# Patch management

Metodi e strumenti per la Sicurezza informatica

Claudio Telmon
claudio@telmon.org

# Cos'è

- Il processo di acquisizione, verifica, test e installazione delle “patch”
  - Correzioni al software
- È uno dei processi di base della sicurezza informatica
- Problemi di base:
  - Costo del processo/centralizzazione
  - Compatibilità/opportunità delle patch
  - Tempistiche
  - Completezza

# Fonti

- Tutti i componenti possono avere bisogno di aggiornamenti
  - Apparati di rete, Sistemi operativi, supporti a runtime, applicazioni COTS e proprietarie...
- Dove reperire le informazioni?
  - Bollettini
  - Servizi
  - Accordi diretti
  - ...

# Reperire le patch

- Canali sicuri
  - Alternativa: firma
- Fornitura diretta
- Accesso diretto da parte degli outsourcer
  - Manutenzione in outsourcing

# Prima di applicare le patch

- Verifiche sulla necessità
  - Patch di grande impatto possono essere ritardate o evitate in funzione di una valutazione del rischio
  - La valutazione è specifica, non quella inclusa nei bollettini
- Verifiche di compatibilità
  - Anche per problemi di licenza
- Test
  - In ambiente di test
  - A volte su singoli elementi di un cluster (ma non sempre c'è compatibilità)

# Distribuzione

- In ambienti complessi si usano sistemi centralizzati
  - Serve un canale di accesso ai sistemi da gestire (critico)
- La distribuzione può andare male per molti motivi
  - Nonostante siano “tutti uguali' alla fine i sistemi sono tutti diversi
  - Serve una successiva verifica di cosa non ha funzionato
    - Feedback per il miglioramento continuo del processo

# Tempi

- Applicare la patch “appena possibile”?
  - Emergenza continua
  - Processo sempre “in corso”
  - Costoso...
- Scelta es. Microsoft: release mensili salvo eccezioni gravi
  - Compatibile con i tempi effettivi di applicazione delle patch
  - Spesso anche con i tempi di produzione delle patch

# Processo misurabile

- È relativamente semplice prendere delle misure sull'efficacia del processo:
  - Numero di sistemi gestiti vs. totale
  - Numero di sistemi all'ultimo livello di patch
  - Tempo medio di applicazione delle patch
  - Finestra di esposizione (a senso principalmente con il virtual patching)

# Virtual patching

- Consiste essenzialmente nell'utilizzare sistemi di intrusion prevention per intercettare gli attacchi riconducibili a una vulnerabilità e bloccarli, sopperendo all'indisponibilità o inapplicabilità della patch
- Si usano per ridurre la finestra di esposizione o per sopperire all'inapplicabilità, spesso a scopo di compliance