Esempi reali di vulnerabilità

Le vulnerabilità come quella discussa nella sezione precedente sono pressoché infinite.
Alcuni altri esempi:

- Poisoned YouTube ads serve Caphaw banking trojan
- Second Anonymous member sentenced for role in DDoS attack
- Pre-installed security software leaves computers vulnerable to remote hijack, experts reveal

Spesso abbiamo fiducia nel software preinstallato, dimenticando che è soggetto a vulnerabilità come tutti gli altri.
Dobbiamo anche considerare gli aspetti mediatici della sicurezza.

Strumenti generali per la sicurezza

- **Crittografia**
  - simmetrica (DES, 3DES) e asimmetrica (RSA, DSA)
  - **Problema**: la cifratura ha un costo.
- **Policy**: insiemi di regole
  - privacy policy
  - access-control policy
- **Conoscenza (knoledge)**: conoscere una certa informazione da potere.
  - Password e PIN
  - Può anche tradursi come un vero e proprio oggetto di possesso (smartcard e smart token), oppure dati biometrici (impronte, iridi)
- **Programmi di protezione**
  - antivirus, IDS, firewall, DMZ, sandbox
- **Protocolli di sicurezza**
  - SSH, SSL
- **Sensibilizzazione dell'utente**
  - informazione, istruzione

Tutti questi strumenti, singolarmente e combinati insieme, hanno comunque dei limiti.

📝 **Domanda d'esame**: cos'è l'approccio **risk-based**?
Per un esempio di risposta leggere: Il risk-based thinking nella ISO 9001:2015

Misure di mitigazione, limiti degli strumenti e minacce: overview

Reference: slide del prof G.B., sezione limiti della crittografia e limiti dell'uso della password.

Una delle misure estreme di mitigazione del phishing è disattivare il sistema di preview (visto che la mail è spesso fatta in HTML è può contenere codice malevolo.)

Attacco a dizionario: consiste nel provare tutte le parole per violare una password

Euristica per mitigare: sostituire lettere con numeri che vi somigliano. Questo approccio non funziona se il dizionario utilizza una word list che prevede varianti della parola con numeri.

Misure di mitigazione per gli attacchi bruteforce

Utilizzo una soglia sul numero di inserimenti (rendono non fattibile il bruteforce) come misura preventiva.

Attacchi statistici: fatta analisi sulla vittima (social engineering), si intuisce quale password può aver scelto

Periodicità della password: quanto dura. Il cambio periodico di una password è esso stesso un protocollo di sicurezza. Per cambiare password c'è bisogno infatti di conoscere password vecchia.

Elenco di lettura e approfondimenti:

- Garante per la protezione dei dati personali