Shorr Kan IT Engineering Srl

Tipo documento:	**Attacchi alle infrastrutture telematiche**
Cliente:	**VARI**
Versione:	**2.1**
Data documento:	**11/01/2007**
Autore:	**D. Casale**
Revisore:	**D. Nigro**

Attacchi alle infrastrutture telematiche

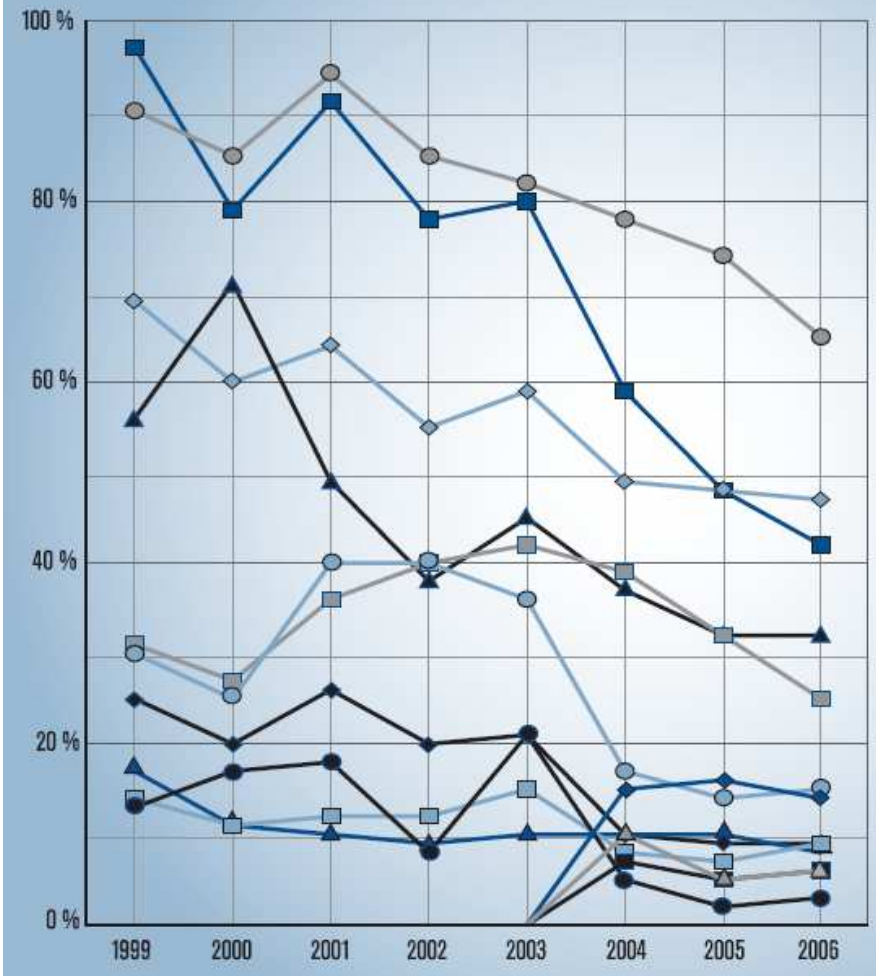
Qualsiasi infrastruttura di rete è soggetta ad attacchi informatici automatici od umani provenienti sia dall'esterno (Internet) che dall'interno da parte di persone che accidentalmente (portandosi dietro sul loro client virus, malware o trojan) o con malevolezza effettuano attività dannose verso i nostri sistemi.

Una preziosa fonte aggiornata di informazioni a supporto di quanto appena affermato è il 'Computer Crime and Security Survey' edito annualmente dall'FBI e dal Computer Security Institute statunitense (www.gocsi.com).

Gli ultimi dati sugli attacchi o usi fraudolenti dei sistemi evidenziano che negli ultimi anni le tipologie di azioni malevoli si sono notevolmente diversificate, ma permangono ai primi tre posti come volume i virus, il furto fisico di apparati (specialmente portatili o pda) e l'abuso di sistemi da parte del personale interno.

Figure 14. Types of Attacks or Misuse Detected in the Last 12 Months

By Percent of Respondents



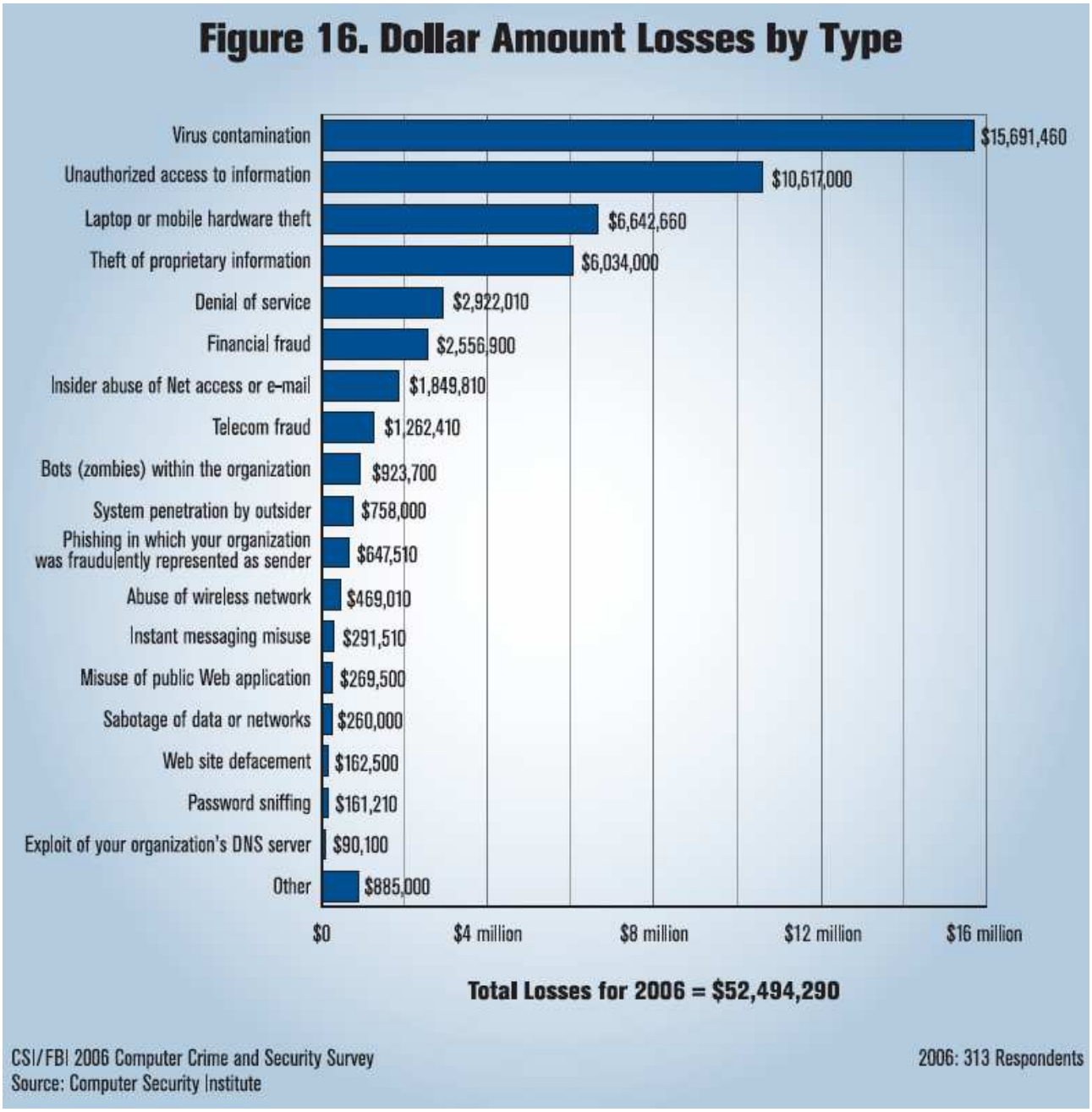
TYPE OF ATTACK	2006
Virus	65%
Laptop/mobile theft	47%
Insider abuse of Net access	42%
Unauthorized access to information	32%
Denial of service	25%
System penetration	15%
Abuse of wireless network*	14%
Theft of proprietary information	9%
Financial fraud	9%
Telecom fraud	8%
Misuse of public Web application*	6%
Web site defacement*	6%
Sabotage	3%

* questions added in 2004

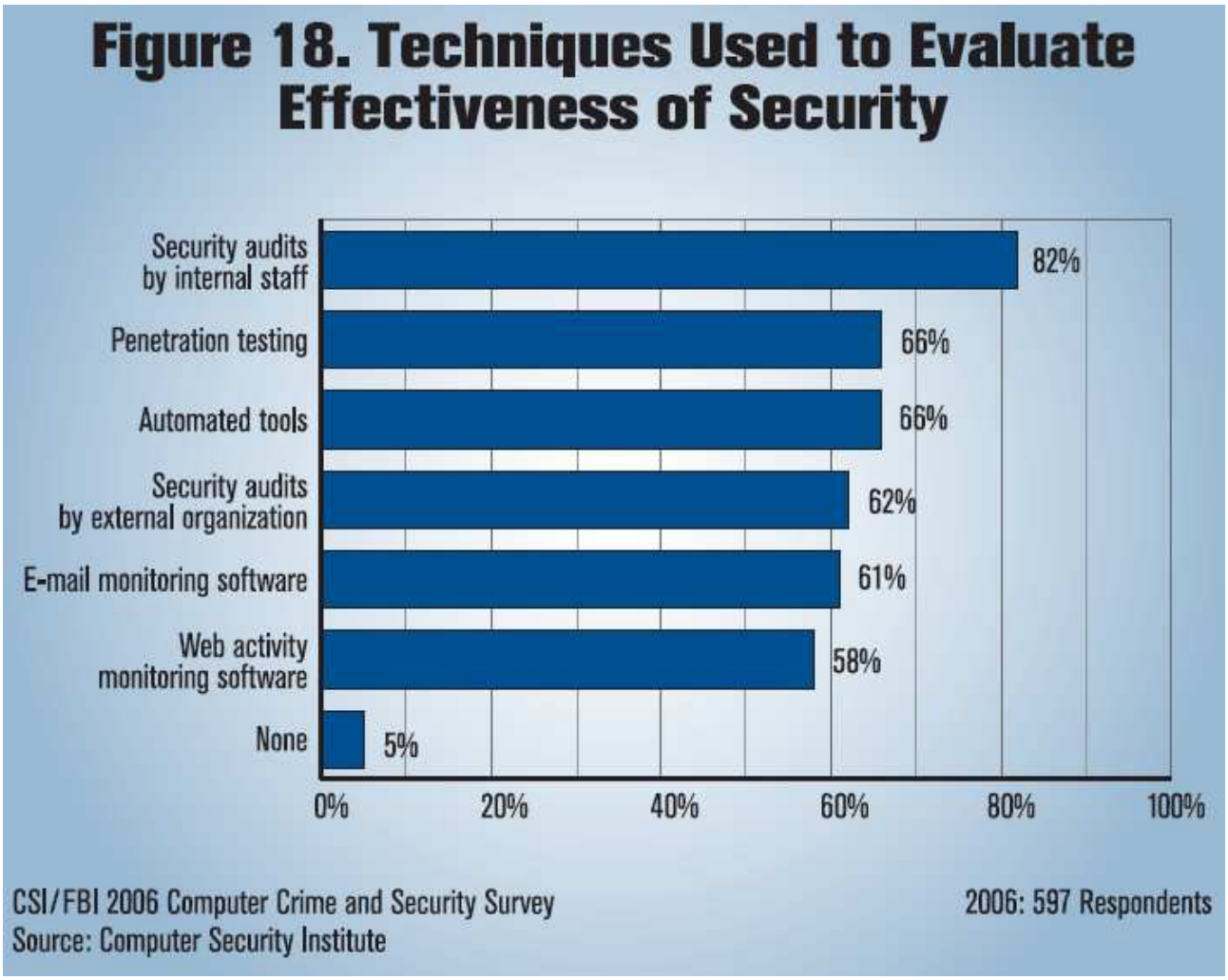
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute

2006: 616 Respondents

Le perdite dal punto di vista economico sul campione di aziende intervistate (313 unità) è notevole e distribuito in proporzione alle tipologie di attacchi più diffusi :



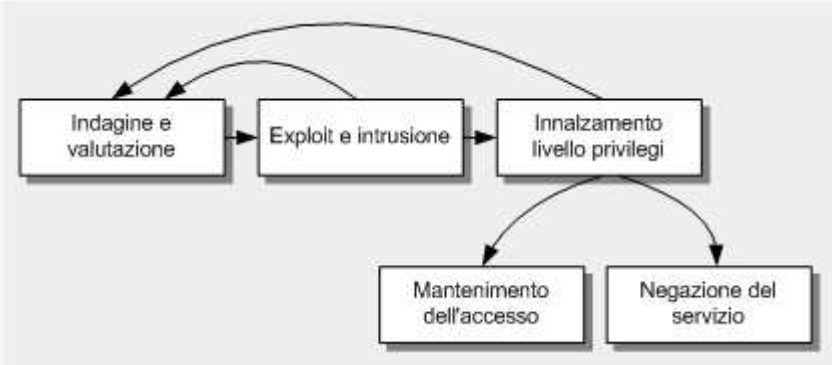
Da notare che il 'Penetration Testing' od 'Ethical Hacking' stà diventando (a parte l'audit continuo da parte del personale interno) la metodologia migliore per valutare lo stato e l'efficacia dei sistemi di sicurezza della propria azienda :



Proviamo ora a descrivere i principali pericoli che potrebbero compromettere la rete, l'infrastruttura host e le applicazioni. Conoscere quali siano le minacce alla stabilità del sistema e le contromisure da adottare è un passaggio fondamentale per poter procedere all'modellazione dei pericoli.

ANATOMIA DI UN ATTACCO

Comprendendo l'approccio di base utilizzato dagli utenti malintenzionati per danneggiare i vostri sistemi, e riconoscendo quindi la minaccia da fronteggiare, sarà più semplice adottare misure difensive. I passaggi di base della metodologia di attacco sono riepilogati di seguito e illustrati nella seguente figura :



Passaggi di base dei metodi di attacco

1.1 Analisi e valutazione

L'analisi e la valutazione del potenziale obiettivo vengono eseguite in parallelo. Il primo passaggio di un utente malintenzionato consiste nell'analizzare il potenziale obiettivo per identificarne e valutarne le caratteristiche, che possono includere servizi e protocolli supportati ed eventuali vulnerabilità e punti di ingresso. Le informazioni raccolte nella fase di analisi e valutazione vengono utilizzate per pianificare un attacco iniziale.

Potrebbe essere individuata, ad esempio, una vulnerabilità su un servizio POP3 di posta elettronica o se parliamo di un servizio web based una vulnerabilità a livello di script tra i siti, mentre si verifica se i controlli di una pagina Web producono un output.

1.2 Sfruttamento delle vulnerabilità e penetrazione nel sistema

Dopo aver esaminato il potenziale obiettivo dell'attacco, il passaggio successivo consiste nello sfruttare la vulnerabilità individuata e penetrare nel sistema. Se la rete e l'host sono completamente protetti, il pirata informatico utilizzerà l'applicazione (il front end) come canale di attacco.
Il modo più semplice per introdursi in un'applicazione è utilizzare lo stesso punto di ingresso degli utenti autorizzati, ad esempio una pagina di accesso dell'applicazione che non richieda autenticazione.

1.3 Acquisizione di privilegi più elevati

Dopo essere riuscito a compromettere un'applicazione o una rete, ad esempio introducendo codice nell'applicazione o creando una sessione autenticata con il sistema operativo, il pirata informatico tenterà immediatamente di acquisire privilegi più elevati. In particolare, cercherà di ottenere i privilegi di amministrazione forniti dagli account appartenenti al gruppo Administrators o all'utente root (se parliamo di macchine unix). Tenterà anche di individuare il livello più elevato di privilegi offerto dagli account di sistema locali.
Come difesa principale contro gli attacchi volti ad acquisire privilegi più elevati è consigliabile utilizzare account di servizio con il livello minimo di privilegi. Inoltre, molti degli attacchi con acquisizione di privilegi elevati a livello di rete richiedono una sessione di accesso interattiva.

1.4 Gestione dell'accesso

Dopo aver avuto accesso al sistema, l'attaccante intraprende azioni mirate a rendere più semplice l'accesso in futuro e a coprire le tracce dell'intrusione. Le strategie più diffuse per semplificare l'accesso futuro includono l'inserimento di programmi backdoor o l'uso di un account esistente privo di protezione avanzata. Per coprire le tracce dell'intrusione si procede, in genere, a cancellare i registri o i log files e a nascondere gli strumenti. In questa prospettiva è chiaro che i registri di controllo sono uno degli obiettivi principali di un utente malintenzionato.
I file di registro ed i log giles devono essere protetti e regolarmente analizzati. L'analisi può rivelare i segni di un tentativo di intrusione prima che siano prodotti danni.

1.5 Negazione del servizio

Se non riescono a ottenere l'accesso al sistema, i pirati informatici sferrano, in seconda battuta, attacchi di tipo Denial of Service, per impedire ad altri di utilizzare l'applicazione. Per alcuni utenti malintenzionati, tuttavia, questo tipo di attacco è l'obiettivo principale sin dall'inizio. Negli attacchi di tipo SYN flood, ad esempio, l'utente malintenzionato utilizza un programma per inviare un flusso di richieste SYN TCP e riempire la coda delle connessioni in attesa del server. In questo modo si impedisce che altri utenti stabiliscano connessioni di rete.

Conoscendo i metodi comunemente utilizzati dai pirati informatici per danneggiare i sistemi e gli obiettivi a cui mirano è possibile applicare contromisure più efficaci. Inoltre, la consapevolezza degli obiettivi possibili è di grande utilità per la valutazione e la modellazione dei pericoli.

L'attività di security probe e vulnerability assessment permette di avere una precisa fotografia della propria infrastruttura in termini di sicurezza logica e con questa di intervenire in modo rapido e mirato a chiudere le falle ed innalzare così il proprio livello di sicurezza complessivo.

APPENDICE A : ESEMPIO DI SQL INJECTION

Un applicazione (client o web based) potrebbe essere soggetta ad attacchi di tipo SQL injection, se si incorpora input utente non convalidato nelle query di database. Particolarmente esposto a questo tipo di attacchi è il codice che crea istruzioni SQL dinamiche con input utente non filtrato.

Considerare il codice seguente:

```
SqlDataAdapter myCommand = new SqlDataAdapter(

         "SELECT * FROM Users

          WHERE UserName ='" + txtuid.Text + "'", conn);
```

I pirati informatici possono inserire codice SQL chiudendo l'istruzione SQL con una virgoletta singola seguita da un punto e virgola per iniziare un nuovo comando e, quindi, eseguendo il comando desiderato. Esaminare la seguente stringa di caratteri immessa nel campo **txtuid**.

```
'; DROP TABLE Customers -
```

Il risultato sarà l'invio al database dell'istruzione riportata di seguito perché venga eseguita.

```
SELECT * FROM Users WHERE UserName=''; DROP TABLE Customers --'
```

L'esecuzione dell'istruzione provoca la cancellazione della cartella Clienti, ammesso che l'account di accesso dell'applicazione abbia autorizzazioni sufficienti nel database (un altro motivo per utilizzare account di accesso al database con privilegi minimi). Il doppio trattino (--) indica un commento SQL e viene utilizzato per impostare come commento gli eventuali altri caratteri aggiunti dal programmatore, come la virgoletta finale.
Nota: il punto e virgola non è realmente necessario. Il sistema SQL Server eseguirà due comandi separati da spazi.
È possibile mettere in atto altre astuzie più sottili. Immettendo questo input nel campo **txtuid**:

```
' OR 1=1 -
```

viene creato il seguente comando:

```
SELECT * FROM Users WHERE UserName='' OR 1=1 -
```

Poiché l'equazione 1=1 è sempre vera, l'autore dell'attacco recupera tutte le righe della tabella Utenti.

Le contromisure adottabili per impedire gli attacchi di tipo SQL injection includono:

- Convalida completa dell'input. L'applicazione deve convalidare l'input prima di inviare una richiesta al database.
- Utilizzo di stored procedure con parametri per l'accesso al database, per garantire che le stringhe di input non siano considerate istruzioni eseguibili. Se non è possibile utilizzare stored procedure, per la creazione di comandi SQL utilizzare parametri SQL.
- Utilizzo di account con privilegi minimi per la connessione al database.