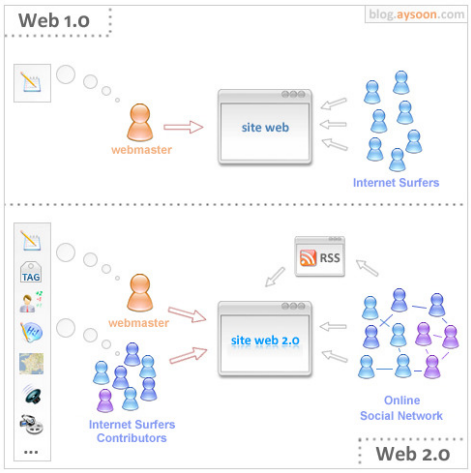
WEB 2.0

Pericolosità nella nuova frontiera del web

Introduzione al Web 2.0

- Usare la rete in maniera nuova e innovativa
- Condividereinformazioni
- Basato su di un concetto «opensource »
- Possibilità di interagire, gestire, integrarecontemporamente su piu' fonti
- Condividere, Mischiare, Riutilizzare
- Esempi: Facebook, Google Maps, Google Docs, Paypal, Flickr , Likedin

WEB 1.0 vs WEB 2.0



Pericolositàdel Web 2.0

(fonte IDC 2009 su 1300 IT)

- 95% delle aziende permette l'accesso a sitiweb 2.0 ritenendolenecessarie per il lorolavoro
  - 71% Wiki
  - 66% Facebook
  - 71% Linkedin
  - 87% Portali

Pericolositàdel Web 2.0

- **Information Leakage**

- Utentepuo' pubblicare delle informazioniritenutesensibili da parte dellasocietà;

- Difficilmentesipuo' arrivare a controllarequestotipodiinformazioni;

- Le informazionipossoessere replicate sutantissimisitiancheincosapevolmente;

Pericolositàdel Web 2.0

- **Phishing**

- Utilizzare un sito compromesso per veicolare unfinto sitomalevolo;

- Ricezioneedinstallazione di un widgetmalevolo via email;

Pericolositàdel Web 2.0

- **InsufficientAnti-Automation**

  - Sfruttandole particolaritàdel 2.0 si possonoautomatizzarealcuniattachi ex: Bruteforcing, CSRF (Cross site requestforgery);

Pericolositàdel Web 2.0

- **Information Integrity**

- Correttezza delle informazioni è unodeglielementifondamentali, compromendoalcuneinformazioni e modificandole si potrebberecrearedelladisinformazione;

Pericolositàdel Web 2.0

- **Cross Site Request Forgery (CSRF) / Cross Gadget Request Forgery (CGRF)**

  - Visitando un sitomalevolo o compromesso è possibiledirottare la vittima verso un sitoautorizzato e cambiare o rubareinformazioni;

Pericolositàdel Web 2.0

- **Cross Site Scripting (XSS)**

  - Sfruttandouna non corretta validazionedegli input è possibile far eseguirecodicescriptingall'utente; ex: rubareidentità, visualizzazione di finteinformazioni, redirezione verso siticontenti Web malware;

Considerazioni

- **Da tener presente che la maggioranza dei siti del Web 2.0 fa parte dei 50 più attivi dispensatori di malware**.
- Attualmente gli strumenti di protezione basati sulle segnalazioni della community sottostante come quelli implementati da YouTube e Blogspot risultano inefficaci nel quasi 80% dei casi

Futuro?

- Aumentare la sensibilità sul tema
- Coadiuvare gli sforzi necessari a bloccare questi veicoli di ingresso ex:

  - Società che sviluppato CMS / Portaili WEB 2.0, sanitizzazione degli input e maggiore attenzione al codice;
- Browser e strumenti sempre piu' intelligenti che riscono a riconoscere in maniera preventiva il «cattivo » ;