

Συστήματα Ανίχνευσης Εισβολών

- Ανίχνευση εισβολών
 - Παρακολούθηση και ανάλυση των συμβάντων σε υπολογιστές ή δίκτυα για εντοπισμό ενδείξεων εισβολής
 - » Εισβολή: απόπειρα παραβίασης της
 - ακεραιότητας
 - εμπιστευτικότητας
 - διαθεσιμότητας
 - ή παράκαμψης των μηχανισμών ασφαλείας
 - » Οι εισβολές προέρχονται
 - από εξωτερικούς χρήστες χωρίς δικαίωμα πρόσβασης
 - από εσωτερικούς χρήστες με περιορισμένα δικαιώματα
 - από εσωτερικούς χρήστες που καταχρώνται τα δικαιώματα
 - Συστήματα: λογισμικό ή/και υλικό για αυτοματοποίηση

Σ.Α.Ε. – Γιατί τα χρησιμοποιούμε

- Πρόληψη προβλημάτων αυξάνοντας την πιθανότητα ανακάλυψης και τιμωρίας εισβολέων
- Ανίχνευση επιθέσεων και παραβιάσεων που δεν ανιχνεύονται με άλλα μέσα
- Εντοπισμός και αντιμετώπιση προσπαθειών ανίχνευσης
- Τεκμηρίωση υπαρκτής απειλής
- Έλεγχος ποιότητας για το σχεδιασμό ασφάλειας και τη διαχείριση
- Παροχή πληροφοριών για επιτυχείς εισβολές, για καλύτερη διάγνωση, ανάκαμψη και προληπτικά μέτρα

Συμπλήρωση άλλων τεχνικών

- Ανάγκη ύπαρξης παλαιών συστημάτων που δεν μπορούν να επιδιορθωθούν ή να ενημερωθούν
 - Ακόμη και αν είναι διαθέσιμα προγράμματα επιδιόρθωσης, δεν είναι εύκολο να εγκαθίστανται πάντα εγκαίρως, ειδικά σε πολύπλοκα περιβάλλοντα
 - Οι χρήστες απαιτούν την παροχή υπηρεσιών που είναι εύκολοτε σε επίθεσης
 - Χρήστες και διαχειριστές κάνουν λάθη στη χρήση και ρύθμιση του συστήματος
 - Η πολιτική ασφαλείας δεν απεικονίζεται πάντα πιστά στους κανόνες πρόσβασης
- Συνολικά: εντοπισμός εισβολών και επισήμανση στους διαχειριστές

Εντοπισμός και αντιμετώπιση προσπαθειών ανίχνευσης

- Τυπικό σχήμα επίθεσης:
 - ανίχνευση προσφερομένων υπηρεσιών
 - ανάσυρση από βιβλιοθήκες τεχνικών επίθεσης
 - χρήση τεχνικών επίθεσης
- Το σύστημα ανίχνευσης εισβολών
 - παρεμποδίζει την ανίχνευση υπηρεσιών
 - αποθαρρύνει τον επίδοξο εισβολέα
 - ενημερώνει τους διαχειριστές

Τεκμηρίωση υπαρκτών απειλών

- Η τεκμηρίωση πείθει τη διοίκηση για χρηματοδότηση
- Βοηθά στον προσδιορισμό των μέτρων ασφαλείας που είναι πιο κατάλληλα για το σύστημα
- Βοηθά στην ορθολογική κατανομή των πόρων ασφαλείας

Μοντέλο διαδικασιών για ανίχνευση εισβολών

- Κύρια συστατικά
 - Πηγές πληροφοριών
 - » συνήθως: παρακολούθηση δικτύου, υπολογιστών, εφαρμογών
 - Ανάλυση πληροφοριών
 - » Εξαγωγή συμπερασμάτων για απόπειρες εισβολών, επιτυχημένες εισβολές, συνέπειες εισβολών
 - » Συνηθέστερα: ανίχνευση καταχρήσεων, ανίχνευση ανωμαλιών
 - Αντίδραση
 - » ενεργά έναντι παθητικών μέτρων

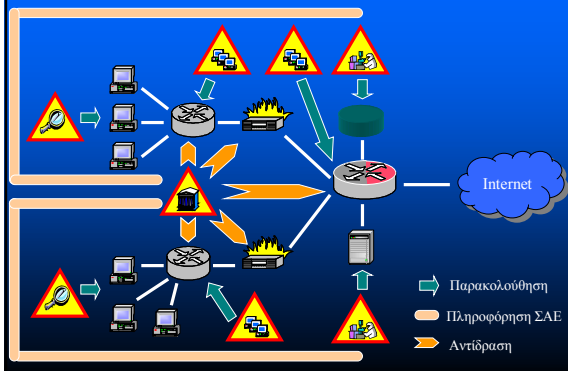
Αρχιτεκτονική

- «Συστέγαση» παρακολουθούμενου και Σ.Α.Ε.
 - Ιδιαίτερα οικονομικό, κυρίως για εγκαταστάσεις με μεγάλους υπολογιστές
 - Αν ο εισβολέας επιτύχει απενεργοποιεί το Σ.Α.Ε.
- Παρακολουθούμενος χωριστά από Σ.Α.Ε.
 - Μεγαλύτερο κόστος
 - Περισσότερη ασφάλεια - ο εισβολέας μπορεί να μην γνωρίζει ούτε την ύπαρξη του Σ.Α.Ε.

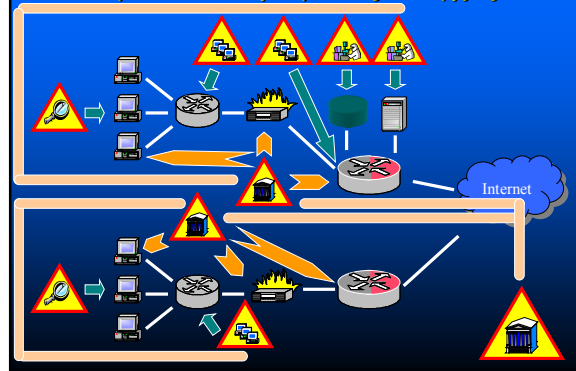
Στόχοι

- Καταλογισμός ευθυνών
 - Λιγότερο εφικτός σε συστήματα με TCP/IP και χαλαρούς μηχανισμούς πιστοποίησης ταυτότητας
 - Αν ξέρω τους υπεύθυνους, αντιμετωπίζω τα πάντα
- Αντίδραση
 - Η δυνατότητα αναγνώρισης των εισβολών και η παρεμπόδισή τους από την επίτευξη του στόχου τους
 - Αρκεί να αντιλαμβάνομαι τις επιθέσεις και να τις σταματάω

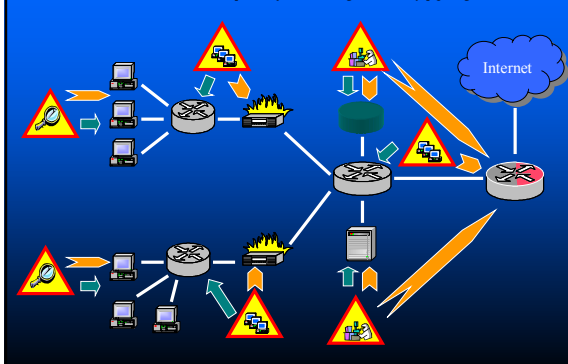
Συγκεντροτική στρατηγική έλεγχου



Ημιαποκεντρωμένος έλεγχος



Αποκεντρωμένος έλεγχος



Χρονισμός

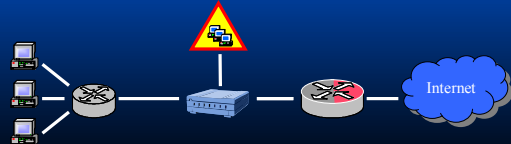
- Χρόνος που μεσολαβεί μεταξύ των συμβάντων και της ανάλυσής τους
 - Πραγματικού χρόνου
 - » τα συμβάντα αναλύονται άμεσα
 - » απαιτούν καλή δικτύωση και ισχυρούς υπολογιστές
 - » δυνατότητα για άμεση αντίδραση
 - Περιοδικά
 - » τα συμβάντα αναλύονται μαζικά
 - » βολικό όταν συστεγάζονται υπολογιστές και Σ.Α.Ε.
 - » δεν έχουν δυνατότητα για άμεση αντίδραση

Πηγές πληροφοριών

- Η κύρια κατηγοριοποίηση είναι βάσει της πηγής συλλογής πληροφορίας
 - Συλλογή από τη δικτυακή κυκλοφορία
 - Συλλογή από στοιχεία συγκεκριμένου υπολογιστή

Συλλογή πληροφοριών από το δίκτυο

- Η πολυπληθέστερη κατηγορία
 - ✓ Με κατάλληλη τοποθέτηση παρακολουθούν και προστατεύουν πολλούς υπολογιστές
 - ✓ Μπορούν να χρησιμοποιούν τεχνικές απόκρυψης, οπότε να είναι «αόρατα» στους εισβολείς

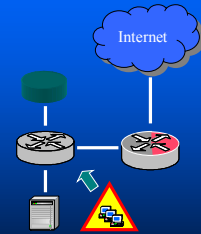


Συλλογή πληροφοριών από το δίκτυο

- ✗ Σε υπερφορτωμένα δίκτυα δεν είναι εύκολο να αναλύσει το Σ.Α.Ε όλα τα πακέτα
 - Υλοποίηση σε υλικό
 - Ανίχνευση υποσυνόλου επιθέσεων
 - Διενέργεια των λιγότερο χρονοβόρων αναλύσεων
- ✗ Η τεχνολογία μεταγωγής δυσχεραίνει την παρακολούθηση
- ✗ Η κρυπτογραφημένη πληροφορία δεν μπορεί να αναλυθεί
- ✗ Δεν γνωρίζουν αν η επίθεση πέτυχε – μόνο ότι έγινε
- ✗ Πολλές υλοποιήσεις έχουν προβλήματα ευστάθειας με επιθέσεις που βασίζονται σε χρήση τμημάτων πακέτων

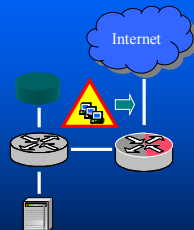
Τοποθέτηση δικτυακών Σ.Α.Ε (1)

- Πίσω από το εξωτερικό firewall
 - ✓ Ανιχνεύουν επιθέσεις που ξεπερνούν την περιμετρική άμυνα
 - ✓ Αποκαλύπτουν ζητήματα ασφάλειας και επιδόσεων του firewall
 - ✓ Ανιχνεύουν επιθέσεις που στοχεύουν στους εξυπηρετές Web ή FTP
 - ✓ Ακόμη και η επίθεση επιτύχει, μπορεί να επισημανθεί πρόβλημα βάσει της εξερχόμενης κυκλοφορίας από το θύμα



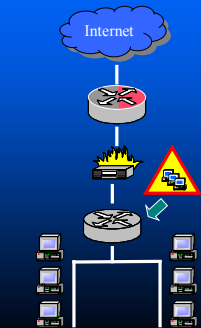
Τοποθέτηση δικτυακών Σ.Α.Ε (2)

- Έξω από το εξωτερικό firewall
 - ✓ Ανιχνεύει και τακτοποιεί και τις επιθέσεις που αντιμετωπίζει το firewall



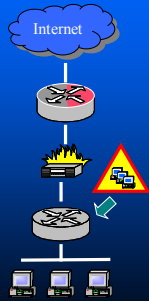
Τοποθέτηση δικτυακών Σ.Α.Ε (3)

- Σε μεγάλους δικτυακούς κόμβους
 - ✓ Εποπτεύει μεγάλο μέρος της δικτυακής κυκλοφορίας → ανίχνευση περισσότερων επιθέσεων
 - ✓ Ανιχνεύει και επιθέσεις «εκ των έσω»



Τοποθέτηση δικτυακών Σ.Α.Ε (4)

- Σε υποδίκτυα μεγάλης σημασίας
- ✓ Προστατεύει τους πιο πολύτιμους πόρους
- ✓ Ιδιαίτερα χρήσιμο σε περιπτώσεις περιορισμένων πόρων για αγορά-εγκατάσταση-λειτουργία Σ.Α.Ε.



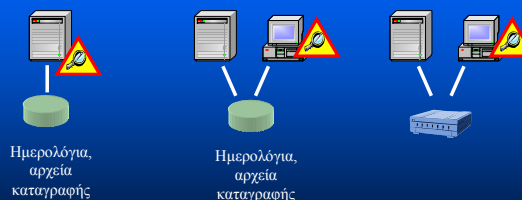
Συλλογή πληροφοριών από συγκεκριμένο υπολογιστή

- Αναλύουν αρχεία ημερολογίου, διεργασίες, αρχεία συστήματος, μνήμη, στοιχεία κατάστασης, ταυτότητες χρηστών
- ✓ Μπορούν να ανιχνεύσουν επιθέσεις που χρησιμοποιούν νόμιμα πακέτα δικτύου
- ✓ Λειτουργούν και με μηχανισμούς κρυπτογράφησης, πάντα όμως σε μη κρυπτογραφημένα δεδομένα
- ✓ Λειτουργούν θαυμάσια σε περιβάλλον μεταγωγής
- ✓ Με ανάλυση των αρχείων καταγραφής ενεργειών μπορούν να αποκαλύψουν δούρειους ίππους ή άλλες προσπάθειες παραβίασης της ασφάλειας

Συλλογή πληροφοριών από συγκεκριμένο υπολογιστή

- ✗ Δυσκολότερη εγκατάσταση και ρύθμιση
 - Εγκατάσταση σε κάθε υπολογιστή
 - Ξεχωριστές πιθανόν ρυθμίσεις
- ✗ Αν παραβιασθεί η ασφάλεια του υπολογιστή, το Σ.Α.Ε. μπορεί να απενεργοποιηθεί
- ✗ Δεν μπορούν να ανιχνεύσουν απόπειρες ανίχνευσης υπηρεσιών στο εταιρικό δίκτυο
- ✗ Υπάρχουν επιθέσεις άρνησης παροχής υπηρεσιών που απενεργοποιούν το Σ.Α.Ε.
- ✗ Αν βασίζονται σε αρχεία καταγραφής λειτουργιών του Λ.Σ., μπορεί να υπάρξει πρόβλημα αποθήκευσης
- ✗ Χρησιμοποιούν υπολογιστικούς πόρους του συστήματος

Λειτουργία σε διαφορετικό υπολογιστή



Τοποθέτηση Σ.Α.Ε. υπολογιστών

- Πρώτα σε κρίσιμους εξυπηρέτες
 - για περιβάλλοντα υψηλής ασφάλειας μετέπειτα εγκατάσταση και σε λοιπούς υπολογιστές
- Ίδια τεχνολογία
- Όταν εγκαθίστανται σε πολλούς υπολογιστές, προτιμώνται προϊόντα με κεντρικοποιημένο σύστημα αναφοράς
- Σχέδιο για τακτικό έλεγχο των ευρημάτων

Συλλογή πληροφοριών από συγκεκριμένες εφαρμογές

- Ειδική περίπτωση της συλλογής πληροφοριών από συγκεκριμένο υπολογιστή
- Συνήθως παρακολουθούν τα ημερολόγια δοσοληψιών ή την επικοινωνία της εφαρμογής
- ✓ Έχοντας αυξημένη γνώση για τη συγκεκριμένη εφαρμογή, μπορούν να διαγνώσουν μεγάλο πλήθος παραβιάσεων
 - Ακόμη και καταχρήσεις δικαιωμάτων
- ✓ Μπορούν να λειτουργήσουν και σε κρυπτογραφημένα περιβάλλοντα

Συλλογή πληροφοριών από συγκεκριμένες εφαρμογές

- Τα ημερολόγια εφαρμογών είναι συνήθως πλημελέστερα προστατευμένα, σε σχέση με αυτά του Λ.Σ.
- Είναι πολύ ειδικού σκοπού
 - Πρέπει να συμπληρώνονται με Σ.Α.Ε. δικτύου ή υπολογιστή

Τεχνικές ανάλυσης συμβάντων

- Ανίχνευση καταχρήσεων
 - Η δημοφιλέστερη τεχνική
 - Εντοπισμός συμβάντων που είναι χαρακτηρισμένα ως «άσχημα»
- Ανίχνευση ανωμαλιών
 - Κυρίως ερευνητική προσπάθεια
 - Προσπάθεια εντοπισμού «μη φυσιολογικών» συμπεριφορών στο σύστημα
- Τα περισσότερα συστήματα χρησιμοποιούν κυρίως ανίχνευση καταχρήσεων με στοιχεία ανίχνευσης ανωμαλιών

Ανίχνευση καταχρήσεων

- Ανάλυση της δραστηριότητας του συστήματος για εντοπισμό συμβάντων ή συνόλων συμβάντων που αντιστοιχούν σε γνωστές επιθέσεις
 - αιτήσεις
 - GET ../..
 - GET <http://www.domain.com/scripts/..\scriptname>σε σύστημα με IIS
 - Σύνδεση από κάποιο IP στη θύρα x του TCP/IP
 - » Ακολουθούμενη από σύνδεση από το ίδιο IP στη θύρα x+1
 - » Ακολουθούμενη από σύνδεση από το ίδιο IP στη θύρα x+2

Ανίχνευση καταχρήσεων

- Γενικώς ανιχνεύουν «απογραφές επιθέσεων»
- Οι πιο προηγμένες τεχνικές χρησιμοποιούν και κάποια «κατάσταση»
- ✓ Πολύ αποτελεσματική τεχνική για ανίχνευση επιθέσεων χωρίς πολλές ψευδείς αναφορές επιθέσεων
- ✓ Ανιχνεύουν έγκαιρα συγκεκριμένες επιθέσεις και εργαλεία ώστε να θωρακιστεί κατάλληλα το σύστημα
- ✓ Κατάλληλα και για διαχειριστές χωρίς ιδιαίτερες τεχνικές γνώσεις

Ανίχνευση καταχρήσεων

- Ανιχνεύουν μόνο τις επιθέσεις για τις οποίες γνωρίζουν – ανάγκη ενημέρωσης
- Οι περισσότερες υλοποιήσεις δεν ανιχνεύουν παραλλαγές γνωστών επιθέσεων

Ανίχνευση ανωμαλιών

- Βασική υπόθεση: η επίθεση *διαφέρει* από την κανονική χρήση
- Χρειάζονται κωδικοποιήσεις της *κανονικής συμπεριφοράς*
 - κατασκευάζονται από ιστορικά στοιχεία που συλλέγονται σε κάποια χρονική περίοδο
 - αφορούν χρήστες, υπολογιστές ή δικτυακές συνδέσεις
- Η παρατηρούμενη συμπεριφορά του κάθε χρήστη συγκρίνεται με την αντίστοιχη κωδικοποίηση κανονικής συμπεριφοράς

Μέτρα και τεχνικές για ανίχνευση ανωμαλιών

- Ανίχνευση κατοφλίου
 - συγκεκριμένα χαρακτηριστικά της συμπεριφοράς χρηστών και του συστήματος εκφράζονται ως πληθάρημοι
 - » πλήθος αρχείων που προσπελούνται σε χρονικό διάστημα, πλήθος σφαλμάτων σύνδεσης, φόρτος ΚΜΕ για συγκεκριμένη διεργασία κ.λπ.
 - » υπάρχουν περιθώρια σφάλματος
 - » τα όρια είναι στατικά ή δυναμικά
 - Στατιστικά, παραμετρικά (το μέγεθος ακολουθεί κατανομή) ή μη (το μέγεθος συνάγεται από ιστορικά στοιχεία)
 - Μέτρα βασισμένα σε κανόνες που ορίζουν αποδεκτές συμπεριφορές αλλά ποιοτικά, όχι ποσοτικά
 - » π.χ. κατάλογοι εγγράφων που χρησιμοποιεί ένας χρήστης
 - Νευρωνικά δίκτυα, γενετικοί αλγόριθμοι κ.λπ.
 - Μόνο οι δύο πρώτες κατηγορίες χρησιμοποιούνται πρακτικά

Αποτίμηση ανίχνευσης ανωμαλιών

- ✓ Μπορούν να ανιχνεύσουν νέους τύπους επιθέσεων
- ✓ Μπορούν να τροφοδοτήσουν τα συστήματα ανίχνευσης καταχρήσεων με κανόνες
- Τάση για δημιουργία ψευδών αναφορών εισβολής
- Χρειάζονται εκτεταμένα στοιχεία για δημιουργία κωδικοποιήσεων «κανονικής συμπεριφοράς»

Αντιδράσεις των Σ.Α.Ε.

- Ενεργές αντιδράσεις
 - Συλλογή περισσότερων πληροφοριών
 - » στοχεύει στην καλύτερη αξιολόγηση της επίθεσης ή και τη συλλογή στοιχείων για νομικές ενέργειες
 - » αύξηση της ευαισθησίας των «αισθητήρων» π.χ. αρχείων καταγραφής, πακέτων δικτύου που αναλύονται κ.λπ.
 - Τροποποίηση περιβάλλοντος
 - » Στοχεύει στο να οδηγήσει την επίθεση σε αποτυχία
 - » Αποστολή πακέτων τερματισμού σύνδεσης, επαναρυθμισμό firewalls και δρομολογητών εισάγοντας απαγορεύσεις για διεθύνσεις IP, θυρών, δικτυακών πρωτοκόλλων, υπηρεσιών ή φυσικών συνδέσεων
 - Αντεπίθεση
 - » Χρήση τεχνικών για αδρανοποίηση του επιτιθέμενου ή συλλογή πληροφοριών για αυτόν
 - » Μπορεί να έχει νομικά προβλήματα, να «θυμώσει» τους εισβολείς ή και να την πληρώσουν αθώοι
 - » *Πάντα με ανθρώπινη επίβλεψη ειδικών*

Αντιδράσεις των Σ.Α.Ε.

- Παθητικές αντιδράσεις
 - Ειδοποιήσεις και συναγερμοί για το προσωπικό
 - » Με κυμαινόμενο βαθμό λεπτομέρειας
 - » Σε χώρο της εφαρμογής, σε παράθυρο μηνύματος, σε συσκευές τηλεειδοποίησης, με μηνύματα σε κινητά
 - » Το ηλεκτρονικό ταχυδρομείο είναι επισφαλές
 - Χρήση του πρωτοκόλλου SNMP
 - » Συνήθως οι αναφορές προωθούνται σε κάποιο σύστημα διαχείρισης δικτύου
 - » Αξιοποιεί περαιτέρω μια δαπανηρή υποδομή (λογισμικού και επικοινωνίας), ολοκληρώνει τις λειτουργίες διαχείρισης, λιγότερο απαιτητικό σε πόρους από μία ενεργό αντίδραση

Σ.Α.Ε.: Αυτοάμυνα

- Προστασία του ίδιου του Σ.Α.Ε. από ανίχνευση, παράκαμψη ή ακρήστευση
 - Μέτρα ώστε το ίδιο το Σ.Α.Ε. να μην γίνεται στόχος
 - Το Σ.Α.Ε. να μην κοινοποιεί την παρουσία του με δικτυακά μηνύματα καθολικής εκπομπής
 - » ακόμη και σε περιπτώσεις συναγερμού
 - Χρήση ξεχωριστών καναλιών επικοινωνίας, κρυπτογράφηση, διακρίβωση ταυτότητας