

INTRODUZIONE

Per l'introduzione del presente volume, gli autori hanno consultato i mezzi di informazioni principali e i blog dedicati alla sicurezza, trovando più segnalazioni che mai sui problemi di sicurezza. La situazione non è confortante:

- ▼ le autorità delle finanze avvertono i contribuenti su truffe con furti di identità;
- negli USA sono state sottratte le informazioni personali di oltre 200.000 persone;
- virus ricattatori impostati in modo da cancellare file;
- troiani che sottraggono migliaia di login alle banche;
- bot e malware che favoriscono lo sviluppo del crimine informatico;
- ▲ un difetto “molto critico” in Windows, Internet Explorer, OSX, Firefox.

In sostanza, il mondo non è un luogo sicuro (fisicamente ed elettronicamente). Il presente volume presenta al lettore 20 nuove situazioni reali, che descrivono argomenti attuali come quelli indicati di seguito:

- ▼ phishing;
- rootkit;
- nuovi attacchi wireless;
- attacchi VoIP;
- ▲ attacchi peer-to-peer.

Nella misura in cui Internet aumenta di dimensioni e di utenti, cresce il numero di incidenti relativi alla sicurezza dei computer. Un elemento che non viene mai spiegato dalla stampa è il modo in cui si verificano tali incidenti, cosa abbia portato all'incidente, cosa lo abbia consentito, cosa lo abbia provocato, cosa lo avrebbe potuto evitare, come mitigare i danni e soprattutto come si sia verificato l'incidente. Se il lettore è interessato a tali argomenti, questo volume fa per lui.

Il presente volume presenta storie relative alla sicurezza informatica, basate su fatti reali, portando il lettore all'interno della storia. Nello sviluppo degli avvenimenti vengono presentate informazioni sull'incidente e il lettore viene invitato a risolvere il caso.

Gli autori hanno ritenuto opportuno ricreare gli eventi, perché la sicurezza delle informazioni non è mai noiosa, né un campo per persone timide. Non è una disciplina per le persone che si ritengono "arrivate": ogni professionista della sicurezza deve adattarsi continuamente a nuove strategie di attacco e di mitigazione.

Non molto tempo fa, nessuna università offriva corsi sulla sicurezza informatica. In quei tempi la maggior parte degli autori del presente volume si è trovata nel campo della sicurezza informatica inseguendo un sogno esagerato dai film, non considerato da molti nel campo della tecnologia e reso affascinante dall'industria. Tuttavia la sicurezza informatica era una scelta di carriera diversa, non una destinazione resa possibile da un consulente dell'orientamento nelle scuole superiori. Molti degli autori del presente volume hanno conseguito diplomi e certificazioni in aree molto lontane dalla sicurezza informatica, ma ciascuno si è trovato in questo campo per scelta deliberata.

Hanno seguito il sogno della soddisfazione sul lavoro e nel percorso sono stati incoraggiati dalle ricompense. Tale scelta di carriera ha visto la nascita di una delle migliori generazioni di esperti della sicurezza mai esistite.

Dagli anni ottimistici dell'esplosione della sicurezza informatica, questa si è evoluta da un hobby o da una tecnologia divertente in un ruolo vitale nell'economia moderna. Non tutto il lavoro sulla sicurezza delle informazioni è stimolante dal punto di vista intellettuale: molte giornate sono piene di analisi tediose con lunghi e noiosi esami di log o di revisioni di politiche ripetute, documentando semplicemente il buon senso per i meno esperti. Alcuni documenti sono colmi di valutazioni o di test di penetrazione, solo per trovare la stessa vecchia vulnerabilità o il medesimo errore di programmazione.

Oggi la prossima generazione di professionisti della sicurezza formati all'università inizia a dominare l'industria. L'industria nel suo insieme ha subito una trasformazione significativa, principalmente in base alle minacce sempre diverse e al rapido sviluppo di exploit e in parte grazie al nuovo gruppo di professionisti. Sono lontani i giorni in cui era possibile ripararsi dietro un firewall e affidarsi a un sistema di rilevamento di intrusioni per l'avvertimento di eventi: oggi i professionisti della sicurezza devono considerare minacce mirate ai clienti, quali phishing, pharming e registrazioni di pressioni di tasti. È necessario lavorare in un ambiente che richiede ore per reagire alle nuove vulnerabilità, non giorni. È necessario essere preparati per gli attacchi di tipo zero-day. È necessario decidere consciamente di non proteggere qualcosa se il costo della protezione supera la perdita prevista.

Le storie presentate nel presente volume intendono ricordare ai veterani perché gli autori hanno iniziato a lavorare nel campo della sicurezza. Gli autori si augurano che tali storie siano utili per l'incoraggiamento e la formazione della prossima generazione di professionisti in questo campo in continua

espansione, e per ricordare agli autori stessi perché hanno iniziato a lavorare per la sicurezza. Il presente volume è pensato per fornire un ambiente sicuro in cui raccontare le storie sulla sicurezza delle informazioni reali che ispirano tutti nel loro lavoro, per mantenere attive le proprie capacità, per divertire e per insegnare.

Organizzazione

Il volume è suddiviso in due parti. La prima parte contiene tutti gli studi di casi; in ciascuno di essi si trova una descrizione dettagliata del caso con tutte le prove e le informazioni legali (file di log, mappe di rete e così via) necessarie al lettore per determinare esattamente quanto accaduto. Per motivi di brevità in molti capitoli è stata eliminata gran parte delle prove, lasciando quasi esclusivamente le informazioni rilevanti (per evitare di inserire molte pagine di dati da esaminare). Alla fine di ciascuno studio di caso, alcune domande specifiche guidano il lettore verso un'analisi corretta.

La seconda parte del libro contiene tutte le soluzioni alle sfide lanciate nella prima parte. In questa parte lo studio di caso viene attentamente esaminato, con tutte le informazioni probatorie completamente spiegate, insieme alle risposte alle domande. I paragrafi sulla mitigazione e sulla prevenzione offrono ulteriori informazioni.

Proteggere gli innocenti

Per proteggere l'anonimato delle organizzazioni presenti nelle storie, molti dettagli di ogni caso sono stati modificati o eliminati. È stata prestata attenzione alla protezione dell'integrità di ciascuno studio di caso, quindi nel processo non è andata perduta alcuna informazione. Le informazioni modificate comprendono quanto segue:

- ▼ nomi delle società;
- nomi di dipendenti;
- indirizzi IP;
- date;
- dettagli sulla modifica Web (modifiche ai messaggi per eliminare volgarità o altri contenuti inopportuni);
- ▲ dettagli non essenziali per la storia.

Informazioni sulle vulnerabilità

Nel presente volume, dove possibile, si fa riferimento a risorse esterne contenenti ulteriori informazioni sulle vulnerabilità descritte (paragrafo "Ulteriori risorse" alla fine delle soluzioni). Inoltre le organizzazioni MITRE e Secu-

rityFocus contengono database leggermente diversi delle vulnerabilità, utili come risorse generali.

MITRE (<http://cve.mitre.org>) è una risorsa no profit per le tecnologie nazionali americane, che offre supporto a ingegneria di sistemi, ricerca e sviluppo di tecnologie informatiche. *Common Vulnerabilities and Exposures (CVE*, vulnerabilità ed esposizioni comuni) è un elenco, o dizionario, che offre nomi comuni di vulnerabilità ed esposizioni nella sicurezza delle informazioni note al pubblico. L'utilizzo di un nome comune facilita la condivisione di dati su database e strumenti diversi, che fino a questo momento non erano facilmente integrati. Questo rende CVE la chiave per la condivisione di informazioni.

SecurityFocus (<http://www.securityfocus.com>) è il fornitore di servizi di informazioni sulla sicurezza leader per l'industria. La società gestisce la più grande e più attiva comunità sulla sicurezza dell'industria e gestisce il portale principale dell'industria della sicurezza, che serve oltre 250.000 utenti diversi al mese. Il database di vulnerabilità di SecurityFocus è la raccolta più completa disponibile delle vulnerabilità sulla sicurezza informatica pubblicate.

Tassonomia della complessità

Tre classificazioni di complessità, presenti in una tabella all'inizio di ciascun capitolo, descrivono la complessità generale di ciascun incidente. Tali classificazioni descrivono l'incidente dal punto di vista dell'aggressore e dell'esperto in sicurezza.

Complessità dell'attacco

La complessità dell'attacco indica il livello di abilità tecnica dell'aggressore. Definisce la sofisticazione generale dell'aggressore. Spesso si osserva che più un ambiente è complesso e protetto, più deve essere complesso l'aggressore per comprometterlo (naturalmente non è sempre vero).

- ▼ **Bassa** Solitamente gli attacchi di questo livello sono effettuati da principianti degli script. L'aggressore fa poco più che eseguire uno script di attacco, compilare codice di facile reperibilità o utilizzare un metodo di attacco noto al pubblico, con un comportamento poco o per nulla innovativo. Si tratta del tipo di attacco più semplice.
- **Media/Moderata** L'aggressore utilizza un metodo di attacco noto al pubblico, ma lo estende e inserisce alcune innovazioni. Tra di esse si possono trovare la contraffazione di indirizzi o lievi modifiche ai comportamenti di attacco "normali".
- ▲ **Alta** L'aggressore è intelligente e ragionevolmente preparato. La vulnerabilità può essere pubblica o no, e probabilmente l'aggressore scrive il proprio codice.

Complessità di prevenzione e mitigazione

La complessità della prevenzione indica il livello di complessità che sarebbe stato necessario da parte dell'organizzazione per prevenire l'incidente. La complessità della mitigazione indica il livello di complessità necessario a ridurre l'impatto del danno causato dall'incidente all'infrastruttura dell'organizzazione. Sono simili, e possono essere definite con la stessa tassonomia:

- ▼ **Bassa** La prevenzione o la mitigazione del problema può essere semplice quanto una patch o un aggiornamento software, oppure l'aggiunta di una regola a un firewall. Solitamente tali modifiche sono semplici e non implicano un lavoro eccessivo.
- **Media/Moderata** Il rimedio può richiedere una patch o un aggiornamento software complessi, spesso insieme a modifiche delle politiche su un firewall. Può inoltre essere necessaria una nuova installazione di una macchina infettata e/o piccole modifiche all'infrastruttura.
- ▲ **Alta** Sono necessari una patch o un aggiornamento complessi, oppure una serie di aggiornamenti a molte macchine, oltre a modifiche importanti all'infrastruttura. Questo livello può anche comprendere vulnerabilità estremamente difficili da prevenire o da mitigare.

Convenzioni utilizzate nel libro

Per sfruttare al meglio il presente volume, può essere utile sapere come è stato ideato. Di seguito un breve riassunto.

Nel testo di ciascun capitolo si trovano file di log, mappe di rete, elenchi di file, output di comandi, codice e diverse altre prove legali. Tali informazioni sono stampate il più fedelmente possibile agli originali di ciascun caso, ma è necessario considerare che le limitazioni relative alla stampa e la riservatezza hanno richiesto alcune modifiche.

Il libro è suddiviso in due sezioni. Nella prima parte i capitoli da 1 a 20 presentano i dettagli di incidenti reali. Ciascun capitolo inizia con una tabella riassuntiva che elenca il settore della società colpita e la classificazione della complessità per attacco, prevenzione e mitigazione.

Domande

Alla fine di ciascun capitolo si trova un elenco di domande che indirizza la ricerca dei dettagli dell'incidente e guida il lettore verso la soluzione generale. Il lettore può prendere appunti in questo paragrafo o nel testo, mentre risolve il caso.

Risposte

Nella seconda parte del libro si trovano le soluzioni corrispondenti, da 1 a 20. Ciascuna soluzione spiega in dettaglio come è stato risolto l'incidente, oltre a fornire le risposte alle domande presentate nella prima parte del libro.

Prevenzione

La soluzione contiene un paragrafo "Prevenzione", in cui si trovano suggerimenti su come fermare un attacco prima del suo inizio. Tali informazioni possono risultare utili per società che si trovano in situazioni simili a quella della sfortunata organizzazione descritta nel libro.

Mitigazione

La soluzione contiene inoltre un paragrafo "Mitigazione", in cui si apprendono le azioni intraprese dalla società colpita per riparare i danni dopo l'attacco.