Centralizzazione, log e monitoraggio

Inventario

- È importante conoscere le risorse per controllarle:
  - Computer
  - Connessioni
  - Programmi
  - Account
  - Dati
  - Dati personali
  - Misure per dati particolari

Strumenti generali per la sicurezza

- Sono un presupposto per mantenere il controllo della rete
  - Non ha senso autenticare i propri utenti se poi è facile per un malintenzionato accedere ai dati
  - Alcuni strumenti di base sono richiesti almeno per i sistemi su cui sono trattati i dati personali (non solo i server o i client)
  - In generale sono necessari per tutelare il patrimonio e le attività dell'organizzazione

Strumenti centralizzati

- Sono il sistema più efficace per garantire una configurazione ed un aggiornamento corretti
  - Sistemi più uniformi, meno lavoro, maggiore efficacia
- Esempio tipico: antivirus centralizzato
  - Attenzione: è centralizzata la gestione, ma non basta un antivirus sul server di posta!

Come?

- Gli strumenti di gestione centralizzata sono i più efficaci e semplici da gestire
- Difficile l'integrazione con applicazioni proprietarie, ma non per tutte è necessario
  - Se non vi si trattano dati personali
  - Se non c'è interesse per l'organizzazione
- Per farlo (come per molti degli strumenti descritti) è necessaria un'infrastruttura affidabile

Log e monitoraggio

- I log hanno tre usi principali:
  - Debugging
  - Analisi
  - Compliance
- In tutti e tre i casi può essere utile un sistema centralizzato
  - Ma per la compliance è sostanzialmente indispensabile

Cosa loggare

- Debugging: soprattutto errori
  - Servono pochi dati personali; l'informativa può essere gestita insieme alla gestione dei ticket (nelle strutture più piccole, direttamente con l'utente)
  - Lo stesso per il consenso
- Analisi: i dati possono/devono essere anonimizzati
- Compliance: principalmente dati di accesso, quindi personali, da trattare come tali
  - Con alcuni requisiti in più, tipicamente “inalterabilità”

Retention

- Debugging: di solito molto breve, dell'ordine dei pochi giorni (tipicamente, rotazione a sette giorni)
- Analisi: tipicamente fino ad un mese, oltre solo dati anonimi e aggregati
- Compliance: da zero a 24 mesi, in funzione della normativa
- **Attenzione!** I dati non anonimi devono essere cancellati non appena non più necessari per gli scopi previsti (da informativa e consenso)

Soluzioni “monomarca”

- Ambiente *nix: sylog/syslog-ng
  - Ampiamente supportato anche da molti apparati
  - Syslog-ng supporta traffico TCP/TLS
  - Syslog: UDP non cifrato/autenticato
  - Supporto per multihup
- Ambiente Windows: con Windows Vista e Server 2008 è stato (finalmente!) introdotto Windows Remote Management
  - Supportato anche da XPSP2 e 2003
  - Traffico su http/https
  - Supporto per multihop e proxy

Infrastruttura tecnologica in ambiente eterogeneo

- Problemi principali
  - Le modalità di raccolta
  - I protocolli di trasmissione e la loro protezione
  - La normalizzazione dei dati
  - Le modalità di archiviazione e cancellazione
  - Le modalità di accesso
- Due filoni principali:
  - Prodotti proprietari
  - Prodotti/protocolli pubblici/diffusi

Modalità di raccolta

- Push o pop
  - Push: opera di un agente (es.syslogd, trap snmp, agente proprietario...)
    - Semplici da gestire per il server, throttling principalmente sul client
  - Pop: richieste dal log server via un servizio sul client (snmp, file via ftp, rpc...)
    - Più impegnative per il server, che però gestisce priorità e volumi

Protocolli

- Standardizzato syslog/syslog su TLS (RFC 5425)
  - Garanzia di integrità e riservatezza
  - Possibilità di rilevare la disconnessione
- Protocolli proprietari
  - Spesso non vengono date garanzie o usano anche loro TLS

Normalizzazione dei dati

- Non esiste uno standard neppure per il formato (a parte facility/severity di syslog, RFC 5427)
- Non sembra facile arrivarci
  - Diversi tentativi, tutti falliti
  - Lo stesso syslog ha un formato non strutturato
- Prodotti proprietari: elenco degli specifici prodotti supportati
  - Vengono normalizzati “conoscendo il prodotto”
  - Possibilità di definire delle tracce personalizzate
  - Difficile comunque, perché un singolo prodotto può usare molte tracce diverse (o nessuna)

Modalità di archiviazione

- DBMS e query per la consultazione
  - Standard, portabili
  - es. syslog-ng e mysql
- Scrittura diretta sul disco
  - Più efficienti per grandi volumi, non portabili (dipendenza dal prodotto)
- Storicizzazione
  - Dipende dal prodotto, molti prevedono solo una modalità “online” e cancellazione “manuale” dei record oltre una scadenza
- Le modalità di cancellazione sono critiche per la conformità!

Accesso

- Tipicamente, possibilità di definire query anche con espressioni regolari
- I prodotti generalmente forniscono dei set predefiniti per i prodotti supportati
- La difficoltà è data dalla mancanza di normalizzazione
- Non è un vero problema per la compliance:
  - Viene richiesto principalmente di conservarli e averli a disposizione, non di fare ricerce
  - Interessano principalmente i log di accesso, sono pochi tipi

Rapporto con i processi aziendali

- Quando l'attività di monitoraggio ha lo scopo di individuare attività fraudolente, è importante ragionare sul processo aziendale
- Servono strumenti che possano incrociare i dati in modo intelligente
  - Più complesso che fare semplici query
- Generalmente personalizzati

Le risorse umane

- La gestione di allarmi è solo in parte una soluzione
  - Falsi positivi
  - Conoscenza a priori di cosa segnalare
- Serve un approccio intelligente
- Non è un'attività a tempo pieno se non in grandi strutture
  - Ma se messa in carico a chi “fa altro”, finisce in coda alle priorità