/it)). Con le prime naturalmente ci si riferisce a quell'insieme di direttive di cui si è dotata l'azienda per rispondere alle richieste di conformità provenienti da regolamenti interni ed esterni; i controlli saranno quelli applicati per ridurre i rischi di sicurezza e di non conformità; le evidenze infine si concretizzeranno nella raccolta delle prove a dimostrazione dell'efficacia dei controlli effettuati. «La presenza di regole formalizzate è fondamentale affinché l'audit possa produrre risultati validi per l'azienda», sostiene Forzieri.

### MANCATA SPONSORIZZAZIONE

L'audit di sicurezza coinvolge non solo prodotti e applicazioni, ma anche i processi ed è essenziale che ci sia collaborazione e consapevolezza dell'importanza

di ciò che si sta facendo. In questa fase, secondo **Paola Gattoni, director Cisco Services Italia** ([www.cisco.com/it](http://www.cisco.com/it)), «l'errore da evitare è la mancata sponsorizzazione». È importante cioè che i manager dell'azienda preparino tempestivamente i propri dipendenti, spiegando loro le motivazioni alla base del

processo, i benefici che ne possono derivare, in termini di miglioramento del modo di gestire il business e di riduzione dei costi, e i risultati complessivi che si vogliono raggiungere; «ciò permette di attenuare la resistenza di coloro che vivono queste procedure come strategie volte al monitoraggio e alla valutazione dell'attività svolta», argomenta Gattoni; tutta l'organizzazione deve perciò essere coinvolta e motivata nella realizzazione di tali iniziative; «in caso contrario è possibile che questi processi risultino inefficaci o portino addirittura a risultati negativi», avverte Gattoni. La raccolta di informazioni sull'azienda normalmente svolta tramite interviste a differenti interlocutori, analisi di documenti e dati pertinenti in effetti non può avere successo senza una collaborazione fattiva. E d'altra parte anche l'auditor deve essere in grado di utilizzare con competenza le tecniche più adatte, gestendo le attività in completo outsourcing o se diversamente stabilito in parziale affiancamento con il personale interno; senza dimenticare il significato della parola audit, ascolto, sapendo quindi relazionarsi con profitto con tutte le componenti umane in azienda. Un buon auditor dovrebbe essere in grado di sviluppare l'impianto della funzione di internal auditing formando le risorse interne da dedicare a questo scopo. Come detto arrivare all'audit di sicurezza senza aver fatto un'autovalutazione sul proprio livello di sicurezza Ict è ovviamente deleterio.



**Paola Gattoni**  
director Cisco  
Services Italia



**Emilio Turani**  
country manager  
di Stonesoft Italia,  
Svizzera Italiana, Grecia  
e Turchia



**Elio Molteni**  
senior technology  
specialist  
di CA

## La presenza di regole formalizzate è fondamentale affinché l'audit produca risultati validi per l'azienda

### GLI ERRORI PIÙ FREQUENTI

La mancanza di regole chiare dalle quali partire, le nostre policy di sicurezza, non è mai (e come potrebbe?) imputabile all'auditor. Ma la corresponsabilità dell'auditor diventa subito evidente nel momento in cui si presta a redigere quelle mancanti al posto dell'azienda negligente. Attenzione. La mancanza *tout court* di policy è un caso limite. Ma non ci discostiamo molto da questo caso quando si scopre, e accade di frequente, che quelle presenti in azienda altro non sono che un coacervo di regole messe insieme plagiando documenti redatti per altri scopi in ambiti completamente differenti senza che vi sia alcuna attinenza con la realtà che avrebbe dovuto esprimerli e senza avere neppure l'accortezza di adattare i nomi dei responsabili e delle funzioni interessate. Quindi: quale interesse potrà mai avere un'azienda a rispettare regole e procedure scritte da altri? I blog dei professionisti dell'auditing sono una lettura divertente e formativa, frustrante e sorprendente al tempo stesso. Le lamentele non sono solo dei profes-

sionisti nostrani. Tutt'altro. In tutti i Paesi dove la normativa in materia è stringente i casi di aziende negligenti sono numerosi. E la negligenza riguarda ambiti che mai ti aspetteresti di trovare così sguarniti. Prendiamo il controllo degli accessi. Le domande di partenza sono ovunque le stesse: chi è responsabile di

aggiungere, modificare, cancellare utenze all'interno di un dominio? Chi esegue materialmente la richiesta? In che modo si tiene traccia? Non per e-mail vero? Perché a molti auditor si chiede ancora di mettere in piedi una procedura formale? Oppure gli aggiornamenti di sicurezza: i server più importanti sono stati aggiornati in modo tempestivo? Perché allora si chiede all'auditor di farlo? Quanti sono gli amministratori del db server? Perché sono ancora registrati come amministratori collaboratori che da tempo hanno lasciato l'azienda? La lista potrebbe continuare a lungo.

### ANALISI SULLA MACCHINA

La valutazione delle misure di sicurezza messe in campo dall'azienda poggia sulla specifica conoscenza degli elementi che la costituiscono (meccanismi, politiche, tecnologie, funzioni organizzative, ...). Le soluzioni tecnologiche, in particolare nel campo della sicurezza, possono fornire un valido supporto, riducendo drasticamente i tempi e i costi di gestione e, al tempo stesso, limitando i possibili errori umani a patto però di non sottovalutare alcuni aspetti evidenziati da **Emilio Turani, country manager di Stonesoft Italia, Svizzera Italiana, Grecia e Turchia** ([www.stonesoft.com/it](http://www.stonesoft.com/it)), quali «la disponibilità di informazioni aggiornate, di facile e immediata comprensione anche sotto forma di resoconti dettagliati di engine e amministratori che illustrino le impostazioni di sicurezza

utilizzate e riepilogano i cambiamenti apportati al sistema». Gli auditor dei sistemi informativi, a maggior ragione quando si parla di sicurezza, sono spesso chiamati a verificare tutto questo ricalcando, come rileva **Elio Molteni, senior technology specialist di CA** ([www.ca.com/it](http://www.ca.com/it)), «le fasi del processo di analisi e gestione dei rischi e fornendo al termine dell'attività di assessment un risultato tangibile di quanto esaminato». Inutile dire che in questa fase di verifica è fondamentale che l'auditor possieda un'adeguata esperienza per ridurre al minimo il margine di errore nell'analisi. Ogni auditor ha modalità proprie per effettuare la verifica tecnica delle falle della sicurezza in azienda. Ci sono esperti che preferiscono fare le prove e i test durante il life-cycle quotidiano di un'azienda e non sulla "macchina smontata". Per altri è vero esattamente il contrario. «L'obiettivo è di verificare la struttura nella sua dinamicità testando e verificando l'esistenza di possibili errori dalla modalità all-on alla modalità all-off – sintetizza **Alexander Moiseev, managing director Kaspersky Lab Italia** ([www.kaspersky.it](http://www.kaspersky.it)) –; in questo senso l'azienda deve prepararsi a essere molto cooperativa, non solo per condividere ma anche per variare la struttura di una rete durante le prove».



**Alexander Moiseev**  
managing director  
Kaspersky Lab Italia



**Bernardino Grignaffini Gregorio**  
practice executive security  
& It governance di Lutech

Un black box audit può sempre condurre a falsi positivi e quindi sarà meno vantaggioso per il cliente

**BLACK BOX AUDIT**

Considerazioni analoghe potrebbero valere per le attività di analisi delle vulnerabilità tecnico/organizzative, le cosiddette "black box", utili secondo alcuni sia per evidenziare le lacune e i punti deboli delle politiche di sicurezza aziendali sia soprattutto per portare all'attenzione dei responsabili il livello di conoscenza e rispetto delle regole da parte del personale.

Secondo **Molteni** di CA un'attività di analisi condotta in modalità black box, ovvero con un livello nullo di conoscenza del sistema da misurare, si limita a fornire informazioni circa la presenza di vulnerabilità sui sistemi target o di vettori di intrusione: «Un black box audit può sempre condurre a falsi positivi e quindi sarà meno vantaggioso per il cliente. È importante – nota **Bernardino Grignaffini Gregorio, practice executive security & It governance di Lutech** ([www.lutech.it](http://www.lutech.it)) – che l'azienda utilizzi questo tipo di analisi solo per avere un riscontro sullo stato di sicurezza del target e non per ottenere informazioni utili su come indirizzare il proprio piano programmatico della sicurezza It». Diverso il parere di **Paola Gattoni** di Cisco secondo cui il black box audit è un approccio molto efficace se applicato utilizzando tool e metodologie costruite sfruttando un'effettiva conoscenza delle reti. «I risultati migliori si ottengono quando poche persone sono a conoscenza del test che si sta effettuando e quindi attraverso l'attacco è possibile non solo individuare le eventuali vulnerabilità, ma anche valutare se, e quando, l'organizzazione si accorge della violazione e in che modo interviene», argomenta Gattoni. Secondo **Claudio**

**De Paoli, solutions principal RSA Emea South** ([www.rsa.com](http://www.rsa.com)), i risultati più interessanti che questo tipo di analisi evidenziano sono quelli relativi agli attacchi di social engineering: «È sorprendente riscontrare quanto sia semplice ottenere informazioni critiche di un'azienda semplicemente facendo leva su tecniche psicologiche in grado di convincere le persone a rivelare password, codici di accesso o anche documenti e informazioni classificate». Per **Luigi Pugnetti, chief technological officer di Symbolic** ([www.symbolic.it](http://www.symbolic.it)), una procedura di questo tipo, conosciuta anche come "penetration test", è solo in parte legata a un security auditing: «Un penetration test inserito all'interno del processo di security auditing è uno strumento che permette di mettere alla prova le capacità del sistema e di rilevare potenziali azioni dannose e le relative capacità di risposta». Ma aggiunge Pugnetti in questo contesto un attacco di tipo black box «è meno adatto di uno lanciato con la piena conoscenza della struttura».

**OBIETTIVO CENTRATO**

Ribadiamo: definire gli obiettivi dell'audit di sicurezza significa in primo luogo stabilire il tipo di informazioni che l'attività di analisi dovrà produrre. Un security audit condotto secondo i criteri evidenziati restituirà due categorie di informazioni: il livello di compliance di sistemi e utenti che fanno parte dell'azienda e di conseguenza gli elementi per determinare il livello di rischio. L'analisi tuttavia deve tenere distinte tecnologia e utenti. L'azienda potrebbe disporre della tecnologia più evoluta, ma non di un livello altrettanto valido di competenze al proprio interno; oppure potrebbe emergere che policy e procedure toccano tutti i processi aziendali, ma non vengono rispettate. Per valutare il livello di rischio l'audit deve mettere in luce tutti i pos-



**Maurizio Martinozzi**  
manager sales  
engineering  
di Trend Micro Italy



**Mariangela Fagnani**  
risk management  
services leader  
di IBM Italia

L'azienda potrebbe disporre di tecnologia evoluta, ma non di un livello valido di competenze interne

sibili rischi. La violazione dei sistemi It può avvenire in diversi modi, originare da una cattiva gestione o configurazione, da utenti interni e partner esterni, da attacchi esterni e così via. Come spesso sentiamo ripetere è proprio dal fuoco amico che possono arrivare gli attacchi più deleteri: «Secondo il Cert, Computer Emergency Response Team, nel 99% dei casi le intrusioni nelle reti informatiche sono possibili sfruttando le vulnerabilità note o gli errori di configurazione dei sistemi, per i quali erano già disponibili le contromisure», ci conferma **Maurizio Martinozzi, manager sales engineering di Trend Micro Italy** ([www.trendmicro.it](http://www.trendmicro.it)). Naturalmente pur ricomprese nelle due categorie evidenziate le informazioni varieranno in funzione degli obiettivi stabiliti. Facciamo qualche esempio. L'azienda potrebbe essere interessata a valutare la presenza di vulnerabilità all'interno di un set di applicazioni; oppure voler valutare l'efficacia generale della propria piattaforma di sicurezza. Ma, qualunque sia l'obiettivo, «il loro consolidamento – rileva **Grignaffi-**

**ni** di Lutech – permetterà all'azienda di concordare le modalità di esecuzione dei test, quali per esempio le regole di ingaggio, le tempistiche di svolgimento, il target delle analisi e i risultati attesi, in modo preciso». Per **Luigi Pugnetti** di Symbolic il contributo maggiore ottenibile dal security auditing è la creazione della consapevolezza sullo stato della propria infrastruttura e la possibilità di mettere a punto le policy per la corretta gestione degli eventi: «La frase "not an event but a process" pur abusata è veritiera. In questo contesto la figura dell'auditor, passa in secondo piano rispetto alla messa in pratica del processo. Ovviamente un "processo" compiuto da persone non preparate sarebbe a sua volta poco utile». In definitiva però un audit di sicurezza ben condotto porterà a risultati che non si discosteranno molto da quelli evidenziati da **Mariangela Fagnani, risk management services leader di IBM Italia** ([www.ibm.com/security](http://www.ibm.com/security)): «La verifica dell'audit di sicurezza, porta all'evidenza del top management, oltre che delle strutture operative, i rischi conseguenti alle vulnerabilità e alle carenze individuate e il loro impatto sui risultati aziendali».

**MISURAZIONI E VALUTAZIONI ERRATE**

Ogni misurazione è soggetta a errori; a maggior ragione quando il sistema da valutare è complesso come un'infrastruttura Ict. Quelli più frequenti sono l'utilizzo di strumenti poco affidabili oppure l'interpretazione errata dei risultati. Per ovviare al primo è importante adottare metodologie consolidate che garantiscano i necessari livelli di ripetibilità della misura riducendo così gli errori di tipo sistematico. Uno degli errori che l'azienda può commettere nell'utilizzo dello strumento Vapt (Vulnerability assessment & penetration testing) è la scarsa sensibilità nel valutare i risultati dell'analisi. La principale conse-



**CHECK POINT: POLICY DI SICUREZZA? IL MINIMO!**

Ogni azienda dovrebbe definire, e possibilmente implementare policy di sicurezza. «Le policy di sicurezza sono necessarie e sovrintendono l'accesso e l'utilizzo delle informazioni principali e più importanti di una organizzazione – spiega **Andrea Bellinzaghi, SE manager di Check Point Italia** ([www.checkpoint.com](http://www.checkpoint.com)) –. Spesso le aziende non definiscono, e se anche lo fanno, non informano in modo esaustivo il personale su quali sono le prassi e i comportamenti da seguire nell'utilizzo delle informazioni e dei sistemi». L'insieme degli strumenti di sicurezza di una azienda (Fw, Ips, Dlp, ...) andrà poi configurato e implementato in modo da attuare accuratamente le policy di sicurezza precedentemente identificate. «Una volta definita, distribuita e implementata, la policy di sicurezza aziendale deve essere costantemente aggiornata per poter far fronte alle nuove tecnologie, modelli di business e richieste del mercato», spiega ancora Bellinzaghi. Inoltre, esistono normative locali e internazionali che richiedono l'implementazione di determinati sistemi e policy di sicurezza. «Si può infine dire che la policy di sicurezza aziendale evolve di pari passo con l'evoluzione dell'impresa stessa e permette alla società di incrementare e proteggere il proprio business», conclude Bellinzaghi.

guenza della mancanza di regole chiare è la soggettività del giudizio dell'auditor. Un altro errore frequente è l'assenza di contestualizzazione dei risultati dell'audit rispetto allo specifico ambito tecnico/organizzativo. Non sono infrequenti neppure i casi in cui i risultati di audit che evidenziano lacune tecniche siano indirizzati al top management così come non lo sono quelli di allarmi ingiustificati tali per cui le lacune evidenziate non sono (da un punto di vista di gestione del rischio) preoccupanti per la sicurezza globale. «Tale situazione risulta di difficile risoluzione quando l'obiettivo di un audit è quello di verificare la rispondenza a una normativa – rileva **Claudio De Paoli** di RSA –; in questi casi anche una “non conformità” non grave da un punto di vista dell'analisi del rischio può essere la causa di una sanzione penale per l'azienda stessa». Altrettanto frequente è l'errata valutazione circa la cadenza con cui svolgere questi test. «Queste analisi rappresentano di fatto delle “istantanee” della situazione di sicurezza dell'azienda e pertanto la loro valenza tende a diminuire con il passare del tempo – argomenta **Gregorio Grignaffini** di Lutech –. La frequenza degli audit andrebbe definita in base a diversi parametri, tra cui la dinamicità dell'ambiente Ict dell'azienda e la scoperta di nuove vulnerabilità». In sintesi è importante non solo il ruolo dell'auditor e la sua competenza nel riuscire ad analizzare lo stato di un sistema e di un'organizzazione, ma, come riconosce De Paoli, «anche e soprattutto il legame fra le attività svolte dall'auditor rispetto alle politiche aziendali e la conoscenza e diffusione di tali politiche all'interno dell'organizzazione».

## PIANO DI RIENTRO INADEGUATO

Uno degli errori più comuni in cui può incorrere l'auditor è quello di fornire un piano di rientro eccessivamente ambizioso che non tenga cioè conto della realtà operativa del cliente o, al contrario, troppo sbilanciato sulla tecnologia perdendo di vista le neces-



La frequenza degli audit  
va definita in base  
a diversi parametri,  
tra cui la dinamicità  
dell'ambiente Ict

sità di business. «È di fondamentale importanza invece raggiungere il dovuto “trade-off” mostrando al business owner a quale rischio è esposto, e fornendo indicazioni utili a compensare le problematiche riscontrate», afferma **Antonio Forzieri** di Symantec.

«La collaborazione con il cliente è fondamentale per definire non solo gli obiettivi sensibili, ma anche le priorità e la qualità degli interventi di difesa», ci dice **Alberto Prandini** di Radware. L'adozione di una certa strategia di difesa non può essere slegata dall'individuazione delle tipologie di attacco più pericolose per la tipologia di business dell'azienda. «Per esempio – si domanda Prandini – la priorità è di arginare l'intrusione nel proprio sistema oppure è quella di contrastare worm o bloccare botnet, o ancora è vitale che il flusso delle informazioni dalla periferia al centro e viceversa raggiunga proprio i destinatari designati, con la massima rapidità e in piena sicurezza, ottimizzando le risorse?». L'assunto di partenza è che ogni area importante per l'azienda presenta dei punti deboli; l'unico modo per anticipare le modalità

di attacco è di essere consapevoli di queste debolezze. In ultima analisi l'auditor deve essere in grado di portare concretezza alla propria analisi. Questo significa che l'azienda non dovrebbe ritrovarsi alla fine del progetto con raccomandazioni corrette teoricamente, ma irrealizzabili per le proprie caratteristiche e dimensioni.

## IL VALORE DELL'AUDIT

Il corretto utilizzo delle risorse It anche dal punto di vista della gestione dei rischi è fondamentale per il successo di un'azienda. Diversamente da quanto avviene in organizzazioni e imprese dove la cultura del controllo e il rispetto delle normative e degli standard rappresentano altrettanti punti fermi del sistema di valore aziendale, in altre realtà le problematiche di audit sono state a lungo sottovalutate per lacune sul piano della cultura organizzativa e manageriale oppure perché si è preferito privilegiare altri paradigmi basati più sull'innovazione al di fuori delle regole. Oggi vari fattori connessi alla liberalizzazione di mercati e capitali e alla conseguente necessità di adattare le proprie regole a quelle transnazionali anche in Italia, soprattutto nelle realtà più importanti e aperte all'internazionalizzazione e sotto la spinta di organi di controllo istituzionali, si assiste alla nascita di strutture di internal auditing preparate a periodici audit da parte di organismi esterni. Il rispetto delle normative è importante, ma non basta. La sicurezza non è superare un test, compilare correttamente una checklist, ottenere un punteggio alto. Nessuna di queste attività autorizza a pensare di essere al sicuro. In effetti al di là di obblighi più o meno stringenti nelle realtà più evolute è ferma la convinzione che l'attività di audit racchiuda un enorme valore per l'azienda. Certo occorre saperlo fare bene e riuscire a spiegarlo altrettanto bene al proprio interno. E soprattutto essere in grado di scoprire i propri punti deboli e vulnerabilità prima di chiunque altro. **DM**