Rischi e vulnerabilità nelle applicazioni aziendali

Presentazione

Salvatore Capuano

Collaboratore scientifico SUPSI e
responsabile del
Microsoft .NET Competence Center

salvatore.capuano@supsi.ch

Obiettivi

- Sensibilizzare nei confronti della sicurezza applicativa
- Dimostrare come è facile minacciare un sistema vulnerabile

Programma

- Rischi e minacce
- Sicurezza applicativa
- Attacchi

Programma

- Demo
- Chi è a rischio?
- Cause e soluzioni
- Opportunità formative

Rischi e minacce

- Danni
- Furto
- Sabotaggio

Sicurezza

- Informatica
  - Infrastrutturale
    - Firewall, SSL,…
  - Applicativa
- Fisica
  - Porte, lucchetti,…
- Procedurale

Sicurezza

- Culturale
  - Password sotto la tastiera, liste di clienti nei cestini, lotterie fantasma…
  - Lavorare con diritti di AMMINISTRATORE!!!
    - Macchina dello sviluppatore :-S
    - Requisiti minimi: amministratore :-S

→ "Internet e il disordine globale", Alessandro Trivilini, dal 29 ottobre nelle maggiori librerie ticinesi

Applicazioni e Infrastruttura

- Devono essere considerate entrambe
- Spesso ci si focalizza solo sulla sicurezza infrastrutturale e si crede di aver risolto tutti i problemi ma…

False certezze

- Tanto c'è il firewall e SSL…
- Tanto i dati sono tutti criptati…
  - Algoritmi inefficienti
  - Chiavi banali
  - Chiavi non securizzate
  - Dati in chiaro mantenuti in memoria (garbage collector)
- Questi sono solo alcuni esempi…

Visione moderna della sicurezza

- Prima si securizzava la risorsa…
- Ora si securizza anche in base all'origine dell'applicazione
  - Locale
  - Intranet
  - Internet
  - Firmato
  - ….

Vediamolo meglio

Attacchi

Attacchi più comuni

- XSS
- SQL Injection
- Buffer Overrun
- DDOS
- Session Hijacking
- Password Cracking
- Reverse-engineering

DEMO

- XSS: « come sa di sale lo cookie altrui »
- Phishing: « pensavo fosse il mio sito invece era un calesse »
- SQL Injection: per entrare ho bisogno di un account? Aspetta: me ne creo uno io più bello del tuo! :-)
- BufferOverrun: guarda che ho una memoria d'elefante!

Chi è a rischio?

- Le aziende:
  - Le applicazioni interne all'azienda?

  → Tanto c'è il firewall…

  - Quelle accessibili dall'esterno?

  → Tanto c'è SSL

  - Chi vuoi che se la prenda con me?

  → Virus, dipendente scontento, errore umano,…

Cause dell'insicurezza

- Convizione che la sicurezza sia cara
- Sottovalutazione del problema
- Disattenzione da parte dello sviluppatore
- Tempi di sviluppo troppo ridotti
- Disegno dell'architettura
- La sicurezza informatica non è ancora una questione culturale

Soluzioni

- Utente tecnico:
  - Testare i sistemi prima di acquistarli (posso usare un sistema insicuro per attaccarne un altro)
  - Identificare le minacce e i rischi
  - FORMAZIONE FUNZIONALE
- Sviluppatore:
  - Sistemi di code review
  - Generatori di codice
  - Design architetturale difensivo
  - FORMAZIONE TECNICA

Tutto ciò, però, con misura…

Livello di sicurezza

- Il 100% non esiste
- Quanto securizzare?
  → Dipende dai rischi, dalle minacce e dai costi
- Un lucchetto qualsiasi riesce già a scoraggiare
- Un lucchetto più sicuro costa un po' di più

→ Ogni soluzione deve essere valutata

Perché costa di più?

- Il lucchetto più sicuro è costruito con:
  - Maggiore precisione
  - Materiali migliori
  - Tecnologia migliore
  - Esperienza maggiore

Opportunità formative

- Corso Postdiploma in Sicurezza informatica

  http://www.dti.supsi.ch

Opportunità formative

- Sulla sicurezza applicativa:
  - DTI 1.27 La sicurezza del software applicativo
  - DTI 1.28 Tecniche di Hacking
  - DTI 1.23 Sviluppo di sistemi per il web con tecnologie .NET
- Sicurezza infrastrutturale:
  - DTI 1.11 La sicurezza dei sistemi e delle reti
  - DTI 1.12 Laboratorio sicurezza delle reti e dei sistemi
  - DTI 1.24 Sicurezza nel Wireless
- Sicurezza informatica e gestione aziendale
  - DTI 1.29 Policies e documenti per la sicurezza informatica
  - DTI 1.31 CobiT® per il governo e il controllo dell'informatica

http://www.macs.supsi.ch/A_04_01_05.html

Conclusione

- La sicurezza è diventata una questione di sopravvivenza
- La mancanza di sicurezza è un pericolo reale
- Basta poco per non avere brutte sorprese
- La sicurezza è un processo

→ Le cose stanno cambiando: PI Schmidt all'assalto degli sviluppatori