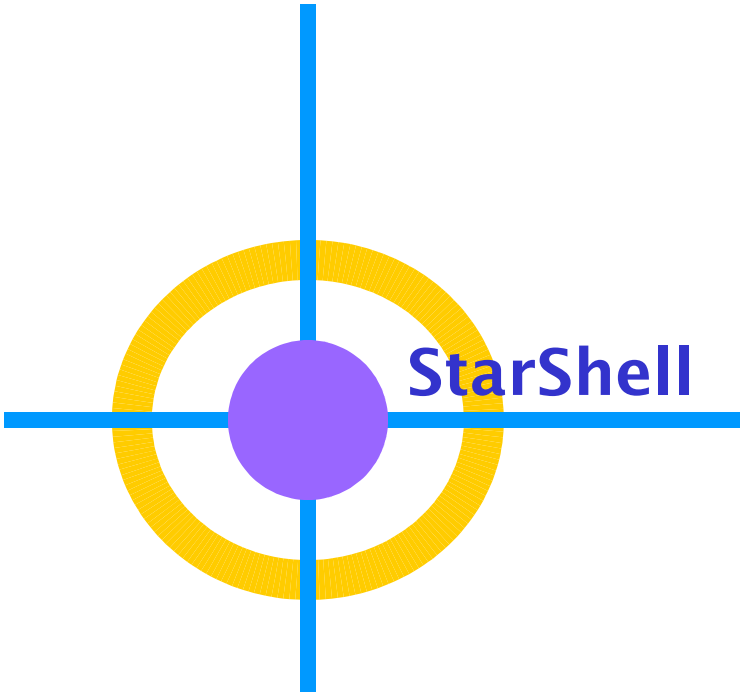


Vulnerabilità ed Esposizioni

Vulnerabilità più Critiche

- Non sono tutte le vulnerabilità esistenti
- Cambiano come la moda
- Sono le più sfruttate al momento
- Per sistemi in rete attaccati dall'esterno

- Concentrarsi prima sulle vulnerabilità critiche
- Poi affrontare le altre vulnerabilità

Perchè esistono Vulnerabilità

- I Sistemi Informativi sono complessi
  - Complessità crescente negli ultimi 30 anni
  - Complessità di organizzazione e amministrazione
  - Possibilità di errori umani pratici o di giudizio
- Errori nel software applicativo
  - Ogni programma utile contiene bachi
  - Occorrono tempo e risorse per mantenere il SW
  - Il Controllo di Qualità non è una priorità
    - **Favoriti ambienti di Rapid Application Development**
    - **Necessario il Fast Time to Market**
    - **Il personale di sviluppo costa più dell'Hardware**
- Non vi è diffusa consapevolezza di sicurezza

Perchè esistono Vulnerabilità

- I Sistemi Informativi sono complessi
  - Complessità crescente negli ultimi 30 anni
  - Complessità di organizzazione e amministrazione
  - Possibilità di errori umani pratici o di giudizio
- Errori nel software applicativo
  - Ogni programma utile contiene bachi
  - Occorrono tempo e risorse per mantenere il SW
  - Il Controllo di Qualità non è una priorità
    - **Favoriti ambienti di Rapid Application Development**
    - **Necessario il Fast Time to Market**
    - **Il personale di sviluppo costa più dell'Hardware**
- Non vi è diffusa consapevolezza di sicurezza

Scarsità di Personale Tecnico

- Troppe promesse, nessuno che le implementi
  - Necessario avere l'ultimo ritrovato HW e SW
  - Microsoft et al. spingono al ricambio piattaforme
  - Mafia del Training e della Certificazione
  - Università obsolete in partenza
- Il Provvisorio diventa Definitivo
  - I programmi prototipi sono adottati come finali
  - Non vi è tempo per la manutenzione HW e SW
  - Non vi è tempo per la sperimentazione di alternative
  - La documentazione è indietro rispetto al SW
- Cultura Business prevale su Cultura Tecnica

Risorse per Hacker

- Non è difficile scrivere Codice Malvagio
  - I programmi che danneggiano sono più semplici di quelli che compiono operazioni utili
- Siti di distribuzione in Internet
  - Kit di sviluppo e Programmi finiti
  - Praticamente tutte le piattaforme
- Conferenze internazionali
- Letteratura Underground
- Hackers per passione, non per necessità

Successo degli Attacchi

- Poco tempo per la difesa
  - Amministratori oberati di lavoro ‘vero’
  - Uso di software obsoleto, senza ‘Patch’
  - Errori e trascuratezze madornali
- Imbarazzo dei difensori
  - Diniego del problema
  - Mancanza di policies efficaci di difesa
  - Difficile prendere e punire i trasgressori
  - Assenza di denunce dei problemi
- Ignoranza dei metodi di attacco e difesa
  - Rapporti ed Advisories in rete

Operazioni Illegali

- Snooping e Downloading
  - Browsing di documenti, configurazioni, file riservati
  - Cattura a log del browsing
  - Scarico dei file interessanti per consultazione offline
    - **Competitive Intelligence**
  - Keystroke Sniffing
    - **Cavalli di Troia intercettano utilizzo successivo**
- Furto di Portatili
  - Permanente o temporaneo
  - Copia dischi fissi
  - Richieste estorsive

Operazioni Illegali

- Tampering e Data Diddling
  - Modificazioni minori ad archivi dati o file
  - Operazioni coperte
  - Dirette o tramite modifica programmi di gestione
    - **Tecniche di Salami Slicing**
- Defacement
  - Modifiche a pagine Web o archivi di pubblica utilità
    - **Scopi: scherzi, vanto, protesta politica, vantaggio concorrenziale, credibilità dell'azienda**
  - Tipi:
    - **Palese - defacement evidente**
    - **Credibile - informazioni false ma verosimili**

Operazioni Illegali

- Furto di Servizi o CPU
  - Inserimento account altrimenti a pagamento
  - Utilizzo tempo CPU per attività legali ma superflue
    - **Programmazione parallela**
  - Inserimento e attivazione server illegali
    - **Chat, Archivi FTP, Anonymous Remailers**
    - **Distributori di Virus e Cavalli di Troia**
  - Attivazione server in modalità Stand-by
    - **Stepping stones**
    - **Agenti di DDoS**
  - Inserimento bombe logiche o a tempo
    - **Dead man traps**

Importanza della Pianificazione di Difesa

  - Non esistono barriere perfette
- Sicurezza limitata nel tempo
  - **Un sistema è sicuro se può resistere ad un attacco per almeno il tempo necessario alla detezione e reazione a tale attacco**
- Rilassare i controlli d'accesso
  - Se si migliorano detezione e responso, si possono rilassare le protezioni
  - D'altronde non vi è assicurazione sull'efficacia della difesa senza capacità di detezione e reazione efficaci

$P_t < D_t + R_t$

Analisi del Rischio

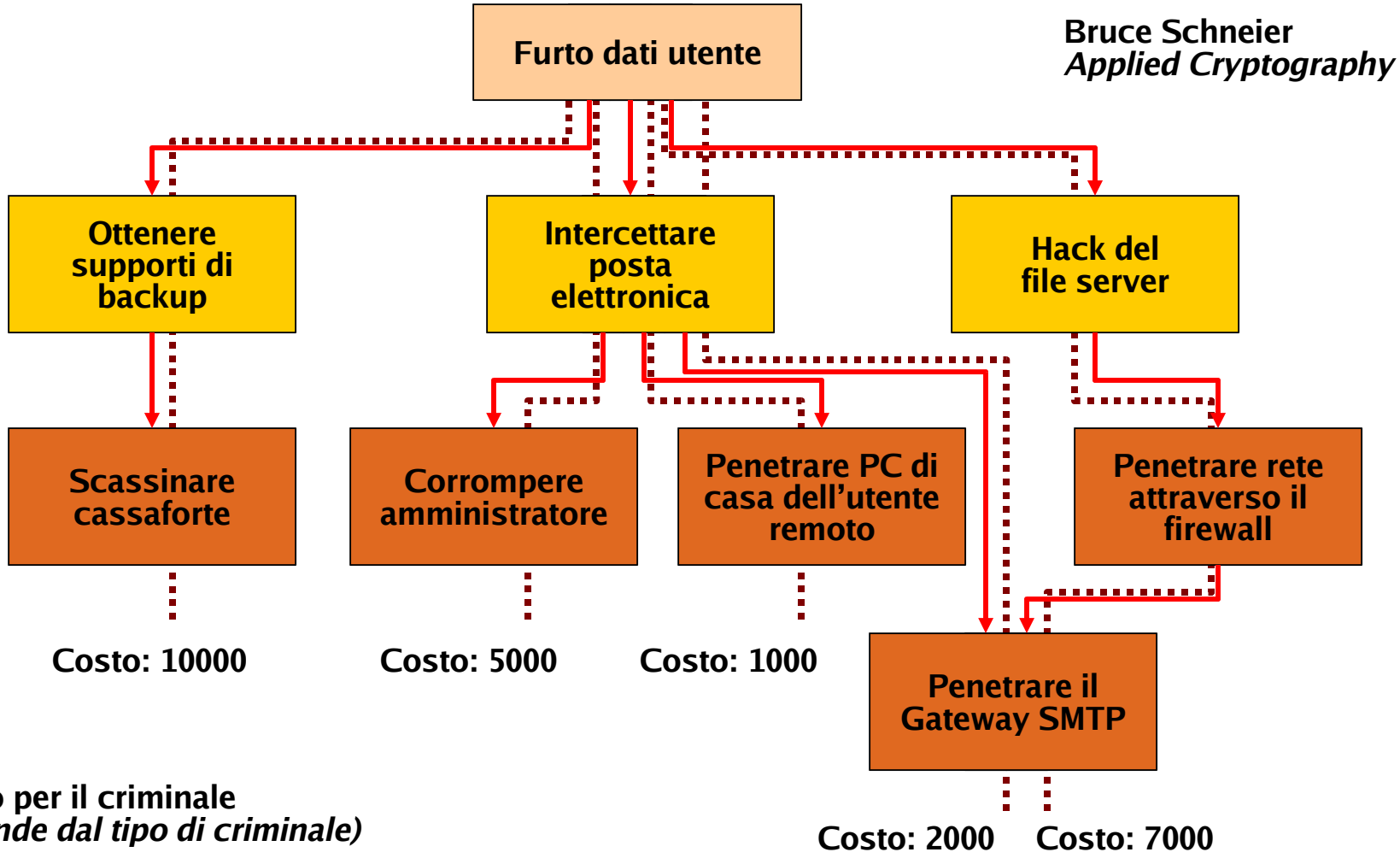
- Rischio
  - **Cosa può accadere?**
  - **Quanto è probabile?**
  - **Quali sono le conseguenze?**
- Analisi del Rischio
  - **Tecniche di valutazione quantitativa dei valori relativi delle misure protettive**
- Aspettativa Annuale di Perdita - Annual Loss Expectancy (ALE)
  - **e = valore atteso**
  - **p = probabilità annuale di perdita**
  - **v = valore corrente**

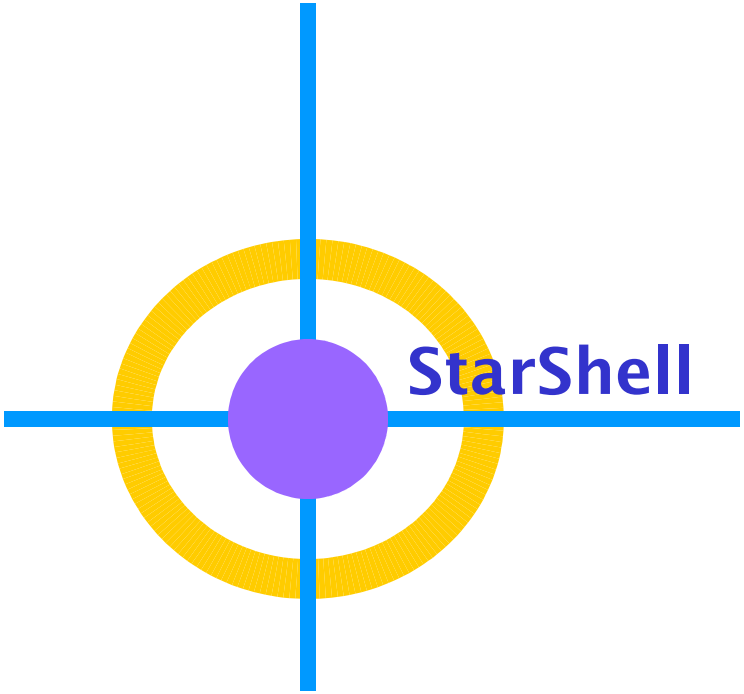
$$ALE = e = p\ v$$

Analisi del Rischio

- Metodologia di Cooper
  - **Identificare e valutare gli asset**
  - **Identificare le minacce**
  - **Identificare le vulnerabilità (come realizzare le minacce)**
  - **Stimare i rischi (probabilità di realizzare le minacce)**
  - **Calcolare lo ALE per ogni vulnerabilità**
  - **Identificare misure protettive**
  - **Estimate risks (probability of realizing threats)**
  - **Stimare la riduzione di ALE per ogni vulnerabilità causata dalle misure protettive**
  - **Selezionare le misure protettive più efficaci**
  - **Inserire componenti di esperienza – costi extra per la modifica delle misure protettive, per il disaster recovery e per perseguire i trasgressori**

Alberi di Attacco




StarShell