Πανεπιστήμιο Μακεδονίας
ΠΜΣ Πληροφοριακά Συστήματα
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων
Υπεύθυνος Καθηγητής: Α.Α. Οικονομίδης
economid@uom.gr

ΑΝΑΛΥΣΗ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΙΣΒΟΛΗΣ (NIDS) & ΣΥΓΚΡΙΣΗ ΔΙΑΘΕΣΙΜΩΝ ΕΜΠΟΡΙΚΩΝ ΠΑΚΕΤΩΝ

ΚΑΤΣΙΚΑΣ ΔΗΜΗΤΡΗΣ
15 Φεβρουαρίου, 2002

ΘΕΣΣΑΛΟΝΙΚΗ 2002

University of Macedonia
Master Information Systems
Network Technologies
Professor: A.A. Economides
economid@uom.gr

NETWORK INTRUSION DETECTION SYSTEMS (NIDS) ANALYSIS & COMMERCIAL/SHAREWARE TOOLS COMPARISON

KATSIKAS DIMITRIS
February 15, 2002

THESSALONIKI 2002

ΠΕΡΙΛΗΨΗ

Ο σκοπός ενός **Συστήματος Ανίχνευσης Ηλεκτρονικών Εισβολών** (ή IDS) είναι να εντοπίζει είτε την μη εξουσιοδοτημένη πρόσβαση ή την εσφαλμένη χρησιμοποίηση ενός πληροφοριακού συστήματος. Σε γενικές γραμμές τα **Συστήματα Ανίχνευσης Ηλεκτρονικών Εισβολών** αποτελούν ένα είδος συμβατικού συναγερμού για τα συστήματα υπολογιστών. Στην πραγματικότητα μπορούν να παράξουν προειδοποιητικούς ήχους ενώ πολλές φορές προβαίνουν σε διορθωτικές κινήσεις, αν και αφόσον εντοπιστεί κάποιος εισβολέας στο σύστημα.

Είναι απαραίτητο να επισημανθεί ότι ένα Σύστημα Ανίχνευσης Ηλεκτρονικών Εισβολών δεν υποκαθιστά την λειτουργία ενός firewall. Στην ουσία αποτελεί μια αυτόνομη λειτουργική μονάδα που ολοκληρώνεται μέσα στο γενικότερο σύστημα ασφαλείας μίας επιχείρησης με σκοπό να συμπληρώσει τις διαδικασίες ασφαλείας ενός firewall. Κατά συνέπεια αποτελεί μια *πρόσθετη* ασφαλιστική δικλείδα η οποία απαντάται συνήθως σε επιχειρήσεις με πολύπλοκη δικτυακή τοπολογία και αυξημένο αριθμό κατανεμημένων δικτυακών στοιχείων.

Παρότι έχουν αναπτυχθεί πολλαπλά και διαφορετικά **Συστήματα Ανίχνευσης Ηλεκτρονικών Εισβολών**, οι τακτικές ανίχνευσης περιορίζονται σε δυο γενικές κατηγορίες, τον εντοπισμό «ανωμαλιών» και την «εσφαλμένη χρήση». Οι ανιχνευτές ανωμαλιών αναζητούν συμπεριφορές οι οποίες αποκλίνουν από την καθιερωμένη χρήση ενός υπολογιστικού συστήματος. Οι ανιχνευτές εσφαλμένης λειτουργίας εξετάζουν συμπεριφορές οι οποίες φαίνεται να ακολουθούν κάποιο από τα γνωστά σενάρια επίθεσης.

Τα τελευταία χρόνια καταβάλονται σημαντικές προσπάθειες και έχουν επενδυθεί σημαντικά κεφάλαια πάνω στα **Συστήματα Ανίχνευσης Ηλεκτρονικών Εισβολών**, τόσο σε ερευνητικό επίπεδο όσο και επίπεδο εμπορικών εφαρμογών, λόγω της επιδημικής αύξησης της ηλεκτρονικής εγκληματικότητας.

SUMMARY

The purpose of an **intrusion detection system** (or IDS) is to detect unauthorized access or misuse of a computer system. **Intrusion detection systems** are kind of like burglar alarms for computers. They sound alarms and sometimes even take corrective action when an intruder or abuser is detected.

It is absolutely necessary to make cleat that an Intrusion Detection System does not substitute *firewall* functionality. In fact an IDS is an independent functional unit that is integrated in the corporate general security framework in order to fill in the security procedures of the firewall. Consequently, an IDS provides a further enforcement in the security policy which we most often meet in complicated network topologies containing large number of network elements.

Many different **intrusion detection systems** have been developed but the detection schemes generally fall into one of two categories, *anomaly* detection or *misuse* detection. Anomaly detectors look for behaviour that deviates from normal system use. Misuse detectors look for behaviour that matches a known attack scenario.

The latest years a great deal of time, effort and money has been invested in **intrusion detection**, in research projects as well as in commercial implementation level, due to the epidemical increment of electronic crime.

ΠΕΡΙΕΧΟΜΕΝΑ

CONTENTS

ΑΝΑΛΥΣΗ IDS

1. Τι είναι το Σύστημα Ανίχνευσης Ηλεκτρονικών Εισβολών

Με τον όρο **«εισβολέα»** χαρακτηρίζουμε κάποιον ο οποίος προσπαθεί να διαρρήξει ηλεκτρονικά ή να προκαλέσει ανεπιθύμητες λειτουργίες σε ένα πληροφοριακό σύστημα. Ο όρος *ανεπιθύμητες λειτουργίες* είναι προφανώς ευρύτατος και ενδέχεται να σημαίνει είτε κλοπή απόρρητων εγγράφων/πληροφοριών είτε στην απλούστερη μορφή υποκλοπή της ηλεκτρονικής αλληλογραφίας για διαφημιστικούς και μόνο λόγους (spamming technics). Οι ορολογίες που χρησιμοποιούνται σήμερα για τους εισβολείς είναι hackers, crackers, sniffers κτλ., ανάλογα με την σκοπιμότητα του καθενός. Κατά συνέπεια, τα **Συστήματα Ανίχνευσης Ηλεκτρονικής Εισβολής** (IDS) είναι τα εργαλεία εκείνα τα οποία επιτρέπουν τον εντοπισμό των εισβολέων. Για να γίνει κατανοητή η λειτουργία των IDS, μπορούμε να θεωρήσουμε της εξής βασικές κατηγορίες:

- **Network intrusion detection systems (NIDS) – *Ανιχνευτές Εισβολής Δικτύου***

  Εποπτεύουν και καταγράφουν όλα τα πακέτα που κυκλοφορούν στα σύρματα του υπο παρακολούθηση δικτύου και επιχειρούν να ανιχνεύσουν αν κάποιος εισβολέας προσπαθεί να διαρρήξει κάποιο στοιχείο του δικτύου (ή να προκαλέσει την πλέον διαδεδομένη *Επίθεση Κατάργησης Εξυπηρέτησης – Denial of service Attack*). Χαρακτηριστικό παράδειγμα είναι ένα τέτοιο σύστημα που παρακολουθεί μεγάλους αριθμούς αιτημάτων σύνδεσης σε πολλαπλές πόρτες ενός στοιχείου δικτύου (SYN) , που σημαίνει ότι κάποιος επιχειρεί να ανακαλύψει τα τρωτά σημεία του δικτύου (port scanning). Ενα NIDS μπορεί να εγκατασταθεί είτε σε ενα και μόνο στοιχείο/υπολογιστή που παρακολουθεί την κίνηση από και προς τον εαυτό του (τότε είναι συνήθως ολοκληρωμένο με τον σωρό και τις υπηρεσίες/services αυτές καθαυτές), είτε να λειτουργεί αυθαίρετα σε ένα ανεξάρτητο υπολογιστικό σύστημα το οποίο παρακολουθεί την κίνηση ενός δικτύου συνολικά (δηλ σε ένα hub, router κτλ.). Στην ουσία οι Ανιχνευτές Εισβολής Δικτύου αποσκοπούν στην συνολική παρακολούθηση ενός δικτύου και είναι τα πιο δημοφιλή IDS.

  *Από όλες τις κατηγορίες των IDS οι **Ανιχνευτές Εισβολής Δικτύου – NIDS** είναι αυτοί που θα μας απασχολήσουν – οι υπόλοιπες κατηγορίες αναφέρονται με σκοπό την ολοκληρωμένη παρουσίαση του θέματος.*

- **System integrity verifiers (SIV) – *Πιστοποιητές Ακεραιότητας Συστήματος***

  Αυτοί παρακολουθούν τα αρχεία του συστήματος με σκοπό να διαπιστώσουν εάν κάποιος εισβολέας τα έχει μεταβάλλει. Ενας SIV μπορεί να παρακολουθεί και άλλα συστατικά ταυτόχρονα, οπως για παράδειγμα την registry των windows, ώστε να πιστοποιήσει την ορθότητα των εγγραφών σε αυτή. Μπορεί ακόμα να εντοπίσει κάποιον απλό χρήστη ο οποίος επιχειρεί να αποκτήσει δικαιώματα γενικού διαχειριστή στο σύστημα (administrator). Τα περισσότερα υπάρχοντα προϊόντα μάλλον πρέπει να τα εκλάβουμε ως απλά εργαλεία και όχι ως ολοκληρωμένα συστήματα, όπως για παράδειγμα ένα από τα πιο διαδεδομένα SIV το *Tripwire* το οποίο ανιχνεύει μεν μεταβολές σε βασικά στοιχεία ενός συστήματος αλλά αδυνατεί να παράξει προειδοποίηση εισβολής σε πραγματικό χρόνο.

- **Log file monitors (LFM) – Επόπτες Αρχείων Ημερολογίου**

  Παρακολουθεί τα αρχεία ημερολογίου που παράγονται από τις υπηρεσίες δικτύου (network services). Με ένα παρόμοιο τρόπο με τους Ανιχνευτές Δικτύου, τα συστήματα αυτά αναζητούν κάποιο από τα γνωστά σχέδια επίθεσης μέσα στα αρχεία ημερολογίου. Κλασσικό παράδειγμα τέτοιου συστήματος θα ήταν ένας parser που αναλύει τα αρχεία ημερολογίου ενός Web Server, αναζητώντας εγγραφές που να καταδεικνύουν προσπάθειες για εκμετάλλευση των τρωτών σημείων ασφαλείας, όπως την εκτέλεση εντολής κελύφους (shell cmd: dir, del, run, κτλ) μέσω προτωκόλου HTTP!

- **Deception systems – Συστήματα Παραπλάνησης**

  Τα συστήματα αυτά εμπεριέχουν ψευδο-υπηρεσίες (pseudo-services), σκοπός των οποίων είναι να προσομοιώσουν διαδεδομένα κενά ασφαλείας, με σκοπό να παγιδεύσουν τους εισβολείς. Ενας τέτοιος τρόπος παραπλάνησης είναι η μετονομασία του γενικού διαχειριστή του συστήματος (administrator), η δημιουργία ενός παραπλανητικού λογαριασμού (dummy account) με περιορισμένα δικαιώματα.
  Βέβαια αυτό που παραμένει θολό σε ότι αφορά την χρήση τέτοιων συστημάτων είναι, για ακόμη μια φορά, το θεσμικό πλαίσιο.

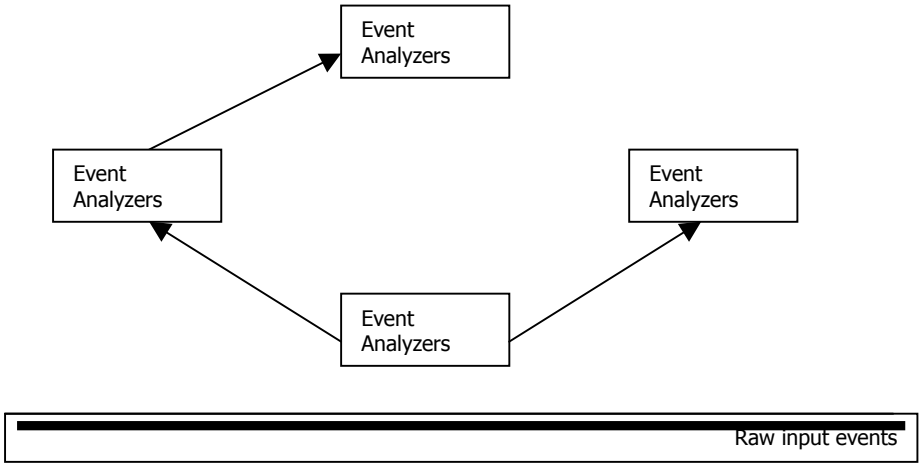
2. Αρχιτεκτονική ενός Συστήματος Ανίχνευσης Ηλεκτρονικών Εισβολών

Παρά τις διαφορές που παρατηρούμε σε διάφορα εμπορικά πακέτα (το καθένα έχει δικά του χαρακτηριστικά και λειτουργικότητα), η βασική αρχιτεκτονική φαίνεται να είναι παρόμοια από πολλές απόψεις. Ενα σύνολο αρχών που περιγράφει ικανοποιητικά του Ανιχνευτές Ηλεκτρονικής Εισβολής είναι το **«Κοινό Πλαίσιο Ανίχνευσης Εισβολών»** - ***Common Intrusion Detection Framework (CIDF)***. Το CDIF αναπτύχθηκε από μια ομάδα εργασίας ο αρχικός σχηματισμός της οποίας προέκυψε από την συνεργασία ανάμεσα στην **DARPA** (Defence Advanced Research Projects Agency) η οποία χρηματοδοτούσε σχετικά προγράμματα και τους οργανισμούς/ινστιτούτα που ανταπροκίθηκαν σε αυτά τα προγράμματα. Η σχεδιαστική αρχή του CIDF είναι να αναπτύξει ένα σύνολο προδιαγραφών που να επιτρέπουν την συνεργασία και τον διαμοιρασμό πληροφοριών μεταξύ των διαφόρων αντικειμένων **Ανίχνευσης Εισβολής και Αμεσης Απόκρισης (IDR)** και ακόμα να επιτρέψουν τη λειτουργία διαφορετικών Υποσυστημάτων IDR σε περιβάλλοντα διαφορετικά από αυτά για τα οποία σχειδάστηκαν.

Το CDIF ορίζει τέσσερα βασικά σημεία αντικείμενα:

- Γεννήτριες γεγονότων – event generators (E-boxes)
- Αναλυτές γεγονότων – event analyzers (A-boxes)
- Βασεις Δεδομένων γεγονότων – event databases (D-boxes)
- Μονάδες Απόκρισης γεγονότων – event response units (R-boxes)

Τα αντικείμενα αυτά φαίνονται στο σχήμα 1



Σχήμα 1

Οι *γεννήτριες γεγονότων* λαμβάνουν πληροφορίες από πηγές γεγονότων μέσα από το υπολογιστικό σύστημα. Τα γεγονότα αυτά μπορούν να προέρχονται από στοιχεία του δικτύου, από εφαρμογές ή οποιοδήποτε αλλο αντικείμενο που μας ενδιαφέρει. Τα γεγονότα αυτά συλλέγονται και μετασχηματίζονται σε μια κοινής αποδοχής μορφοποίηση (format) την gido που έχει επιλεχθεί για λόγους συμβατότητας.

Οι *αναλυτές γεγονότων* λαμβάνουν πληροφορίες (gidos) από τα άλλα αντικείμενα και επιχειρούν να αναλύσουν τα δεδομένα, αναζητώντας ασφαλώς πιθανές εισβολές. Για τον σκοπό αυτό μπορούν να χρησιμοποιηθούν πολλαπλοί μηχανισμοί όπως η στατιστική ανάλυση και η αναγνώριση προτύπων αναζητώντας ακολουθίες γεγονότων.

Η αποθήκευση γεγονότων και πληροφοριών (gidos) γίνεται με τις *βάσεις δεδομένων γεγονότων.* Τόσο τα γεγονότα χαμηλού επιπέδου (raw events) όσο και τα υψηλού επιπέδου (που έχουν μεταφραστεί από τους αναλυτές) είναι θεμιτό να αποθηκεύονται σε μόνιμη βάση (persistent).

Οι *μονάδες απόκρισης* λαμβάνουν τις πληροφορίες αυτές που σχετίζονται με την ασφάλεια του συστήματος και εκκινούν τον αντίστοιχο μηχανισμό απόκρισης για να ματαιώσουν ή να αποτρέψουν κάποια ηλεκτρονική επίθεση. Πιθανές αποκρίσεις είναι ο τερματισμός συγκεκριμένων λειτουργιών (killing processes), ο επαναπροσδιορισμός των συνδέσεων και η αλλαγή των δικαιωμάτων πρόσβασης στα αρχεία του συστήματος.

Οπως προαναφέραμε παρά την διαφοροποίηση που παρατηρείται στις αρχιτεκτονικές των Ανιχνευτών Ηλεκτρονικών Εισβολών, τα περισσότερα από τα υπάρχοντα τέτοια συστήματα είναι συμβατά σε κάποιο βαθμό με το πλαίσιο CIDF!

3. Κριτήρια σύγκρισης Ανιχνευτών Ηλεκτρονικής Εισβολής

Πριν να προχωρήσουμε στην αναλυτική σύγκριση των πιο δημοφιλών Ανιχνευτών Ηλεκτρονικών Εισβολών κρίνεται σκόπιμη μια σύντομη αναφορά στα κριτήρια αξιολόγησης τους, τα οποία ασφαλώς προσδιορίζουν την συνολική εικόνα ενός Ανιχνευτή Ηλεκτρονικών Εισβολών.

Τα κριτήρια αυτά είναι τα εξής:

- ✓ **Κατάτμηση των δεδομένων επεξεργασίας – Granularity of data processing**

  Ο χρόνος απόκρισης ενός IDS εξαρτάται εν μέρει στη κατάτμηση των δεδομένων επεξεργασίας. Η επεξεργασία των δυαδικών δεδομένων που συλλέγονται μπορούν να γίνει είτε συνεχώς είτε κατά ομάδες ανα τακτά χρονικά διαστήματα.

- ✓ **Πηγή Ελέγχου Δεδομένων – Source of audit data**

  Η πηγή ελέγχου των δεδομένων μπορεί να είναι είτε δικτυακή είτε να βασίζεται στα τερματικά. Τα δικτυακά δεδομένα διαβάζονται συήθως απευθείας από κάποιο δίκτυο multicast π.χ Ethernet. Τα δεδομένα με βάση τα τερματικά (αρχεία ασφάλειας) συλλέγονται από τα επιμέρους τερματικά που είναι κατανεμημένα στο δίκτυο και μπορούν να περιέχουν τα αρχεία του πυρήνα του λειτουργικού συστήματος, τα αρχεία χρήσης των εφαρμογών και τα αρχεία υλικού του δικτύου. Ενα πλεονέκτημα της δικτυακής πηγής ελέγχου είναι ότι επιτρέπει στον ανιχνευτή ηλεκτρονικών εισβολών να παρακολουθεί εξολοκλήρου την κίνηση των πακέτων μέσα στο δίκτυο (NIDS). Με αυτό τον τρόπο δεν περιορίζεται να ελέγχει τα δεδομένα που προορίζονται προς τον εαυτό του ή προς κάποιο αλλο τερματικό. Βέβαια η ενίσχυση της κρυπτογράφησης των δικτυακών δεδομένων καθιστά τον ελεγχο των δεδομένων δικτυακά εντελώς άχρηστο.

- ✓ **Μέθοδος Ανίχνευσης – Detection method**

  Η μέθοδος ανίχνευσης αφορά στον μηχανισμό με τον οποίο αναλύονται τα ελεγχόμενα δεδομένα με σκοπό την εύρεση μη εξουσιοδοτημένης πρόσβασης ή μη κανονικών συμπεριφιρών μέσα στο σύστημα. Υπάρχουν δυο διαφορετικές προσεγγίσεις στην ανίχνευση ηλεκτρονικών εισβολών που χρησιμοποιούνται ευρέως: *βάσει κανόνων(rule based)* και *βάσει ανωμαλιών (anomaly based).*

- ✓ **Απόκριση σε ανιχνευόμενες εισβολές – Response to detected intrusions**

  Η απόκριση σε μια εισβολή μπορεί να είναι είτε παθητική είτε ενεργητική. Τα παθητικά συστήματα αποκρίνονται γνωστοποιώντας το πρόβλημα στην αρμόδια αρχή της επιχείρησης. Δηλαδή δεν λαμβάνουν μέτρα με σκοπό να αποτρέψουν ή να περιορίσουν τις ζημίες που προκλήθηκαν από την επίθεση. Αντίθετα τα ενεργητικά συστήματα οχι μονο γνωστοποιούν το πρόβλημα αλλά λαμβάνουν και τα κατάλληλα αντιμέτρα. Τα αντιμέτρα αυτά συχνά αποσκοπούν στον περιορισμό των ζημιών της επίθεσης.

- ✓ **Οργάνωση συστήματος – System Organization**

  Η οργάνωση ενός συστήματος ανίχνευσης ηλεκτρονικών εισβολών μπορεί να είναι είτε συγκεντρωμένη (centralized) ή κατανεμημένη (distributed). Στην πράξη είναι μάλλον δύσκολο να χαρακτηρίσουμε ενα σύστημα ώς αυστηρά συγκεντρωμένο ή πλήρως κατανεμημένο, μια και κάποια υποσυστήματα μπορεί να είναι συγκεντρωμένα και κάποια κατανεμημένα. Στα περισσότερα συστήματα η

συλλογή δεδομένων γίνεται κατανεμημένα ενώ η ανάλυσή τους γίνεται συγκεντρωμένα.

- ✓ **Ασφάλεια – Security**

Η δυνατότητα ενός συστήματος να «αντέχει» στις επιθέσεις προσδιορίζει και τον βαθμό ασφάλειάς του. Η κατάταξη των διαφόρων συστημάτων θα γίνει απλά βάσει υψηλής ή χαμηλής ασφάλειας, διότι η ερευνα σχετικά με τον προσδιορισμό της ασφάλειας ενός συστήματος δεν έχει καταλήξει ακόμα σε ασφαλή συμπεράσματα.

- ✓ **Συμβατότητα/Διαλειτουργικότητα – Degree of interoperability**

Ο βαθμός συμβατότητας ενός ανιχνευτή ηλεκτρονικών εισβολών προσδιορίζει την ικανότητα του να συνεργάζεται με διαφορετικά αλλά παρόμοια συστήματα. Η συμβατότητα μπορεί να αποτελεί αντικείμενο ενδιαφέροντος σε πολλαπλά επίπεδα αρχιτεκτονικής εξυπηρετώντας διαφορετικές σκοπιμότητες όπως:

- Ανταλλαγή ελεγχόμενων εγγραφών δεδομένων
- Ανταλλαγή πολιτικών ασφάλειας
- Ανταλλαγή σχετικά με σχέδια παραβίασης ή στατιστικά στοιχεία που αφορούν τις δραστηριότητες των χρηστών
- Ανταλλαγή αναφορών συναγερμού και προειδοποιήσεων.

- ✓ **Ευκολη διαχείριση – Manageability**

Πρόκειται για την ικανότητα του συστήματος να ελέγχεται με ευκολία ή να αποστέλλει ειδοποίηση συναγερμού σε άλλα συστήματα λήψης αποφάσεων.

- ✓ **Προσαρμοστικότητα – Adaptivity**

Οι παραγόμενες εφαρμογές μιας επιχείρησης καθώς και τα πρωτόκολλα επικοινωνίας είναι δυνατόν να γίνουν στόχοι εσφαλμένης χρήσης ή προσπαθειών εισβολής. Για το λόγο αυτό, είναι ιδιαίτερα σημαντικό για τον ανιχνευτή ηλεκτρονικών εισβολών να μπορεί να αναπροσαρμόζεται σε ανάγκες συγκεκριμένης υποδομής.

- ✓ **Απαιτήσεις συστήματος σε δικτυακή υποδομή – System and network infrastructure requirements**

Οι απαιτήσεις που μπορεί να έχει το σύστημα σε ότι αφορά την δικτυακή υποδομή της επιχείρησης είναι δυνατό να περιορίσει την προσαρμοστικότα ενός προϊόντος. Το κόστος εφαρμογής και οι απαιτήσεις της αγοράς είναι δυνατό να επιβάλλουν σημαντικούς περιορισμούς. Τα τελευταία χρόνια, η χρήση του TCP/IP έχει εξαπλωθεί ευρέως και είναι σίγουρα το πρωτόκολλο που κυριαρχεί στις τοπολογίες των σημερινών δικτύων. Ως αποτέλεσμα περιμένει κανείς να δεί την εφαρμογή του στην λειτουργία των συστημάτων ανίχνευσης ηλεκτρονικών εισβολών που διατίθενται στην αγορά.

4. Κατηγοριοποίηση κριτηρίων σύγκρισης

Στο σημείο αυτό και ενώ έχει προηγηθεί η αναφορά στις σημαντικότερες παραμέτρους σύγκρισης των ανιχνευτών ηλεκτρονικών εισβολών κρίνεται σκόπιμη η ομαδοποίησή τους σε γενικότερες κατηγορίες που αφορούν διαφορετικές έννοιες των συστημάτων αυτών. Η ομαδοποίηση αυτή φαίνεται συνοπτικά στο σχήμα που ακολουθεί (σχήμα 2):

Οπτική γωνία	**Κριτήρια**
Λειτουργικότητα	1. Κατάτμηση των δεδομένων επεξεργασίας 2. Πηγή Ελέγχου Δεδομένων 3. Απόκριση σε ανιχνευόμενες εισβολές 4. Συμβατότητα 5. Μέθοδος Ανίχνευσης 6. Προσαρμοστικότητα 7. Δυνατότητες ανίχνευσης
Ασφάλεια	8. Βαθμός ασφάλειας
Αρχιτεκτονική	9. Οργάνωση συστήματος 10.Απαιτήσεις συστήματος σε δικτυακή υποδομή
Αποδοτικότητα	11. Επιδόσεις
Διαχείριση	12. Ευκολία στην διαχείριση

Θα ακολουθήσει συνοπτική παρουσίαση των πιο δημοφιλών συστημάτων ανίχνευσης ηλεκτρονικών εισβολών και στην συνέχεια θα επιχειρηθεί η σύγκρισή τους βάσει των κριτηρίων, όπως αυτά ομαδοποιήθηκαν παραπάνω.

ΠΑΡΟΥΣΙΑΣΗ IDS

5. Παρουσίαση δημοφιλών Συστημάτων Ανίχνευσης Ηλεκτρονικών Εισβολών

Στην ενότητα που ακολουθεί θα παρουσιάσουμε 6 από τους πιο δημοφιλής ανιχνευτές ηλεκτρονικών εισβολών της αγοράς.

5.1 RealSecure (Internet Security Systems)

Προϊον	**RealSecure**
Κατασκευαστής	Internet Security Systems (ISS)
Υποστηριζόμενες πλατφόρμες	Solaris (Sparc and x86), Windows NT
Πηγή δεδομένων	Δικτυακή & Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

5.1.1 Εισαγωγή

Ο ανιχνευτής RealSecure λειτουργεί με δικτυακή και τερματική λογική και εχει σύστημα απόκρισης που λειτουργεί σε πραγματικό χρόνο (real time response). Χρησιμοποιεί προκαθορισμένα σχήματα επιθέσεων ή εσφαλμένων χρήσεων, για να ανιχνεύσει ενέργειες που παραβιάζουν την δεδηλωμένη πολίτικη ασφάλεια της επιχείρησης.

5.1.2 Αρχιτεκτονική

Η αρχιτεκτονική του RealSecure αποτελείτε από τρεις βασικές λειτουργικές μονάδες:

- Μηχανή του RealSecure (RealSecure Engines)
- Εντολοδόχους του RealSecure (RealSecure Agents)
- Γενικός διαχειριστής (RealSecure Manager)

Οι μηχανές του RealSecure «τρέχουν» σε αποκλειστικά για αυτήν την εργασία τερματικά και παγιδεύουν και στην συνέχεια αναλύουν τα πακέτα που κυκλοφορούν στο υπο παρακολούθηση δίκτυο. Τα πακέτα αυτά που παγιδεύονται συγκρίνονται με γνωστά σενάρια επιθέσεων που είναι καταχωρημένα στις βάσεις δεδομένων, ελπίζοντας ότι μπορεί να διαχωρίσει μεταξύ τους επιθέσεις που τυχών να συμβαίνουν ταυτόχρονα.

Η εσωτερική αρχιτεκτονική της μηχανής του RealSecure αποτελείτε από πέντε βασικές μονάδες:

- Interface δικτύου
- Μονάδα παγίδευσης πακέτων
- Μονάδα φιλταρίσματος
- Μονάδα αναγνώρισης επίθεσης
- Μονάδα απόκρισης

Οι εντολοδόχοι (agents) είναι οι ομόλογοι της μηχανής του RealSecure βασιζόμενοι όμως σε τερματική λογική (δηλ. τρέχουν σε αυτόνομα τερματικά στοιχεία του δικτύου). Οι εντολοδόχοι αναλύουν τα αρχεία ημερολογίου των τερματικών με παρόμοιο τρόπο με αυτόν που χρησιμοποιεί η μηχανή του RealSecure για την ανάλυση των πακέτων του δικτύου. Εφόσον έχει ανιχνευτεί επίθεση ο εντολοδόχος έχει την δυνατότητα να τερματίσει διεργασίες του συστήματος ή να απενεργοποιήσει λογαριασμούς χρηστών. Οι εντολοδόχοι του RealSecure έχουν ακόμα την δυνατότητα να αναδιαμορφώσουν τόσο την μηχανή όσο και τους firewalls, έτσι ώστε να εμποδίσουν/μπλοκάρουν πιθανές μελλοντικές επιθέσεις/εισβολές από συγκεριμένες πηγές. Προς το παρών, το λογισμικό τω εντολοδόχων διατίθεται μόνο για πλατφόρμες Windows NT.

Ο γενικός διαχειριστής του RealSecure είναι μια κονσόλα διαχείρισης που δίνει την δυνατότητα συνολικής παρακολούθησης με γραφικό περιβάλλον όλου του συστήματος καθώς και της μηχανής και των εντολοδόχων που προαναφέρθηκαν. Η κονσόλα υποστηρίζει τρεις βασικές υπηρεσίες:

- Κεντρική παρουσίαση συναγερμών σε πραγματικό χρόνο
- Κεντρική διαχείριση δεδομένων
- Κεντρική ρύθμιση (configuration) της μηχανής του RealSecure

5.2 Intruder Alert (Axent Technologies)

Προϊον	**Intruder Alert**
Κατασκευαστής	Axent Technologies Inc.
Υποστηριζόμενες πλατφόρμες	Solaris (Sparc), SunOS, Windows 98/NT, NetWare, AIX, Digital Unix, HP-UX, IRIX, SVR4 (Motorolla 88000), AT&T GIS (NCR), OpenVMS
Πηγή δεδομένων	Δικτυακή & Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

5.2.1 Εισαγωγή

Το Intruder Alert είναι ένα πραγματικού χρόνου, βασισμένο σε κανόνες σύστημα ανίχνευσης ηλεκτρονικών εισβολών. Παρακολουθεί τα ακολουθιακά δεδομένα ελέγχου των τερματικών μέσα σε ένα κατανεμημένο περιβάλλον. Η ανίχνευση των προσπαθειών εισβολών βασίζεται σε κανόνες ή απρόβλεπτα λάθη του συστήματος (exceptions). Η μηχανή που βασίζεται σε κανόνες αναζητά συγκεκριμένες και προκαθορισμένες ακολουθίες δεδομένων. Οι ακοουθίες αυτές ονομάζονται «χνάρια» (footprints) και αναγνωρίζουν μονοσήμαντα ανώμαλες συμπεριφορές/πλάνα μέσα στα ακολουθιακά δεδομένα ελέγχου των τερματικών (audit trails).

5.2.2 Αρχιτεκτονική

Το Intruder Alert αποτελείτε από τρείς βασικές λειτουργικές μονάδες:

- Interface κονσόλας (interface concole)

- Γενικός διαχειριστής (Manager)
- Εντολοδόχοι (Agent)

Το interface κονσόλας καθώς και ο γενικός διαχειριστής επιτρέπουν την ρύθμιση των κανόνων σύμφωνα με την πολίτικη ασφάλειας της επιχείρησης. Παρότι οι *διαχειριστές συναγερμού* και οι *εντολοδόχοι* του Intruder Alert υποστηρίζονται από πληθώρα λειτουργικών συστημάτων (συμπεριλαμβανομένου του UNIX), η κονσόλα και ο γενικός διαχειριστής υποστηρίζονται μόνο από τα Windows NT.

Οι εντολοδόχοι είναι διεργασίες και δαίμονες (daemons) που «τρέχουν» στα τερματικά που είναι υπο παρακολούθηση. Οι εντολοδόχοι συλλέγουν δεδομένα ελέγχου και εφαρμόζουν το σύνολο κανόνων όπως αυτό έχει ρυθμιστεί από τον administrator του συστήματος. Ολοι οι *εντολοδόχοι* πρέπει να έχουν καταχωρηθεί στον *γενικό διαχειριστή,* για να γίνει εφικτή η ρύθμισή τους. Στην φάση της καταχώρησης αυτής, δημιουργείται ένα ασφαλές κανάλι επικοινωνίας με σκοπό να προστατεύσει τα δεδομένα που ανταλάσονται μεταξύ των συμμετεχόντων στοιχείων του δικτύου.

Πρόσθετα Χαρακτηριστικά

Net Prowler

Εκτός απότην ανάλυση δεδομένων σε τερματική βάση το Intruder Alert έχει την δυνατότητα να αναλύσει και τα πακέτα του συστήματος δικτυακά. Η διεργασία αυτή πραγματοποιείται στην ουσία από ξεχωριστό προϊόν. Αυτό συλλέγει δεδομένα από τα interface των καρτών δικτύου, γεγονός που επιτρέπει στον εντολοδόχο να παγιδεύσει πακέτα που προορίζονται σε άλλες διευθύνσεις εκτός από την δική του. Η Axent Technologies αποκαλεί την παραπάνω διεργασία **«Τεχνολογία Net Prowler»**. Το Net Prowler υποστηρίζεται μόνο από πλατφόρμα Windows NT.

Μονάδα Περίπολου (PATROL module)

Οι οργανισμοί που έχουν στην διάθεσή τους μεγάλα δίκτυα και σημαντικό αριθμό τερματικών, χρησιμοποιούν συνήθως κάποια εφαρμογή διαχείρισης δικτύου/τερματικών έτσι ώστε να μειώσει το κόστος συντήρησης και εποπτείας. *Ασφάλειας Διαχείρισης* σημαίνει ότι αυτές καθαυτές οι διαδικασίες διαχείρισης πρέπει να είναι ασφαλισμένες και ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν την δυνατότητα να εκτελέσουν τέτοιες διαδικασίες. *Διαχείριση Ασφάλειας* σημαίνει ότι οι παράμετροι του συστήματος ασφαλείας μπορούν να ρυθμιστούν με την ίδια ευκολία που ρυθμίζεται οποιαδήποτε αλλη παράμετρος του δικτύου ή των τερματικών.
Η Μονάδα Περίπολου από την BMC Software είναι ένα ολοκληρωμένο πακέτο προγραμμάτων που μπορεί να χρησιμοποιηθεί στην διαχείριση πολύπλοκων δικτυακών δομών μέσα σε ένα κατανεμημένο περιβάλλον.

5.3 NetRanger (Cisco Systems, Inc)

Προϊον	**NetRanger**
Κατασκευαστής	Cisco Systems, Inc
Υποστηριζόμενες πλατφόρμες	Εξειδικευμένο hardware και Solaris x86 v.2.6
Πηγή δεδομένων	Δικτυακή
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

5.3.1 Εισαγωγή

Το NetRanger είναι ένα πραγματικού χρόνου σύστημα ανίχνευσης ηλεκτρονικών εισβολών σχεδιασμένο έτσι ώστε να εντοπίζει επιθέσεις μέσα στην δικτυακή υποδομή των επιχειρήσεων. Είναι αμιγώς σύστημα με δικτυακή λογική και αναλύει διεξοδικά τα πακέτα που κυκλοφορούν στο δίκτυο. Το μοντέλο ανίχνευσης «εσφαλμένης χρήσης» χρησιμοποιείται στον εντοπισμό παραβιάσεων της πολιτικής ασφάλειας της επιχείρησης. Ακόμα το NetRanger έχει δυνατότητες απόκρισης σε πραγματικό χρόνο με ενέργειες όπως ο τερματισμός συγκεκριμένων συνδέσεων και το μπλοκάρισμα αναμενόμενων προσπαθειών εισβολής.

Αρχιτεκτονική

Το NetRanger αποτελείτε από τρεις βασικές λειτουργικές μονάδες:

- Αισθητήρες (Sensors)
- Οδηγό (Director)
- Διαδικασίες Post Office

Η αρχιτεκτονική συστήματος του NetRanger είναι από τα πολύ δυνατά σημεία του. Οι *αισθητήρες* σε συνδυασμό με τους *οδηγούς* μπορούν να σχηματίσουν ιεραρχικές δομές, που επιτρέπουν την παρακολούθηση μεγάλου αριθμού δικτυακών τμημάτων (network segments).

Οι αισθητήρες του συστήματος είναι αυτές που παρακολουθούν την κίνηση στο δίκτυο και συλλέγουν σχετικές πληροφορίες. Υπό φυσιολογικές συνθήκες, ένας αισθητήρας παρακολουθεί την κίνηση σε ένα και μόνο τμήμα του δικτύου. Ενα εξειδικευμένο σύστημα χρησιμοποιείται για να μειώσει την κίνηση στο δίκτυο. Η ύποπτες συμπεριφορές ανιχνεύονται με τον εντοπισμό συγκεκριμένων ακολουθιών δυαδικών δεδομένων. Επιπρόσθετα το NetRanger ελέγχει και τα αρχεία συστήματος των δρομολογητών της Cisco, για πιθανές παραβιάσεις.
Στην σημερινή έκδοση του προϊόντος οι αισθητήρες διατίθενται για Ethernet, Fast Ethernet, Token Ring και FDDI.
Το NetRanger αποκρίνεται σε πιθανές παραβιάσεις της πολιτικής ασφάλειας με τον τερματισμό ενεργών TCP συνδέσεων ή την ενημέρωση των *καταλόγων ελέγχου πρόσβασης* (ACL) των δρομολογητών ή των firewall.

Ο *οδηγός* παρέχει την δυνατότητα κεντρικής διαχείρισης των αισθητήρων που είναι κατανεμημένοι μέσα στο δίκτυο. Από τον *Οδηγό* ο διαχειριστής του συστήματος μπορεί να ρυθμίσει τους αισθητήρες και να αναλύσει τα

ενδεχόμενα κενά ασφαλείας στο σύστημα. Ο *Οδηγός* χρησιμοποιείται ακόμα για την εξαγωγή δεδομένων σε συστήματα αναφορών (reporting systems) και το download/δημιουργία νέων σχεδίων επίθεσης.

Οι διαδικασίες Post Office χειρίζονται την επικοινωνία μεταξύ του *Οδηγού* και των *Αισθητήρων*. Οι διαδικασίες αυτές χρησιμοποιούν ένα πρωτόκολλο εφαρμογής βασισμένο στο UDP με χαρακτηριστικά για εξουσιοδότηση και μηχανισμούς ελέγχου δυσλειτουργιών (fault tolerance).

5.4 POLYCENTER (Compaq)

Προϊον	**POLYCENTER**
Κατασκευαστής	Compaq (former Digital Equiment Corp.)
Υποστηριζόμενες πλατφόρμες	SunOS, Open VMS
Πηγή δεδομένων	Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες και σε ευρεση ανωμαλιών
Συμπεριφορά	Ανίχνευση & Απόκριση

5.4.1 Εισαγωγή

Το POLYCENTER είναι ανιχνευτής ηλεκτρονικών εισβολών που λειτουργεί βασισμένο σε τερματική λογική που σημαίνει ότι είναι εγκατεστημένο στα τερματικά που είναι κατανεμημένα μέσα στ δίκτυο. Εντοπίζει εισβολές και προσπάθειες εισβολής εξετάζοντας τα αρχεία ελέγχου στα επιμέρους τερματικά.

Το POLYCENTER μπορεί να ρυμιστεί έτσι ώστε να ανιχνεύει πολλαπλές κατηγορίες εισβολών όπως:

- Προσπάθειες εκτέλεσης προγραμμάτων χωρίς εξουσιοδότηση
- Υποπτες μεταφορές αρχείων μέσα στο δίκτυο
- Υποπτες ενέργειες προς κάποιο τερματικό, χρήστη ή αρχείο
- Δραστηριότητες εκτός του κανονικού ωραρίου εργασίας

Η ανάλυση των δεδομένων ελέγχου χρησιμοποιεί διαδικασίες τεχνητής νοημοσύνης (AI) που σχεδιάστηκαν στα πλαίσια έρευνας από την Digital Equipment Corp. Οι πληροφορίες που υπάρχουν σε σχέση με τα γνωστά σενάρια επίθεσης χρησιμοποιούνται από το POLYCENTER, για να εντοπιστούν ύποπτες δραστηριότητες που θα μπορούσαν να υποδείξουν επίθεση προς κάποιο τερματικό στοιχείο του δικτύου. Ενα μοντέλο *«περιπτώσεων»* (case model) χρησιμοποιείται για να αναθέσει σε συγκεκριμένους εικονικούς εντολοδόχους του συστήματος ανίχνευσης (agents) την παρακολούθηση ύποπτων συμπεριφορών. Ο εικονικός εντολοδόχος παρακολουθεί τον ύποπτο και τα αποδεικτικά στοιχεία (log files) της υπόθεσης. Με την ανάλυση των γεγονότων ασφάλειας (security events) ανά υπόθεση/περίπτωση, το POLYCENTER είναι σε θέση να διακρίνει τις πραγματικές απειλές από τις απλές λανθασμένες συμπεριφορές.

Οταν κρίνεται σκόπιμο το POLYCENTER μπορεί να ειδοποιήσει τους administrators του δικτύου, σχετικά με τα κρίσιμα γεγονότα που ανιχνεύτηκαν. Επιπρόσθετα το σύστημα ανίχνευσης μπορεί να ρυθμιστεί με τέτοιο τρόπο ώστε να λαμβάνει χωρίς ανθρώπινη παρέμβαση.

5.5 Network Flight Recorder (Network Flight Recorder, Inc.)

Προϊον	**Network Flight Recorder**
Κατασκευαστής	Network Flight Recorder, Inc.)
Υποστηριζόμενες πλατφόρμες	Windows NT, Solaris (Sparc)
Πηγή δεδομένων	Δικτυακή
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

Εισαγωγή

Το Network Flight Recorder (NFS) δεν μπορεί να χαρακτηριστεί ως ένα αμιγές σύστημα ανίχνευσης ηλεκτρονικών εισβολών, παρότι έχει αρκετά χαρακτηριστικά ενός IDS. Οπως καταδεικνύει και το όνομα του προϊόντος το Network Flight Recorder σχεδιάστηκε με πρωταρχικό στόχο την επίτευξη μιας μεταμοντέρνας ανάλυσης των γεγονότων που συμβαίνουν σε ένα δίκτυο, όπως για παράδειγμα όταν ένας administrator θέλει να διαπιστώσει τι πραγματικά έγινε στο δίκτυο κατά την εισβολή ή κάποια αλλη ανωμαλία του συστήματος.

Το Network Flight Recorder παρέχει δυνατότητες καταγραφής και φιλτραρίσματος της κίνησης στο δίκτυο με σκοπό την καταχώρηση σε αρχεία ή την στατιστική ανάλυση και μπορεί να ρυθμιστεί έτσι ώστε να πυροδοτεί (trigger) συναγερμό σε συγκεκριμένα γεγονότα. Σύμφωνα με την ομάδα που το ανάπτυξε, το Network Flight Recorder σχεδιάστηκε για να συμπληρώνει ένα σύστημα ανίχνευσης ηλεκτρονικών εισβολών. Χρησιμοποιεί μια «σκούπα πακέτων» για να συλλέξει όλα τα πακέτα από το δίκτυο. Τα πακέτα αυτά τροφοδοτούνται σε μια μηχανή απόφασης, όπου γίνεται η εκτίμηση μέσω ειδικών φίλτρων γραμμένων σε N-code, μια γλώσσα που αναπτύχθηκε αποκλειστικά για το NFR. Με ένα τέτοιο φίλτρο, είναι δυνατό να καταγραφούν οι επιλεγμένες πληροφορίες από τα φιλτραρισμένα πακέτα σε δίσκους και να πυροδοτήσουν συναγερμό. Οι πληροφορίες που καταγράφονται στον δίσκο μπορούν να γίνουν προσπελάσιμες μέσω ενός υποστηρικτικού υποσυστήματος υποβολής ερωτημάτων (queries), το οποίο είναι σαφώς διαχωρισμένο με το υποσύστημα καταγραφής. Οι χρήστες μπορούν μέσω ενός Web browser να συνδεθούν με τον HTTP διακομιστή που επικοινωνεί με το NFR, με σκοπό την υποβολή των ερωτημάτων. Ο browser κατεβάζει και εκτελεί Java Applets που εξυπηρετούν το user interface του NFR. Τα αποτελέσματα των ερωτημάτων αυτών οπτικοποιούνται στον χρήστη με τη βοήθεια της Java και με τη μορφή διαφορετικών τύπων λιστών ή διαγραμμάτων.

5.6 CyberCorp (Network Associates, Inc.)

Προϊον	**CyberCorp**
Κατασκευαστής	Network Associates, Inc.
Υποστηριζόμενες πλατφόρμες	Windows NT, Solaris (Sparc)
Πηγή δεδομένων	Δικτυακή & Τερματική
Μοντέλο ανίχνευσης	Μοντέλο ανίχνευσης βασισμένο σε κανόνες
Συμπεριφορά	Ανίχνευση & Απόκριση

Εισαγωγή

Η Network Associates παρέχει μια σειρά από προϊόντα ανίχνευσης ηλεκτρονικών εισβολών υπό την ονομασία CyberCorp. Τα CyberCorp Network και CyberCorp Server είναι τμήματα του συνόλου προγραμάττων της Network Associates με την ονομασία Net Tools Secure.

Το CyberCorp Network (**CCN**) παρέχει ανίχνευση ηλκτρονικών εισβολών σε πραγαμτικό χρόνο αξιοποιώντας πληροφορίες από το τοπικό δίκτυο. Το CyberCorp Server (**CCS**) εστίαζει στην προστασία των servers και των άλλων τερματικών μέσα στο δικτυακό περιβάλλον.

Αισθητήρες τοποθετούνται σε στρατηγικές θέσεις στο δίκτυο με σκοπό να εντοπίσουν ύποπτες συμπεριφορές. Οι αισθητήρες λειτουργούν σε συνεργασία με ένα διακομιστή διαχείρισης (management server) ο οποίος καταγράφει σε αρχεία ύποπτα γεγονότα και στέλνει ειδοποιήσεις συναγερμού στις κονσόλες διαχείρισης (management consoles). Στην συνέχεια ενεργοποιούνται αυτοματοποιημένες διαδικασίες απόκρισης, για να τερματίσουν διεργασίες του συστήματος ή να ειδοποιήσουν τους administrators μέσω email. Ακόμα το CCN είναι εξοπλισμένο με μια ζωτικής σημασίας λειτουργία που προστατεύει τους αισθητήρες από εξωτερικές παρεμβάσεις.

Το CyberCorp Network βασίζεται στην τεχνολογία ανίχνευσης της Wheelgroup, Inc (είναι πλέον αγορασμένη από την Cisco). Για την ακρίβεια το NetRanger της Cisco και το CyberCorp Network χρησιμοποιούν παρόμοιες τακτικές για την ανίχνευση των επιθέσεων. Η βασική διαφορά ανάμεσα σε αυτά τα δυο προϊόντα είναι ότι το NetRanger εστιάζει στην προστασία της περιμέτρου του δικτύου χρησιμοποιώντας firewalls ή δρομολογητές (routers) για να μπλοκάρει τις εισσβολές, ενώ το CyberCorp εστιάζει στην προστασία του δικτύου από εσωτερικές επιθέσεις.

Τα αντικείμενα στα οποία το CyberCorp ανιχνεύει επιθέσεις συμπεριλαμβάνουν:

- Unix & Windows/Windows NT τερματικά
- Δικτυακές Υπηρεσίες (network Services)
- Web Servers & browsers
- Διάφορες εφαρμογές
- Σωρούς πρωτοκόλλων (Protocol stacks)

Αρχιτεκτονική

Το CyberCorp έχει δυο βασικές λειτουργικές μονάδες:

- Τους αισθητήρες CyberCorp (sensors)
- Τον διακομιστή διαχείρισης CyberCorp (management server)

Οι αισθητήρες κατανέμονται μέσα στο δίκτυο και ρυθμίζονται έτσι ώστε να ανιχνεύουν εισβολές, βασιζόμενοι στις πληροφορίες που συλλέγουν στο τμήμα δικτύου (network segment) όπου είναι συνδεδεμένοι. Η Network Associates συνιστά την τοποθέτηση των αισθητήρων σε σημεία υψηλής επικινδυνότητας όπως:

- Wide Area Links
- Dial-in συνδέσεις
- Server clusters
- Σε άλλα κρίσιμα τμήματα του δικτύου

Ο διακομιστής διαχείρισης (management server) συλλέγει τα δεδομένα ελέγχου από τους αισθητήρες και παρέχει καταγραφή τους σε αρχεία και αντίστοιχες ειδοποιήσεις συναγερμού. Στην συνέχεια χρησιμοποιείται μια εφαρμογή βασισμένη σε τεχνολογίες web (web-based interface) η οποία επιτρέπει στον γενικό διαχειριστή να επιβλέψει το σύστημα από οποιαδήποτε τοποθεσία. Η ασφάλεια του συστήματος βελτιώνεται με την χρήση διαδικασιών κρυπτογράφησης με σκοπό να προστατεύσουν τα κανάλια επικοινωνίας ανάμεσα στους αισθητήρες/διαχειριστές και την web εφαρμογή που προαναφέρθηκε.

6. Αλλα εμπορικά IDS

Στην ενότητα αυτή θα γίνει απλή αναφορά κάποιων επιπλέον διαδεδομένων συστημάτων ανίχνευσης ηλεκτρονικής εισβολής, για λόγους πληρότητας της παρουσίασης του θέματος.
Ενδεικτικά αναφέρουμε τους εξής:

- **Stake Out I.D.** (Harris Communications, Inc.)
- **Kane Security Monitor** (Security Dynamics)
- **Session Wall-3** (AbirNet)
- **Entrax** (Centrax Corporation)
- **CMDS** (Science Application International Corporation)
- **SecureNet Pro** (MimeStar, Inc.)
- **INTOUCH INSA** (Touch Technologies, Inc.)
- **T-Sight** (EnGarde Systems, Inc.)
- **NIDES** (SRI International)
- **ID-Trak** (Internet Tools, Inc.)
- **SecureCom Suite** (ODS Networks)

ΣΥΓΚΡΙΤΙΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Στην ενότητα αυτή θα επιχειρήσουμε την σύγκριση των 6 εμπορικών Συστημάτων Ανίχνευσης Ηλεκτρονικών Εισβολών βάσει των κριτηρίων που έχουμε ήδη αναλύσει και κατηγοριοποιήσει. Η παράθεση των συγκριτικών αποτελεσμάτων θα γίνει βάσει των κατηγοριών των κριτηρίων (*Ενότητα 4*).

7. ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ

7.1 Μηχανισμοί Απόκρισης

Τα περισσότερα συστήματα ανίχνευσης έχουν πολλάπλούς τρόπους απόκρισης, δηλ. αποστολής ειδοποιήσεων συναγερμού προς εξωτερικές συσκευές. Οι ικανότητες σελιδοποιήσης (paging) και η αποστολή email (SMTP messages) είναι οι πιο διαδεδομένοι μηχανισμοί. Ο πίνακας που ακολουθεί τους διαφόρους τρόπους απόκρισης που υποστηρίζει το κάθε σύστημα:

Προϊόν	SMTP	Paging	SNMP	OPSEC (Incl.FW-1)	Raptor (FW from Axent)	Pix (FW from Cisco)	Cisco Routers	Lucent FW Security Mgmnt Server
RealSecure	*		*	*				*
Intruder Alert	*	*	*	*	*		*	
NetRanger	*	*	*				*	
CyberCorp	*	*	*			*		
PolyCenter	*							
Network Flight Recorder	*	*						

7.2 Μέθοδοι Ανίχνευσης

Στην ενότητα αυτή παρουσιάζονται συγκεντρωτικά οι μέθοδοι ανίχνευσης που υποστηρίζουν τα υπό σύγκριση συστήματα

Προϊόν	Βασισμένο σε κανόνες	Βασισμένο σε ανωμαλίες
RealSecure	*	
Intruder Alert	*	
NetRanger	*	
CyberCorp	*	
PolyCenter	*	*
Network Flight Recorder	*	

Εδώ έχει προβάδισμα το Intruder Alert με την επιπλέον λειτουργική μονάδα που διαθέτει το NetProwler που επιτρέπει εκτεταμένη προσαρμογή στην ανίχνευση επιθέσεων με την χρήση μάλιστα ενός πολύ εύχρηστου γραφικού περιβάλλοντος. Το σύστημα του RealSecure είναι παρόμοιο μια και αυτό αναζητά για ακολουθίες χαρακτήρων στα αρχεία ημερολογίου του συστήματος. Στην πραγματικότητα όμως το RealSecure έχει μόνο περιορισμένες δυνατότητες στην ανίχνευση των ακολουθιών αυτών.
Από την άλλη το Network Flight Recorder παρέχει μια ιδιαίτερα εύπλαστη λύση, δίνοντας την δυνατότητα προσαρμογής της μηχανής ανάλυσης δεδομένων, μέσω μιας εξειδικευμένης γλώσσας προγραμματισμού η οποία φαίνεται να έχει απεριόριστες δυνατότητες διαμόρφωσης σχημάτων εντοπισμού επιθέσεων. Ωστόσο, λόγω αυτής της ελαστικότητας που παρέχεται, τέτοιες προσπάθειες διαμόρφωσης μάλλον απαιτούν μεγάλη ικανότητα (προγραμματιστική) αλλά και χρόνο!

7.3 Δυνατότητες Ανίχνευσης

Οι ικανότητες ανίχνευσης των συστημάτων παρουσιάζουν σημαντικές διαφοροποιήσεις, γεγονός που καθιστά την σύγκρισή τους μάλλον επίπονη. Γενικά, ένας δικτυακός ανιχνευτής ηλεκτρονικών εισβολών (NIDS) έχει προφανώς μεγαλύτερες ικανότητες να παγιδεύει και να αναλύει τα πακέτα στο υποκείμενο δίκτυο. Από την άλλη τα συστήματα που βασίζονται σε τερματική λογική περιορίζονται στην ανάλυση των δεδομένων ελέγχου που τους παρέχουν τα λειτουργικά συστήματα και τα αρχεία εφαρμογών των τερματικών. Παρακάτω φαίνονται συνοπτικά οι ικανότητες ανίχνευσης των συστημάτων βάσει ενός απλουστευμένου μοντέλου λειτουργικών επιπέδων.

Προϊόν	**Physical and datalink layer**	**Network and transport layer**	**Λειτουργικά Συστήματα**	**Εφαρμογές, βάσεις δεδομένων, συστήματα διαχείρισης & υποστήριξης, αυτοματοποιημένες διαδικασίες γραφείου**
RealSecure	▬	▬	▬	▬
Intruder Alert	▬	▬	▬	▬
NetRanger	▬	▬	▬	▬
CyberCorp	▬	▬	▬	▬
PolyCenter		▬	▬	
Network Flight Recorder	▬	▬	▬	▬

Η διακεκομένη γραμμή στο Network Flight Recorder υποδεικνύει ότι η γλώσσα προγραμματισμού που παρέχει μπορούν να επεκτείνουν τις δυνατότητες ανίχνευσής του.

7.3 Συγκεντρωτικά

Ο πίνακας που ακολουθεί παρουσιάζει συνοπτικά την σύγκριση των συστημάτων βάσει όλων των κριτηρίων λειτουργικότητας όπως αυτά ορίσθηκαν στην ενότητα 4.

Προϊόν	Κατάτμηση των δεδομένων επεξεργασίας	Πηγή Ελέγχου Δεδομένων	Απόκριση σε ανιχνευόμενες εισβολές	Συμβατότητα	Προσαρμοστικότητα	Δυνατότητες ανίχνευσης
RealSecure	Πραγματικό Χρόνο	Δικτυακή & Τερματική	Ενεργητική	Μέτρια	Υψηλή	Υψηλή
Intruder Alert	Πραγματικό Χρόνο	Δικτυακή & Τερματική	Ενεργητική	Μέτρια	Υψηλή	Υψηλή
NetRanger	Πραγματικό Χρόνο	Δικτυακή	Ενεργητική	Μέτρια	Μέτρια	Υψηλή
CyberCorp	Πραγματικό Χρόνο	Δικτυακή & Τερματική	Ενεργητική	Μέτρια	Μέτρια	Υψηλή
PolyCenter	Πραγματικό Χρόνο	Τερματική	Ενεργητική	Χαμηλή	Μέτρια	Χαμηλή
Network Flight Recorder	Πραγματικό Χρόνο	Δικτυακή	Ενεργητική	Χαμηλή	Μέτρια	Υψηλή

8. ΑΣΦΑΛΕΙΑ

Η ασφάλεια ενός συστήματος ανίχνευσης ηλεκτρονικών εισβολών είναι ένα ιδιαίτερα πολύπλοκο κριτήριο το οποίο εξαρτάται από ένα πλήθος παραμέτρων. Μια από τις βασικότερες απαιτήσεις είναι η ικανότητα ενός IDS να διατηρεί το επίπεδο λειτουργίας του δικτύου, ανεξάρτητα από το πλήθος και το είδος των επιθέσεων. Δυστυχώς πολλοί λίγοι κατασκευαστές συζητούν αυτό το θέμα, ίσως επειδή αποτυγχάνουν να εναρμονιστούν μα αυτή την απαίτηση. Εντούτοις, υπάρχουν προϊόντα που ενσωματώνουν μηχανισμούς προστασίας από τις επιθέσεις.

Παρακάτω θα αναφέρουμε τους εξι πιο βασικούς άξονες αναφοράς που σχετίζονται με το επίπεδο ασφαλείας των IDS, χωρίς να επιχειρήσουμε την σύγκριση μεταξύ των προϊόντων λόγω ελειπών στοιχείων που παρέχουν οι αντίστοιχοι κατασκευαστές:

- Εμπιστευτικότητα των δεδομένων ελέγχου
- Ακεραιότητα των δεδομένων ελέγχου
- Εμπιστευτικότητα της πολιτικής ανίχνευσης
- Ακεραιότητα της πολιτικής ανίχνευσης
- Προστασία των μηχανισμών απόκρισης
- Διαθεσιμότητα (no idle time)

Θα μπορούσαμε με κάθε επιφύλαξη να ξεχωρίσουμε το RealSecure και το NetRanger λόγω του γεγονότος ότι διαθέτουν τα εξής χαρακτηριστικά:

- Ύπαρξη ασφαλών καναλιών επικοινωνίας
- Ύπαρξη διαδικασιών πυρήνα που εξασφαλίζουν την ασφάλεια των επιμέρους κομματιών του IDS, ακόμα και όταν αυτά δέχονται επίθεση.
- Εχουν την δυαντότητα να λειτουργούν σε stealth mode που σημαίνει ότι δεν απαιτείται διεύθυνση IP για την λειτουργία τους

μέσα στο δίκτυο. Η επικοινωνία με τα αλλα στοιχεία του δικτύου επιτυγχάνεται απλά με την χρήση δεύτερης κάρτας δυκτύου (faking technic).

9. ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Θεωρητικά όλα τα συστήματα μπορούν να λειτουργήσουν σε κατανεμημένο περιβάλλον. Για παράδειγμα το Intruder Alert είναι μερικώς κατανεμημένο. Θα επιχειρήσουμε την παράθεση συγκεντρωτικών αποτελεσμάτων των συστημάτων ανίχνευσης βάσει των λειτουργικών που υποστηρίζουν σε σχέση με τον βαθμό που μπορούν να λειτουργήσουν κατανεμημένα και ακόμα με τις τεχνολογίες δικτύων που υποστηρίζουν.

9.1 Λειτουργικά Συστήματα

Παρότι η αγορά τείνει να προσαρμόσει την λειτουργία των προϊόντων τους για χρήση σε πλατφόρμες windows NT, ένας μεγάλος αριθμός συστημάτων ανίχνευσης λειτουργούν σε περιβάλλοντα UNIX. Ο πίνακας που ακολουθεί συνοψίζει τις απαιτήσεις του γενικού διαχειριστή (manager) και των εντολοδόχων (agents), σε ότι αφορά τα λειτουργικά συστήματα με τα οποία μπορουν να συνεργαστούν.

Προϊόν	**Λειτουργικό Σύστημα για τον Manager**	**Λειτουργικό Σύστημα για τον Agent**
RealSecure	Solaris, NT	NT, (Solaris ?)
Intruder Alert	Solaris, AT&T/NCR SVR4, IBM-AIX, OSF/1, Digital/UNIX, HP-UX, IRIX, SunOS, Novell, NT	Solaris, AT&T/NCR SVR4, IBM-AIX, OSF/1, Digital/UNIX, HP-UX, IRIX, SunOS, Novell, NT, SVR Motorolla 88000
NetRanger	HP/UX, Solaris	Solaris x86
CyberCorp	Solaris, NT	Solaris, NT
PolyCenter	SunOS, Open VMS	SunOS, Open VMS
Network Flight Recorder	Java based user interface	BSD/OS (x86), FreeBSD (x86), HP-UX, OpenBSD (x86), Solaris, NetBSD (x86), Slackware Linux (x86), Debian Linux (x86)

9.2 Τεχνολογίες Δικτύων

Όπως είναι γνωστό, το TCP/IP είναι το κυρίαρχο πρωτόκολλο που υποστηρίζουν οι πιο διαδεδομένες τεχνολογίες δικτύων. Ο πίνακας που ακολουθεί συνοψίζει τις τεχνολογίες δικτύων που υποστηρίζουν τα διάφορα συστήματα ανίχνευσης.

Προϊόν	**Datalink layer protocol**	**Network layer protocol**
RealSecure	Ethernet, FDDI, Token Ring	TCP/IP
Intruder Alert	Ethernet	TCP/IP, IPX/SPX
NetRanger	Ethernet, FDDI, Token Ring	TCP/IP
CyberCorp	Ethernet	TCP/IP

PolyCenter	-	-
Network Flight Recorder	Ethernet	TCP/IP

10. ΑΠΟΔΟΤΙΚΟΤΗΤΑ

10.1 Επιβάρυνση στην επικοινωνία (Communication overhead)

Ελάχιστα από τα συστήματα ανίχνευσης που αναλύσαμε προσδιορίζουν την επιβάρυνση στην επικοινωνία του συστήματος με την εφαρμογή ενός ανιχνευτή ηλεκτρονικών εισβολών. Για τους ανιχνευτές που λειτουργούν με δικτυακή λογική η επιβάρυνση προκαλείτε από την κατανομή των δεδομένων ελέγχου και την επικοινωνία μεταξύ των διαφόρων υποσυστημάτων του IDS. Για το ***RealSecure*** η εταιρία ISS ανέφερε μια επιβάρυνση στο φορτίο του δικτύου της τάξης του 5-10%.

10.2 Υπολογιστική επιβάρυνση

Υπολογιστική επιβάρυνση προκαλείτε μόνο στους ανιχνευτές που λειτουργούν με τερματική λογική (host-based IDS). Ενώ οι δικτυακοί ανιχνευτές «τρέχουν» σε κάποιο εξειδικευμένο γιαυτό το σκοπό σύστημα, οι ανιχνευτές τερματικής λογικής εκτελούν και συλλέγουν δεδομένα ελέγχου στο τερματικό το οποίο παρακολουθούν. Στην περίπτωση αυτή η ζημία στην απόδοση εξαρτάται ως επί το πλείστον από παραμέτρους όπως ο κερματισμός της επεξεργασίας των δεδομένων, το μέγεθος και ο ρυθμός αύξησης των αρχείων ημερολογίου του συστήματος, το μέγεθος και η πολυπλοκότητα του συνόλου των κανόνων του ανιχνευτικού συστήματος κτλ. Είναι λοιπόν προφανές ότι εξαιτίας της υποκειμενικότητας των παραπάνω παραμέτρων είναι μάλλον απίθανο να εκτιμήσει κανείς την επιβάρυνση. Εντούτοις, αυτό που πρέπει να γίνει αντιληπτό είναι ότι όλα τα συστήματα τερματικής λογικής προκαλούν υπολογιστική επιβάρυνση στο υπο παρακολούθηση σύστημα. Η εταιρία Centrax ανάφερε για το προϊόν της το Entrax (δεν αναλύθηκε διεξοδικά) μειώνει την απόδοση των επιμέρους τερματικών κατά λιγότερο από 2%. Η εταιρία Axent αναφέρει μια επιβάρυνση της τάξης του 5% για το Intruder Alert.

11. ΔΙΑΧΕΙΡΙΣΗ

Η διαχείριση ενός συστήματος ανίχνευσης ηλεκτρονικών εισβολών έχει κρίσιμη σημασία για την εφαρμογή του στην δικτυακή υποδομή μια επιχείρησης.

11.1 Διαχείριση Ρυθμίσεων (configuration management)

Η διαχείριση των ρυθμίσεων παρέχει διαδικασίες για την επιβολή ελέγχου, την συλλογή δεδομένων και την τροφοδότηση με δεδομένα προς τις οντότητες που αποτελούν τμήματα του συστήματος ανίχνευσης ηλεκτρονικών εισβολών. Με σκοπό την ανίχνευση επιθέσεων η διαχείριση των ρυθμίσεων συμπεριλαμβάνει και διαχείριση των δυνατοτήτων ανίχνευσης και των μηχανισμών απόκρισης που χρησιμοποιούνται.

Όλα τα συστήματα που αναλύσαμε υποστηρίζουν κάποιας μορφής διαχείρισης των ρυθμίσεων.

11.2 Διαχείριση Πολιτικής Ασφάλειας (security management)

Ασφάλεια πρόσβασης

Οι διάφοροι administrators θα πρέπει να επιτρέπεται να διαχειρίζονται μόνο τις περιοχές στις οποίες έχουν σχετική εξουσιοδότηση. Θα πρέπει ακόμα να είναι εφικτή η δημιουργία διαφορετικών views στο σύστημα για διαφορετικούς χρήστες του συστήματος ανίχνευσης.

Διαχείριση ασφάλειας

Οι διαδικασίες διαχείρισης πρέπει να προστατεύονται έτσι ώστε να απαγορεύουν σε έναν εισβολέα να αποκτά πρόσβαση στις πληροφορίες ή να παίρνει τον έλεγχο των πόρων του συστήματος ανίχνευσης.

Ακολουθίες ελέγχου και συναγερμοί ασφάλειας

Ενας διαχειριστής με περιορισμένο δικαίωμα πρόσβασης πρέπει να μπορεί να εξουσιοδοτηθεί στην οπτική επαφή (view) με τις ακολουθίες ελέγχου και τις πληροφορίες των γεγονότων που αφορούν στην ασφάλεια. Συναγερμοί ασφάλειας πρέπει να παράγονται έτσι ώστε να υποδεικνύουν τις προσπάθειες επίθεσης σε κάποιο στοιχείο του δικτύου ή ακόμα και στο ίδιο το IDS. Θα πρέπει να είναι εφικτή η δυνατότητα εγκρισης πρόσβασης στις ακολουθίες ελέγχου και τους σχετικούς συναγερμούς.

Τα προϊόντα **RealSecure**, **Intruder Alert**, **Net Ranger** και το **CyberCorp** έχουν αναφέρει την ύπαρξη διαδικασιών ελέγχου της πρόσβασης στο υποσύστημα ρύθμισης των παραμέτρων και των συναγερμών

11.3 Γραφικό περιβάλλον διαχείρισης (management interfaces)

Η διαλειτουργικότητα/συμβατότητα μεταξύ των αντικειμένων από διαφορετικούς κατασκευαστές συνήθως απαιτεί κάποια στάνταρντς σε ότι αφορά το γραφικό περιβάλλον επικοινωνίας. Σε ότι αφορά την διαχείριση, ένα τυποποιημένο γραφικό περιβάλλον θα επέτρεπε τον σχεδιασμό και την δημιουργία δυνατοτήτων ανίχνευσης εισβολών χρησιμοποιώντας υποσυστήματα από διαφορετικούς κατασκευαστές. Σήμερα, το **Net Ranger** είναι το μόνο προϊόν που είναι πλήρως ολοκληρωμένο με μια εφαρμογή διαχείρισης (HP Openview). Αυτό επιτρέπει στον administrator να διαχειρίζεται εξολοκλήρου το IDS μέσα από το υπάρχων σύστημα διαχείρισης. Επίσης, το **Intruder Alert** και το **RealSecure** μπορούν να επεκταθούν έτσι ώστε να συνεργάζονται με το HP Openview.

11.4 Μοντέλο διαχείρισης (management model)

Ο συγκεντρωμένος έλεγχος και διαχείριση είναι ζωτικής σημασίας για την επιτυχή εφαρμογή ενός συστήματος ανίχνευσης εισβολών, ειδικά μέσα σε ένα κατανεμημένο περιβάλλον στο οποίο μπορεί να γίνεται χρήση πολλαπλών υποσυστημάτων ανίχνευσης επιθέσεων. Συνεπώς θα πρέπει να είναι εφικτός ο καθορισμός μιας ιεραρχικής σχέσης μεταξύ του γενικού διαχειριστή και των εντολοδόχων έτσι ώστε κάποια συγκεκριμένη διεργασία να μπορεί να εφαρμόζεται διαδοχικά σε όλα τα κατανεμημένα στοιχεία.

Οι σχέσεις αυτές είναι οι εξής:

- **Πολλά προς πολλά (mant to many).** Πολλαπλές κονσόλες διαχείρισης μπορούν να διαχειριστούν πολλούς κατανεμημένους εντολοδόχους.
- **Ένα προς πολλά (one to many).** Μια και μόνο κονσόλα διαχείρισης μπορεί να διαχειρστεί πολλούς κατανεμημένους εντολοδόχους.
- **Ένα προς ένα (one to one).** Μια και μόνο κονσόλα διαχείρισης μπορεί να διασειριστεί ένα και μόνο εντολοδόχο.

Τα προϊόντα RealSecure, Intruder Alert και το Net Ranger υιοθετούν την σχέση πολλά προς πολλά. Επιπρόσθετα το Net Ranger υποστηρίζει την διαμόρφωση ιεραρχικής διαχείρισης των σχέσεων, όπου ένα δένδρο διαχειριστών και εντολοδόχων μπορεί να ρυθμιστεί από ένα και μόνο ανώτερο επίπεδο διαχείρισης. Τα PolyCenter και CyberCorp υποστηρίζουν σχέσεις ένα προς πολλά. Τέλος το NFR λόγω της ιδιαίτερης αρχιτεκτονικής του δεν μπορεί να κατηγοριοποιηθεί σ'υμφωνα με τα μοντέλα που περιγράφηκαν παραπάνω.

ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ

12.1 Ο ρόλος των IDS στην υποδομή ασφάλειας μιας επιχείρησης

Τα τελευταία χρόνια, έχει σημειωθεί δραματική αύξηση σε ότι αφορά την χρήση υπηρεσιών ασφάλειας όπως τα firewalls. Υπάρχει μια κοινή αυταπάτη ότι μόλις εγκατασταθεί κάποιο firewall, τότε όλα τα προβλήματα ασφάλειας θα λυθούν. Είναι σαφές ότι κάτι τέτοιο φυσικά δεν ισχύει, άσχετα για το πόσο προσπαθούν να μας πείσουν για κάτι τέτοιο συγκεκριμένοι μηχανισμοί της αγοράς. Ο ίδιος ενθουσιασμός υπάρχει σε ότι αφορά και τα συστήματα ανίχνευσης ηλεκτρονικών εισβολών. Εντούτοις, πρέπει να γίνει κατανοητό ότι ένα σύστημα ανίχνευσης δεν υποκαθιστά κάποιες άλλες υπηρεσίες ασφάλειας όπως τα firewalls ή οι διακομιαστές εξουσιοδότησης κτλ. Μάλλον θα πρέπει να θεωρηθεί ως συμπληρωματικό εργαλείο στις άλλες υπηρεσίες ασφάλειας το οποίο επεκτείνει περαιτέρω το επίπεδο προστασίας των δικτυακών υποδομών.

12.2 IDS τερματικής λογικής vs. IDS δικτυακής λογικής

Τα συστήματα ανίχνευσης ηλεκτρονικών εισβολών ξεκίνησαν ως μια τεχνολογία που ανάλυε τα δεδομένα ελέγχου των τερματικών. Τα τελευταία χρόνια, εμφανίστηκαν τα δικτυακά IDS τα οποία επέκτειναν τις δυνατότητες ανίχνευσης. Μια ερευνα στην αγορά, όπως αυτή που επιχειρήθηκε καθιστά σαφές ότι όλα τα εμπορικά συστήματα ανίχνευσης λειτουργούν με δικτυακή λογική. Ωστόσο, η διαρκώς αυξανόμενη χρήση κρυπτογράφησης στις δικτυακές υποδομές περιορίζουν αισθητά την δυνατότητα των IDS να προσπελαύνουν τα δικτυακά δεδομένα ελέγχου. Εξαιτίας αυτού του λόγου ίσως τα IDS τερματικής λογικής να γίνουν ιδιαίτερα δημοφιλή τα προσεχή χρόνια. Πιθανότητα κάποιες υβριδικές μορφές θα είναι αυτές που θα επικρατήσουν στο μέλλον.

12.3 Ασφάλεια των IDS

Η ασφάλεια των σημερινών εμπορικών συστημάτων ανίχνευσης αποτελεί ερωτηματικό. Παρότι χρησιμοποιούνται μέθοδοι κρυπτογράφησης για να προστατεύσουν τις ζεύξεις επικοινωνίας μεταξύ των διαφορετικών αντικειμένων, παραμένει ασαφές το πώς οι πληροφορίες που περιέχονται σε ένα IDS προστατεύονται στο σύνολό τους.

12.4 Έλλειψη συμβατότητας και τμηματοποίησης

Η δυνατότητα τμηματοποίησης των σημερινών εμπορικών συστημάτων ανίχνευσης είναι ιδιαίτερα περιορισμένη. Τις περισσότερες φορές, δεν είναι καν σαφώς διαχωρισμένα η συλλογή των γεγονότων εισόδου με τις διαδικασίες ανίχνευσης και απόκρισης. Το γεγονός αυτό περιορίζει αισθητά την δυνατότητα δημιουργίας ενός συστήματος ανίχνευσης που να απαρτίζεται από υποσυστήματα προερχόμενα από διαφορετικούς κατασκευαστές. Ένα παράδειγμα είναι η χρήση των βάσεων δεδομένων που ενσωματώνουν τα σχέδια δράσης των επιθέσεων. Κάθε κατασκευαστής παρέχει την δική του βάση

δεδομένων η οποία δεν μπορεί να χρησιμοποιηθεί από άλλους κατασκευαστές. Για την ακρίβεια οι βάσεις δεδομένων αποτελούν ένα σημείο έντονου ανταγωνισμού μεταξύ των κατασκευαστών.

Οι διάφοροι φορείς έρευνας και οι μικρότεροι κατασκευαστές είναι αυτοί που προσπαθούν να διαταράξουν την κυριαρχία κάποιων στην αγορά και τείνουν στην ανάπτυξη συστημάτων πλήρως διαλειτουργικών. Η αλήθεια είναι πως υπάρχουν αρκετές προσπάθειες δημιουργίας συστημάτων βασισμένες στην λογική του ανοιχτού κώδικα (open source), αλλα δυστυχώς δεν μπορούν ακόμα να εγγυηθούν υψηλό επίπεδο υπηρεσιών.

12.5 Προφίλ κατασκευαστών

Διανύουμε την εποχή της πληροφορίας, όπου τα όρια μεταξύ των εφαρμογών λογισμικού και των τεχνολογιών δικτύων μοίαζει να εξαλείφονται. Οι παραδοσιακές εταιρίες λογισμικού παρέχουν πλέον εφαρμογές και υπηρεσίες οι οποίες είναι στενά συνδεδεμένες με δικτυακές υποδομές. Ένα καλό παράδειγμα είναι τα IPφωνα. Παράλληλα, οι παραδοσιακοί κατασκευαστές δικτυακών στοιχείων επιζητούν τρόπους να επεκτείνουν το χαρτοφυλάκιό τους, παραδίδοντας πακέτα λογισμικού τα οποία ενισχύουν την υπάρχουσα γκάμα προϊόντων τους. Το αποτέλεσμα είναι και οι δυο πλευρές δραστηριοποιούνται σε τομείς οι οποίοι τελικά επικαλύπτονται. Φαίνεται, λοιπόν, ότι και τα συστήματα ανίχνευσης ηλεκτρονικών εισβολών εμπλέκονται στην ίδια σύγχυση. Ένα τέτοιο σύστημα αποτελεί ένα υψηλής τεχνολογίας κομμάτι λογισμικού του οποίου ο σχεδιασμός και η εφαρμογή απαιτούν ιδαίτερα προσόντα. Από την άλλη, ένα IDS αποτελεί ένα υψηλής απόδοσης δικτυακό αντικείμενο με ιδιαίτερα υψηλό βαθμό εξάρτησης με τα υπόλοιπα στοιχεία ενός δικτύου.

Δυστυχώς τα Συστήματα Ανίχνευσης Ηλεκτρονικών Εισβολών δεν έχουν ακόμα επιτύχει τέτοιο βαθμό ωριμότητας ώστε να δικαιολογήσουν την ουσιαστική συμμετοχή τους στην πολιτική ασφάλειας πολύπλοκων δικτυακών δομών σε μέγάλους οργανισμούς και επιχειρήσεις!

ΑΝΑΦΟΡΕΣ

1) http://www.cs.purdue.edu/coast/intrusion-detection/ids.htm
2) http://www.ietf.org
3) http://www.iss.net Internet Security Systems Corp.
4) http://www.axent.com Axent Technologies Inc.
5) http://www.cisco.com Cisco Systems Inc.
6) http://www.centrax.com Centrax Corporation
7) http://www.nai.com Network Associates Inc.
8) http://www.digital.com Compaq Corp.
9) http://www.nfr.net Network Flight Recorder Inc.
10) http://www.insecure.org
11) http://www.securityfocus.com
12) http://www.networkmagazine.com
13) http://www.securehq.com
14) http://www.eeye.com
15) http://www.eeye.com
16) http://www.robertgraham.com
17) http://www.cert.org/research/JHThesis/Start.html paper by John D. Howard
18) http://www.gocsi.com/summary.htm Survey Results 1999
19) http://www.nwc.com/1023/1023f19.html
20) http://www.internations.net
21) http://www.networkice.com/
22) http://www.cai.com/solutions/enterprise/etrust/intrusion_detection
23) http://www.network-defense.com/
24) http://www.packetfactory.net
25) http://www.clark.net/~roesch/secinfo.html
26) http://www.nswc.navy.mil/ISSEC/CID/co-ordinated_analysis.txt US Navy Research Project
27) http://www.ticm.com/
28) http://www-rnks.informatik.tu-cottbus.de/~sobirey/ids.html
29) http://www.gocsi.com/intrusion.htm Υποβολή ερωτημάτων σε IDS vendors
30) http://www.cve.mitre.org/
31) http://www.ce.chalmers.se Chalmers University of Technology, Gothenburg, Sweden
32) http://secinf.net/info/unix/lance/ids.html paper by Lance Spitzner
33) http://secinf.net/info/ids/intv2-8.htm paper by by Richard Bejtlich 2000
34) http://secinf.net/info/ids/nvh_ids/ paper by ISS 1999
35) http://secinf.net/info/ids/intrusion/ paper by ICSA
36) http://citeseer.nj.nec.com/axelsson98research.html
37) http://www.nss.co.uk/Articles/IntrusionDetection.htm
38) http://secinf.net/info/ids/ids_mythe.html paper by Marcus J. Ranum CEO, Network Flight Recorder, Inc.
39) http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf
[Allen 2000] Allen, et.al., "State of the Practice of Intrusion Detection Technologies", Technical Report , CMU/SEI-99-TR-028, ESC-99-028, January 2000
40) http://www.usenix.org/publications/library/proceedings/detection99/full_papers/elbaum/elbaum.pdf
[Elbaum 1999] S. Elbaum, J. Munson, "Intrusion Detection Through Dynamic Software Measurement", In Proceedings of the Eighth USENIX Security Symposium, 1999

41) http://citeseer.nj.nec.com/update/120258
[Helmer 1998] Helmer, Guy G., Johnny S. K. Wong, Vasant Honavar, and Les Miller, "Intelligent Agents for Intrusion Detection", *Proc. IEEE Information Technology Congerence* , pp. 121-124, Syracuse, NT, Sept. 1998.
42) http://www.ce.chalmers.se/staff/ulfl/pubs/ul-phd.pdf
[Lindqvist 1999] Lindqvist, Ulf, "On the Fundamentals of Analysis and Detection of Computer Misuse", PhD dissertation, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 1999
43) http://www.cs.unm.edu/~immsec/publications/ids.ps
[Warrender 1999] C. Warrender, S. Forrest, B. Pearlmutter, "Detecting Intrusions Using System Calls: Alternative Data Models", 1999 IEEE Symposium on Security and Privacy pp. 133-145 (1999).
44) http://www.silkroad.com/papers/pdf/acm-p99-bass.pdf
Intrusion Detection Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness by Tim Bass