IS AUDITING PROCEDURE

INTRUSION DETECTION SYSTEM (IDS) REVIEW

Romeo Costanzo – IT Telecom (Gruppo Telecom Italia)
CISA, CCNA, SCJP

Information Systems Audit and Control Association

Agenda

- **L'aspetto tecnologico**
- **Le procedure di verifica**
- **Conclusioni**

Alcune definizioni (1)

- Intrusione: un insieme di azioni atte a compromettere la confidenzialità, integrità e disponibilità di una risorsa
- IDS: componenti SW/HW che automatizzano il processo di analisi degli eventi rilevanti su sistemi elaborativi e segmenti di rete allo scopo di individuare, possibilmente real time, utilizzi non consentiti dei sistemi

Alcune definizioni (2)

- L'accuratezza di un IDS è compromessa quando viene erroneamente rilevata un'intrusione ("falsi positivi")
- La completezza riflette il numero di falsi negativi (quando l'IDS non riesce ad identificare un'intrusione reale).

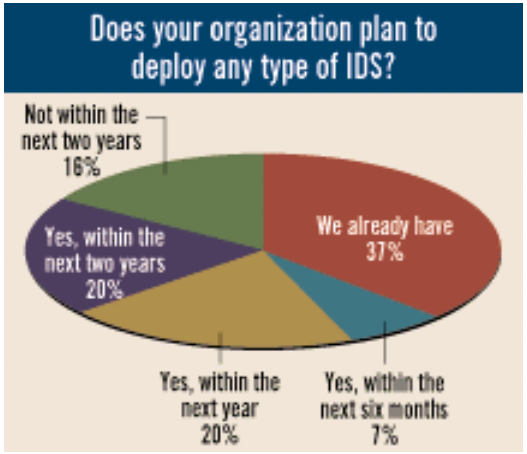
Perché gli IDS ?

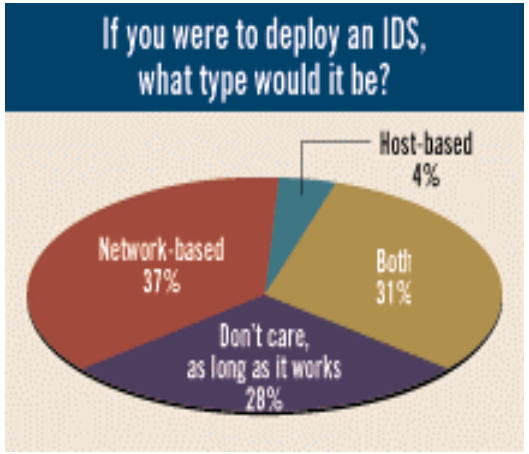
Sono in rapido aumento (Report su Attack Trends - CERT):

- Il livello di automazione negli strumenti usati per gli attacchi ed il loro livello di sofisticazione
- La velocità con la quale si scoprono nuove vulnerabilità nei sistemi (raddoppia ogni anno)
- La “permeabilità” dei firewall
- Le minacce di tipo “asimmetrico” (ossia la catena della sicurezza è sempre più dipendente dal suo anello più debole)
- Le minacce provenienti dalle infrastrutture

Adelante Pedro ....

Gli IDS costituiscono una delle tecnologie di sicurezza informatica su cui attualmente si stanno concentrando interesse, ricerca e investimenti, ma ....





Fonte: http://www.networkcomputing.com/

.... con juicio !!!

Gartner Group [agosto 2002]:

- L'"Intrusion Prevention" sostituirà l'"Intrusion Detection".
- Le aziende dovrebbero aspettare prima di effettuare nuovi importanti investimenti in IDS – che non hanno fornito sicurezza aggiunta – finché non emergeranno degli IPS (Intrusion Prevention Systems) in grado di offrire maggiori difese contro i "cyberattacks."
- I problemi con gli IDS che emettono falsi allarmi o non rilevano attacchi ne hanno eroso il valore. La disponibilità di piattaforme elaborative più veloci e tecniche più avanzate condurranno il mercato degli IDS dalla *Detection* alla *Prevention*.

Aberdeen Group [2003 Predictions for Security & Privacy]

- I Network IDS basati sull'analisi ed il matching del traffico di rete risultano sconfitti dal loro peso e dai loro incomprensibili file di log. Le aziende con IDS di prima generazione decidono di tagliare le perdite nel 2003, invece di continuare ad investire tempo e denaro in quest'area.

Principali tipi di IDS

- IDS Network-Based: analizzano il traffico di rete (sono sostanzialmente “sniffer”).
- IDS Host-Based: analizzano varie fonti di informazioni (ad es. audit logs) forniti dai SO per rilevare intrusioni.

IDS Network-Based

- Basati sull'interpretazione del traffico di rete (analisi di basso livello); si tratta in sostanza di "sniffer", che ottengono copie dei pacchetti che viaggiano in rete senza tener conto della loro destinazione (una normale scheda di rete – NIC – legge solamente i pacchetti a lei indirizzati).
- Un IDS network-based consiste in un insieme di sensori o host installati in vari punti di una rete

Strategie di analisi

Due approcci principali:

- Misuse Detection (o “Signature Analysis”): analisi di eventi che corrispondono a pattern predefiniti di attacchi noti
- Anomaly Detection: analisi di un qualsiasi scostamento dal profilo di normalità definito per un sistema

Misuse Detection: pro & contro

- Vantaggi
  - Efficaci nel rilevare attacchi senza dar luogo ad un numero elevato di falsi allarmi.
  - Possono fornire informazioni di dettaglio sullo specifico attacco usato.
- Svantaggi
  - Capaci di rilevare solo gli attacchi noti.
  - Sfuggono anche tutte le varianti degli attacchi noti

Anomaly Detection: Pro & contro

- Vantaggi
  - Possono rilevare attacchi non noti.
  - Sono potenzialmente in grado di fornire le informazioni che servono per definire le signatures da utilizzare per la Misuse Detection.
- Svantaggi
  - Producono un elevato numero di falsi allarmi dovuti a comportamenti imprevedibili di utenti, reti e sistemi di elaborazione.
  - hanno bisogno di un “training” per imparare quale sia il comportamento “normale” del sistema.

Possibili reazioni

- Reset della sessione TCP
- Modifica delle “regole” del firewall
- Invio di allarmi verso le console di management

IDS Network-Based: Pro & contro

- Vantaggi
  - Pochi IDS di questo tipo ben posizionati possono controllare una rete di ampie dimensioni
  - Il deployment è facile e non ha impatti sulla rete.
- Svantaggi
  - Non possono analizzare informazioni cifrate (sessioni SSL, IPSEC, SSH, ...).
  - Possono solamente rilevare che un attacco è iniziato.
  - Possono essere soggetti ad attacchi (gli IDS sono inerentemente sensibili ad attacchi DoS)

Information Systems Audit and Control Association

IDS Host-Based

- Operano su host protetti.
- Utilizzano informazioni fornite dal SO (ad es. audit trials e system logs).
- Analizzano le attività con affidabilità e precisione determinando con esattezza processi e utenti coinvolti
- Vanno bene nel caso di attacchi da parte di utenti locali.

IDS Host-Based: pro & contro

- Vantaggi
  - Possono rilevare attacchi che non vengono “visti” al livello della rete.
- Svantaggi
  - Usano le risorse computazionali delle macchine su cui sono installati.
  - Difficili da gestire
  - Non adatti per attacchi il cui target è l’intera rete e non la singola macchina.

Qual è la soluzione ?

- Le due tecniche vengono spesso combinate per ottenere una maggiore efficacia

Gli IDS sono vulnerabili ! (1) L'insertion attack

- Un IDS può accettare un pacchetto che il sistema di destinazione scarta (perché ad esempio malformato; ad es. con un errore nel checksum UDP, oppure un campo TTL insufficiente per raggiungere la destinazione).
- Un hacker può sfruttare questa situazione inviando pacchetti verso tale destinazione (dove i pacchetti verranno scartati), con l'IDS che invece pensa che siano validi
- Nell'effettuare ciò, l'attaccante inserisce dati nell'IDS a cui nessun altro sistema nella rete è interessato
- Funziona quando l'IDS è meno rigido dell'end-system nell'elaborazione dei pacchetti

Gli IDS sono vulnerabili ! (2) L'evasion attack

- È l'opposto del precedente
- Un end-system può accettare un pacchetto che l'IDS scarta. In tal caso, il pacchetto si sta sottraendo all'analisi da parte dell'IDS
- il risultato è che l'IDS rimane inattivo in caso di attacchi di questo tipo.

Gli IDS sono vulnerabili ! (3) Frammentazione

- vari IDS (ma anche dispositivi che effettuano filtraggio a livello di pacchetto) non supportano il “packet reassembly” e perciò non rilevano o bloccano attività quando la “signature” è suddivisa su più datagrammi.
- Attacchi DoS spesso fanno uso di traffico altamente frammentato per esaurire le risorse di sistema

Information Systems Audit and Control Association

Procedure di verifica

Pianificare la verifica

Individuare e comprendere:

- la missione dell'azienda e i suoi obiettivi di business;
- grado e maniera in cui i SI supportano l'azienda
- ruoli e responsabilità nell'ambito della gestione degli IDS

Sviluppare e condividere gli obiettivi indirizzando i sette Information Criteria del CobiT: efficacia, efficienza, confidenzialità, integrità, disponibilità, conformità e affidabilità delle informazioni.

Information Systems Audit and Control Association

Posizionare l'IDS nell'architettura di rete

- Determinare i segmenti di rete da monitorare sulla base della collocazione degli asset critici
- Valutare l'impatto sul business di un attacco di tipo DoS sui server e le applicazioni a rischio

Verificare i parametri di installazione

Fornire una ragionevole garanzia che:

- L'IDS sia configurato per rilevare modifiche sospette di file e DB oppure aggiunte di file al sistema
- Siano stati messi a punto filtri basati su una security policy per minimizzare il problema dei falsi positivi

Information Systems Audit and Control Association

Verificare le relazioni con i Firewall

- Fornire la ragionevole garanzia che vengano intraprese azioni appropriate in caso di intrusione. L'approccio base per la risposta ad un attacco portato via rete include i seguenti passi: preparazione, rilevamento, contenimento, risoluzione, recovery e follow-up
- Le procedure di Incident Response vanno sviluppate di pari passo con la diffusione in esercizio dell'IDS

Information Systems Audit and Control Association

Altro

Va verificato se:

- Esistono connessioni di rete non autorizzate effettuate tramite modem (rogue modems)
- Esistono installazioni di SW che creano esposizioni (back-orifice, spyware, ...)
- Gli allegati di posta contenenti “codice malevolo” vengono intercettati
- Vengono impediti gli accessi a URL che pongono minacce di sicurezza

Information Systems Audit and Control Association

Effettuazione dell'Audit

- Documentare il processo e i flussi di dati
- Identificare e testare i controlli sull'IDS
- Verificare se nelle procedure di Incident Response sono coinvolte terze parti
- Verificare il periodo di aggiornamento delle signature
- Effettuare altre verifiche tecniche sugli IDS (lista nella procedura)

Information Systems Audit and Control Association

Reporting

- le debolezze riscontrate nell'IDS, dovute o all'assenza di controlli o alla loro inadeguatezza, vanno riportate al management in modo che possano essere intraprese azioni correttive immediate
- Andrebbero incluse nel report le raccomandazioni per il miglioramento del sistema dei controlli

Conclusioni

- Il veloce aumento degli attacchi portati a sistemi e reti richiede ulteriori strumenti per una risposta efficace.
- Gli IDS, osannati da alcuni criticati da altri, possono aiutare a fronteggiare le minacce ...
- ... ma solo se posizionati, configurati, verificati nella maniera corretta. Il lavoro di audit, mai come in questo caso, può fare la differenza !

Information Systems Audit and Control Association

Grazie per l’attenzione !

Riferimenti

- IS Auditing Procedure – Intrusion Detection System (IDS) Review - ISACA
- Northcutt, Stephen – Novak, Judy *Network Intrusion Detection – An Analyst's Handbook* New Riders, 2001
- Dailey Paulson, Linda *Stopping Intruders Outside the Gates* IEEE Computers, novembre 2002
- *Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection* Secure Networks, Inc. 1998
- Martin, Steve *Anti-IDS Tools and Tactics* SANS Institute - agosto 2001
- Bace, Rebecca – Mell, Peter *Intrusion Detection Systems* NIST Special Publication on IDS
- Carty, Aidan – *Building an IDS solution using SNORT* Entropy Ltd.
- RFC1858 *Security Considerations for IP Fragment Filtering* 1995