ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗΝ
ΔΙΟΙΚΗΣΗ &ΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

ΝΙΚΟΛΟΠΟΥΛΟΣ ΦΩΤΗΣ A.M 6807

ΜΑΚΡΙΝΑΣ ΠΑΝΑΓΙΩΤΗΣ A.M 7213

ΜΕΣΟΛΟΓΓΙ, ΟΚΤΩΒΡΙΟΣ 2003

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΗΝ ΔΙΟΙΚΗΣΗ & ΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ»

ΝΙΚΟΛΟΠΟΥΛΟΣ ΦΩΤΗΣ Α.Μ 6807

ΜΑΚΡΙΝΑΣ ΠΑΝΑΓΙΩΤΗΣ Α.Μ 7213

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΑΚΡΙΔΑ ΚΑΤΕΡΙΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1:Εισαγωγή **4**

1.1 Σκοπός αυτής της εργασίας 4
1.2 Ορισμοί 4
1.3 Βασική προσέγγιση 5
1.4 Αξιολόγηση του κινδύνου 6
1.4.1Εισαγωγή 6
1.4.2Προσδιορισμός των πόρων 6
1.4.3Προσδιορισμός των απειλών 7

ΚΕΦΑΛΑΙΟ 2:Πολιτικές ασφάλειας **8**

2.1 Τι είναι μια πολιτική ασφάλειας και γιατί πρέπει να υπάρχει; 8
2.1.1 Καθορισμός μιας πολιτικής ασφάλειας 9
2.1.2 Στόχοι μιας πολιτικής ασφάλειας 9
2.1.3 Ποιος πρέπει να αναμιχθεί κατά τη διαμόρφωση της πολιτικής 9
2.2 Διαμόρφωση μιας σωστής πολιτικής ασφάλειας 10
2.3 Κρατώντας «εύκαμπτη» την πολιτική 11

ΚΕΦΑΛΑΙΟ 3: Αρχιτεκτονική **13**

3.1 Στόχοι 13
3.1.1 Καθορισμένα σχέδια ασφάλειας 13
3.1.2 Χωρισμός των υπηρεσιών 13
3.1.3 Denny all -Allow all 14
3.1.4 Προσδιορισμός των πραγματικών αναγκών για τις υπηρεσίες 15
3.2 Διαμόρφωση δικτύων και υπηρεσιών 15
3.2.1 Προστασία της υποδομής 16
3.2.2 Προστασία του δικτύου 16
3.2.3 Προστασία των υπηρεσιών 17
3.2.3.1 Name Servers (DNS και NIS(+)) 18
3.2.3.2 Password/Key Servers (NIS(+) και KDC) 19
3.2.3.3 Authentication/Proxy Servers (SOCKS,FWTK) 19
3.2.3.4 Ηλεκτρονικό ταχυδρομείο 19
3.2.3.5 World Wide Web (WWW) 20
3.2.3.6 Μεταφορά αρχείων (FTP,TFTP) 20
3.2.3.7 NFS 21
3.2.4 Προστασία της ασφάλειας 21
3.3 Η έννοια του firewall του Internet 21
3.3.1 Διαλογή πακέτων 23
3.3.2 Χρήση φίλτρων πακέτων για τη δημιουργία firewall 24

ΚΕΦΑΛΑΙΟ 4: Υπηρεσίες & διαδικασίες ασφάλειας.....27

4.1 Καθορισμός όρων.....27
4.2 Πιστοποίηση.....28
4.2.1 One-Time κωδικοί πρόσβασης.....28
4.2.2 Kerberos.....29
4.2.3 Επιλογή και προστασία των μυστικών Tokens και PINs.....29
4.2.4 Διαβεβαίωση κωδικού πρόσβασης.....30
4.3 Προσεγγίσεις για την πιστοποίηση μηνύματος.....31
4.3.1 Πιστοποίηση χρησιμοποιώντας συμβατική κρυπτογράφηση.....32
4.3.1.1 Πιστοποίηση ταυτότητας με ψηφιακές υπογραφές.....32
4.3.2 Πιστοποίηση μηνύματος χωρίς συμβατική κρυπτογράφηση.....33
4.3.2.1 Κώδικας πιστοποίησης μηνύματος.....34
4.3.2.2 Μονόδρομη συνάρτηση τεμαχισμού.....35
4.3.3 RADIUS.....35
4.3.4 TACACS+.....37
4.4 Εμπιστευτικότητα.....37
4.4.1 Κρυπτογράφηση και εμπιστευτικότητα.....38
4.4.1.1 Κρυπτογράφηση δημόσιου κλειδιού.....38
4.5 Ακεραιότητα.....39
4.5.1 Μηχανισμοί ακεραιότητας.....39
4.6 Εξουσιοδότηση.....40
4.6.1 Τεχνολογίες εξουσιοδότησης.....40
4.6.1.1 Καμία εξουσιοδότηση.....40
4.6.1.2 Μηχανισμοί εξουσιοδότησης που είναι ευάλωτοι στις παθητικές επιθέσεις.....41
4.6.1.3 Ευάλωτοι μηχανισμοί εξουσιοδότησης στις ενεργές επιθέσεις.....41
4.6.1.4 Ανθεκτικοί μηχανισμοί εξουσιοδότησης σε ενεργές επιθέσεις.....42
4.7 Πρόσβαση.....42
4.7.1 Φυσική πρόσβαση.....42
4.7.2 Walk-up συνδέσεις δικτύων.....43
4.7.3 Άλλες τεχνολογίες δικτύων.....43
4.7.4 Modems.....43
4.7.4.1 Διαχείριση των γραμμών Modem.....43
4.7.4.2 Οι Dial-in χρήστες πρέπει να επικυρώνονται.....44
4.7.4.3 Ικανότητα επανάκλησης.....44
4.7.4.4 Όλα τα Logins πρέπει να καταγράφονται.....45
4.7.4.5 Προσεκτική επιλογή του Opening Banner.....45
4.7.4.6 Επικύρωση Dial-out.....45
4.7.4.7 Ενδυνάμωση του προγραμματισμού του modem 'Bullet-proof'.....46
4.8 Υπηρεσίες καταγραφής και ανάλυσης δικτυακής δραστηριότητας.....46
4.8.1 Εισαγωγή.....46
4.8.2 Παρουσίαση εφαρμογών network accounting.....47
4.8.3 Διοικητικοί στόχοι ελέγχου.....48
4.8.3.1 Ανάλυση τάσης και προγραμματισμός δυνατοτήτων.....48
4.8.3.2 Accounting.....48
4.8.4 Τι πρέπει να συλλεχθεί.....49
4.8.5 Διαδικασία συλλογής.....49
4.8.6 Φόρτος συλλογής στοιχείων.....50
4.8.7 Χειρισμός και συντήρηση των στοιχείων ελέγχου.....50
4.8.8 Νομικά ζητήματα.....51

4.8.9 Εκτιμήσεις ασφάλειας και Tunneling....51
4.8.9.1 Κλοπή και άρνηση υπηρεσίας....52
4.8.9.2 Εφαρμογές του IPSec....53
4.8.9.3 Ο Σκοπός του IPSec....54
4.8.9.4 Αλληλεπιδράσεις IPSec και Tunneling....55
4.8.9.5 Καταγραφή....56
4.8.10 Πρωτόκολλα Ελέγχου (accounting protocols)....56
4.8.10.1 RADIUS....57
4.8.10.2 TACACS+....57
4.8.10.3 SNMP....58
4.9 Εξασφάλιση των Backups....60

ΚΕΦΑΛΑΙΟ 5: Χειρισμός ασφάλειας....61

5.1 Εισαγωγή....61
5.2 Προετοιμασία και προγραμματισμός για το χειρισμό ενός γεγονότος....62
5.3 Ειδοποίηση και σημεία επαφής....65
5.3.1 Τοπικοί διευθυντές και προσωπικό....65
5.3.2 Επιβολή νόμου και εξεταστικές αντιπροσωπείες....67
5.3.3 Ομάδες διαχείρισης γεγονότων ασφάλειας υπολογιστών....69
5.3.4 Επηρεασμένοι και αναμεμιγμένοι οργανισμοί....69
5.3.5 Εσωτερικές επικοινωνίες....70
5.3.6 Δημόσιες σχέσεις-δελτία τύπου....71
5.4 Προσδιορισμός ενός γεγονότος....72
5.4.1 Είναι πραγματικό;....72
5.4.2 Τύποι και πεδίο γεγονότων....73
5.4.3 Αξιολόγηση της ζημίας και της έκτασής της....74
5.5 Χειρισμός ενός γεγονότος....74
5.5.1 Τύποι ενημερώσεων και ανταλλαγή των πληροφοριών....75
5.5.2 Προστασία στοιχείων και ημερολογίων δραστηριότητας....76
5.5.3 Περιορισμός....77
5.5.4 Χτυπώντας την αιτία....78
5.5.5 Αποκατάσταση....79
5.5.6 Τελικό στάδιο....79
5.6 Συνέπειες ενός γεγονότος....80
5.7 Ευθύνες....80
5.7.1 Καλή συμπεριφορά στο Διαδίκτυο....80
5.7.2 Απάντηση του διαχειριστή στα γεγονότα....81

ΚΕΦΑΛΑΙΟ 6: Τρέχουσες δραστηριότητες....82

ΚΕΦΑΛΑΙΟ 7: Εργαλεία και τοποθεσίες....83

ΚΕΦΑΛΑΙΟ 8: Κατάλογοι διευθύνσεων και άλλοι πόροι....85

8.1 Κατάλογοι διευθύνσεων....85
8.2 Ομάδες πληροφόρησης USENET....86
8.3 Σελίδες στο World Wide Web....86

ΒΙΒΛΙΟΓΡΑΦΙΑ....88

Κεφάλαιο 1. Εισαγωγή

Σε αυτή την εργασία, θα εξεταστεί το σημαντικό ζήτημα της ασφάλειας πληροφορίας. Θα παρουσιαστούν τα χαρακτηριστικά των προβλημάτων της ασφάλειας, θα εξεταστούν τα επίπεδα ασφάλειας που αναμένουν οι χρήστες από ένα δικτυακό σύστημα, και θα εξηγηθούν οι βασικές τεχνικές που χρησιμοποιούνται για τη βελτίωση της ασφάλειας του δικτύου.

1.1 Σκοπός αυτής της εργασίας

Αυτή η εργασία είναι ένας οδηγός για τον καθορισμό των πολιτικών ασφάλειας υπολογιστών για οργανισμούς που έχουν συστήματα στο διαδίκτυο (εντούτοις, οι πληροφορίες που παρέχονται πρέπει επίσης να είναι χρήσιμες σε οργανισμούς που δεν συνδέονται ακόμα με το Διαδίκτυο). Αυτή η εργασία απαριθμεί τα ζητήματα και τους παράγοντες που ένας οργανισμός πρέπει να εξετάσει κατά τη ρύθμιση των πολιτικών του. Υποβάλλει διάφορες συστάσεις και παρέχει συμβουλές στους σχετικούς οργανισμούς. Επίσης σε συνδυασμό με την ανάλυση πολιτικών ασφάλειας θα εξεταστούν σε βάθος οι διαδικασίες και οι υπηρεσίες ασφάλειας πληροφορίας, ο χειρισμός γεγονότων ασφάλειας καθώς και εργαλεία και τοποθεσίες σχετικές με την ασφάλεια.

Προκειμένου να υπάρξει ένα αποτελεσματικό σύνολο πολιτικών και διαδικασιών που εφαρμόζονται για την ασφάλεια, ένας οργανισμός θα πρέπει να λάβει πολλές αποφάσεις, να βρει τα οφέλη, να τα αξιολογήσει και να εφαρμόσει αυτές τις πολιτικές.

Αυτοί που θα πρέπει να λάβουν γνώση της παραπάνω πληροφορίας είναι διαχειριστές συστημάτων και δικτύων, καθώς και οι υπεύθυνοι για τη λήψη αποφάσεων (χαρακτηριστικά "μεσαία στελέχη") επί των οργανισμών. Για συντομία, θα χρησιμοποιηθεί ο όρος "διαχειριστής" σε όλο το παρόν έγγραφο για την αναφορά στους διαχειριστές συστημάτων και δικτύων.

Η παρούσα εργασία δεν απευθύνεται στους προγραμματιστές ή σε εκείνους που προσπαθούν να δημιουργήσουν ασφαλή προγράμματα ή συστήματα. Εστιάζει στις πολιτικές και τις διαδικασίες που πρέπει να είναι σε ισχύ για να υποστηρίξουν τα τεχνικά χαρακτηριστικά γνωρίσματα ασφάλειας που ένας οργανισμός μπορεί να περιλαμβάνει. Κατά κύριο λόγο αυτή η εργασία απευθύνεται σε οργανισμούς που είναι μέλη της κοινότητας Διαδικτύου.

Εντούτοις, πρέπει να είναι χρήσιμη σε οποιοδήποτε οργανισμό που επιτρέπει την επικοινωνία με άλλους οργανισμούς. Σαν γενικός οδηγός για τις πολιτικές ασφάλειας, μπορεί επίσης να είναι χρήσιμη σε οργανισμούς με απομονωμένα συστήματα.

1.2 Ορισμοί

Ένας "οργανισμός" είναι οποιαδήποτε οργάνωση που της ανήκουν υπολογιστές ή άλλοι δικτυακοί πόροι. Αυτοί οι πόροι περιλαμβάνουν τους host (ξενιστές) υπολογιστές που οι χρήστες χρησιμοποιούν, δρομολογητές, τελικούς κεντρικούς υπολογιστές, PCs ή άλλες συσκευές που έχουν πρόσβαση στο Διαδίκτυο.

Ένας οργανισμός μπορεί να είναι ένας τελικός χρήστης των υπηρεσιών Διαδικτύου ή ενός φορέα παροχής υπηρεσιών όπως ένα δίκτυο μεσαίου επιπέδου.
Εντούτοις, το μεγαλύτερο μέρος της εστίασης αυτής της εργασίας απευθύνεται σε εκείνους τους τελικούς χρήστες των υπηρεσιών Διαδικτύου.
Υποθέτουμε ότι ένας οργανισμός έχει τη δυνατότητα να θέσει τις πολιτικές και τις διαδικασίες για την ίδια με τη συμφωνία και την υποστήριξη από εκείνους που είναι κύριοι ,πραγματικά, κάτοχοι των πόρων. Υποτίθεται ότι οι οργανισμοί που είναι μέρη μεγαλύτερων οργανώσεων ξέρουν πότε πρέπει να συμβουλευθούν, να συνεργαστούν, ή να πάρουν συστάσεις από, τη μεγαλύτερη οντότητα.

Το "**Διαδίκτυο**" είναι μια συλλογή χιλιάδων δικτύων που συνδέονται με ένα κοινό σύνολο πρωτοκόλλων και καθιστούν δυνατό για τους χρήστες οποιονδήποτε δικτύων να επικοινωνήσουν, ή να χρησιμοποιήσουν διάφορες υπηρεσίες

Ο όρος "**διαχειριστής**" χρησιμοποιείται για να καλύψει όλους εκείνους τους ανθρώπους που είναι αρμόδιοι για την καθημερινή λειτουργία των πόρων συστημάτων και δικτύων. Μπορεί να είναι διάφορα άτομα ή οργανώσεις.

Ο όρος "**διαχειριστής ασφάλειας**" χρησιμοποιείται για να καλύψει όλους εκείνους τους ανθρώπους που είναι αρμόδιοι για την ασφάλεια των πληροφοριών.
Σε μερικούς οργανισμούς αυτός ο όρος μπορεί να συνδυαστεί με τον όρο του "διαχειριστή" παραπάνω, οπότε πρέπει να τονιστεί ο διαχωρισμός.

Ο όρος "**decision maker**" αναφέρεται σε εκείνους τους ανθρώπους που θέτουν ή εγκρίνουν την πολιτική σε έναν οργανισμό. Αυτοί είναι συχνά (αλλά όχι πάντα) οι άνθρωποι που είναι κύριοι των πόρων.

1.3 Βασική προσέγγιση

Αυτή η εργασία έχει γραφτεί για να παρέχει τις βασικές οδηγίες στην ανάπτυξη ενός σχεδίου ασφάλειας για έναν οργανισμό.
Μια γενικά αποδεκτή προσέγγιση που ακολουθεί προτείνεται από Fites, et. al. [Fites 1989] και περιλαμβάνει τα ακόλουθα βήματα:

(1) Προσδιορίζουμε τι προσπαθούμε να προστατεύσουμε.
(2) Καθορίζουμε τι πρέπει να προστατεύσουμε .
(3) Καθορίζουμε πόσο πιθανές είναι οι απειλές.
(4) Εφαρμόζουμε μέτρα που θα προστατεύσουν τα συστήματα μας κατά τρόπο οικονομικώς αποδοτικό.
(5) Αναθεωρούμε τη διαδικασία συνεχώς και κάνουμε βελτιώσεις κάθε φορά που βρίσκουμε μια αδυναμία.

Δίνεται μεγαλύτερη βαρύτητα στον τέταρτο παράγοντα χωρίς να παραβλέπονται τα υπόλοιπα.
Για να δαπανηθούν πόροι για την ασφάλεια ενός συστήματος θα πρέπει το συνολικό ύψος της δαπάνης να είναι μικρότερο από τη ζημιά που θα προκαλούνταν στο σύστημα εάν αυτό παρέμενε απροστάτευτο.

Οι παράμετροι του κόστους εκφράζονται στο πραγματικό χρηματικό κόστος, τη φήμη, την εμπιστοσύνη, και άλλα λιγότερο προφανή μέτρα. Αυτό θα μπορούσε να είναι δύσκολο ακολουθώντας αυτόν τον κανόνα χωρίς λογική γνώση αυτού που προστατεύετε και τι πιθανές απειλές υπάρχουν.

1.4 Αξιολόγηση του κινδύνου

1.4.1 Εισαγωγή

Ένας από τους σημαντικότερους λόγους για την ανάπτυξη μιας πολιτικής ασφάλειας υπολογιστών είναι να εξασφαλιστεί ότι οι πόροι που ξοδεύονται για την ασφάλεια παράγουν τα οικονομικώς αποδοτικά οφέλη.
Αν και αυτό είναι προφανές, είναι δυνατό να παραπλανά σε σχέση με την πραγματική προσπάθεια που απαιτείται. Για παράδειγμα, υπάρχει πολλή δημοσιότητα για τους εισβολείς στα συγκροτήματα ηλεκτρονικών υπολογιστών αλλά οι περισσότερες έρευνες για την ασφάλεια υπολογιστών δείχνουν ότι η πραγματική απώλεια από "τα μέλη" είναι πολύ μεγαλύτερη.
Η ανάλυση κινδύνου περιλαμβάνει τον καθορισμό του τι πρέπει να προστατεύετε, από τι χρειάζεται να προστατεύετε, και πώς πρέπει να προστατεύετε. Επίσης μπορεί να χαρακτηριστεί ως η διαδικασία ελέγχου όλων των κινδύνων, ταξινομώντας τους έπειτα ανάλογα με το επίπεδο ισχύς τους. Αυτή η διαδικασία περιλαμβάνει τη λήψη των οικονομικώς αποδοτικών αποφάσεων σχετικά με αυτό που θέλουμε να προστατευτεί.
Όπως αναφέρεται ανωτέρω, δεν πρέπει να ξοδευτούν περισσότερα για να προστατευτεί κάτι, από ότι πραγματικά αξίζει.
Μια πλήρης επεξεργασία της ανάλυσης κινδύνου είναι έξω από το πεδίο ανάλυσης της εργασίας.
Εντούτοις, υπάρχουν δύο στοιχεία μιας ανάλυσης κινδύνου που θα καλυφθούν εν συντομία στα επόμενα δύο τμήματα:

(1) Προσδιορισμός των πόρων
(2) Προσδιορισμός των απειλών

Για κάθε πόρο, βασικοί στόχοι της ασφάλειας είναι: διαθεσιμότητα, εμπιστευτικότητα, και ακεραιότητα.
Κάθε απειλή πρέπει να εξεταστεί στοχεύοντας στο πώς θα μπορούσε να έχει επιπτώσεις σε αυτούς τους οργανισμούς.

1.4.2 Προσδιορισμός των πόρων

Σε μια ανάλυση κινδύνου πρέπει να προσδιοριστούν όλα οι πόροι που πρέπει να προστατευθούν. Μερικοί πόροι είναι προφανής, όπως οι πολύτιμες ιδιόκτητες πληροφορίες, η πνευματική ιδιοκτησία, και όλα τα διάφορα κομμάτια του υλικού αλλά, μερικοί αγνοούνται, όπως οι άνθρωποι που χρησιμοποιούν τα συστήματα.

Η απαρίθμηση όλων των πόρων που θα μπορούσαν να επηρεαστούν από ένα πρόβλημα ασφάλειας είναι εξαιρετικής σημασίας.
Ένας κατάλογος κατηγοριών προτείνεται από Pfleeger [Pfleeger 1989]

Αυτός ο κατάλογος προσαρμόζεται σύμφωνα με τα παρακάτω:

(1)**Υλικό**: CPUs, πίνακες, πληκτρολόγια, τερματικά, τερματικοί σταθμοί, προσωπικοί υπολογιστές, εκτυπωτές, δίσκοι κινήσεις, γραμμές επικοινωνίας, τελικοί κεντρικοί υπολογιστές, δρομολογητές.

(2)**Λογισμικό**: προγράμματα πηγής, προγράμματα αντικειμένου, διαγνωστικά προγράμματα, λειτουργικά συστήματα, προγράμματα επικοινωνίας.

(3)**Δεδομένα** : κατά τη διάρκεια της εκτέλεσης, που αποθηκεύεται on-line, που αρχειοθετούνται off-line, backups, αρχεία καταγραφής, βάσεις δεδομένων, και κατά τη μεταφορά μέσα επικοινωνίας

(4)**Άνθρωποι**: χρήστες, διαχειριστές, συντηρητές υλικού.

(5)**Τεκμηρίωση**: στα προγράμματα, υλικό, συστήματα, τοπικοί διαχειριστικοί οργανισμοί.

(6)**Προμήθειες**: έγγραφα, φόρμες, μαγνητικά μέσα.

1.4.3 Προσδιορισμός των απειλών

Μόλις προσδιοριστούν οι πόροι που απαιτούν την προστασία, είναι απαραίτητο να προσδιοριστούν οι απειλές σε εκείνους τους πόρους.
Οι απειλές μπορούν έπειτα να εξεταστούν για να καθοριστεί ποια πιθανότητα υπάρχει για απώλεια.
Βοηθά να εξεταστεί από ποιες απειλές προσπαθούμε να προστατεύσουμε τους πόρους μας. Παρακάτω αναφέρονται οι κλασικές απειλές που πρέπει να εξεταστούν.
Ανάλογα με τον οργανισμό, θα υπάρξουν πιο συγκεκριμένες απειλές που πρέπει να προσδιοριστούν και να εξεταστούν.

(1) Αναρμόδια πρόσβαση στους πόρους ή και τις πληροφορίες

(2) Χωρίς κίνητρο ή και αναρμόδια κοινοποίηση πληροφοριών

(3) Άρνηση υπηρεσίας

Κεφάλαιο 2. Πολιτικές ασφάλειας

2.1 Τι είναι μια πολιτική ασφάλειας και γιατί πρέπει να υπάρχει;

Οι αποφάσεις που παίρνονται σχετικά με την ασφάλεια, μπορεί να μην έχουν το επιθυμητό αποτέλεσμα, δεδομένου ότι ο διαχειριστής καθορίζει κατά ένα μεγάλο μέρος πόσο ασφαλές ή επισφαλές είναι το δίκτυό, ποιες λειτουργίες προσφέρει το δίκτυο, και πόσο εύκολο είναι να χρησιμοποιηθεί το δίκτυο. Εντούτοις, δεν μπορούν να ληφθούν καλές αποφάσεις για την ασφάλεια χωρίς πρώτα να καθοριστούν οι στόχοι ασφάλειας .
Έως ότου καθοριστούν οι στόχοι ασφάλειας, δεν μπορεί να υπάρξει αποτελεσματική χρήση οποιασδήποτε συλλογής εργαλείων ασφάλειας επειδή απλά δεν ξέρουμε τι πρέπει να ελεγχθεί και ποιοι περιορισμοί πρέπει να επιβληθούν.
Παραδείγματος χάριν, οι στόχοι που πρέπει να επιδιωχθούν θα είναι πιθανώς πολύ διαφορετικοί από τους στόχους ενός προμηθευτή προϊόντων.
Οι προμηθευτές προσπαθούν να διαμορφώσουν τα προϊόντα τους όσο-το-δυνατόν απλούστερα, που υπονοεί ότι οι προεπιλεγμένες διαμορφώσεις θα είναι συχνά πιο ανοικτές σε επίθεση(δηλ. πιο επισφαλής).
Ενώ το γεγονός αυτό το καθιστά ευκολότερο να εγκατασταθούν νέα προϊόντα, αφήνει τα συστήματα, και άλλα συστήματα μέσω αυτών, ανοικτά σε οποιοδήποτε χρήστη.
Οι στόχοι θα καθοριστούν κατά ένα μεγάλο μέρος από τα ακόλουθα:

(1)**Υπηρεσίες που δημιουργούν κινδύνους ασφάλειας.**
Κάθε υπηρεσία που προσφέρεται στους χρήστες εγκυμονεί κινδύνους ασφάλειας. Σε μερικές υπηρεσίες ο κίνδυνος αντισταθμίζει το όφελος της υπηρεσίας και ο διαχειριστής μπορεί να επιλέξει να σταματήσει την υπηρεσία παρά να προσπαθήσει να την εξασφαλίσει.

(2) **Ευκολία χρήσης εναντίον ασφάλειας** .
Η χρησιμοποίηση του ευκολότερου συστήματος θα επέτρεπε την πρόσβαση σε οποιοδήποτε χρήστη και δεν θα απαιτούσε κανέναν κωδικό πρόσβασης δηλαδή δεν θα υπήρχε καμία ασφάλεια. Η ανάγκη ύπαρξης κωδικών πρόσβασης καθιστά το σύστημα λιγότερο φιλικό, αλλά ασφαλέστερο. Η χρήση των παραγόμενων από συσκευή one-time κωδικών πρόσβασης καθιστά το σύστημα ακόμα λιγότερο φιλικό, αλλά ασφαλέστερο.

(3) **Κόστος ασφάλειας εναντίον κινδύνου απώλειας** .
Υπάρχουν πολλές διαφορετικές δαπάνες στην ασφάλεια: χρηματικές (δηλ. το κόστος του υλικού και του λογισμικού ασφάλειας όπως τα firewall και οι one-time γεννήτριες κωδικού πρόσβασης), απόδοση (δηλ. η κρυπτογράφηση και η αποκρυπτογράφηση παίρνουν χρόνο), και ευκολία χρήσης. Υπάρχουν επίσης πολλά επίπεδα κινδύνου: απώλεια μυστικότητας (δηλ. η ανάγνωση των πληροφοριών από αναρμόδια άτομα), απώλεια στοιχείων (δηλ. η δωροδοκία ή η εξάλειψη των πληροφοριών), και η απώλεια υπηρεσίας (π.χ. χρήση των υπολογιστικών πόρων, και άρνηση της πρόσβασης στο δίκτυο). Κάθε τύπος κόστους πρέπει να σταθμιστεί ενάντια σε κάθε τύπο απώλειας.

Οι στόχοι πρέπει να κοινοποιηθούν σε όλους τους χρήστες, το προσωπικό διαδικασιών, και τους διαχειριστές μέσω ενός συνόλου κανόνων ασφάλειας, αποκαλούμενου "πολιτική ασφάλειας."
Χρησιμοποιούμε αυτόν τον όρο, παρά τον στενότερο όρο "πολιτική ασφάλειας υπολογιστών" δεδομένου ότι το πεδίο περιλαμβάνει όλους τους τύπους τεχνολογίας πληροφοριών.

2.1.1 Καθορισμός μιας πολιτικής ασφάλειας

Μια πολιτική ασφάλειας είναι μια δήλωση των κανόνων τους οποίους πρέπει να τηρήσουν οι άνθρωποι στους οποίους δίνεται πρόσβαση στους πόρους μιας οργάνωσης.

2.1.2 Στόχοι μιας πολιτικής ασφάλειας

Ο κύριος στόχος μιας πολιτικής ασφάλειας είναι να ενημερωθούν οι χρήστες, το προσωπικό και οι διαχειριστές για τις απαιτήσεις που υπάρχουν γύρω από την πρόσβαση στους πόρους τεχνολογίας και στις πληροφορίες.
Η πολιτική πρέπει να διευκρινίσει τους μηχανισμούς μέσω των οποίων αυτές οι απαιτήσεις μπορούν να καλυφθούν. Ένας άλλος στόχος είναι να παρασχεθεί μια βασική γραμμή κατά την οποία θα αποκτηθούν, θα διαμορφωθούν και θα ελεγχθούν τα συστήματα ηλεκτρονικών υπολογιστών και τα δίκτυα σύμφωνα με αυτή την πολιτική.
Επομένως είναι ανώφελη η χρήση ενός συνόλου εργαλείων ασφάλειας χωρίς την ύπαρξη μιας πολιτικής ασφάλειας. Μια πολιτική χρήσης (AUP) μπορεί επίσης να είναι μέρος μιας πολιτικής ασφάλειας.
Πρέπει να εξηγεί τι οι χρήστες πρέπει ή δεν πρέπει να κάνουν στα διάφορα μέρη του συστήματος, συμπεριλαμβανομένου του τύπου κυκλοφορίας που έχει την άδεια στα δίκτυα.
Το AUP πρέπει όσο το δυνατόν περισσότερο να αποφεύγει την ασάφεια ή την παρανόηση. Παραδείγματος χάριν, ένα AUP να απαριθμεί οποιεσδήποτε απαγορευμένες ομάδες πληροφόρησης USENET.

2.1.3 Ποιος πρέπει να αναμιχθεί κατά τη διαμόρφωση της πολιτικής

Για να είναι μια πολιτική ασφάλειας κατάλληλη και αποτελεσματική, πρέπει να έχει την αποδοχή και την υποστήριξη όλων των υπαλλήλων μέσα στην οργάνωση.
Είναι ιδιαίτερα σημαντικό η διοίκηση να υποστηρίζει πλήρως την πολιτική ασφάλειας. Ακολουθεί ένας κατάλογος ατόμων που πρέπει να συμμετέχουν στη δημιουργία και την αναθεώρηση των πολιτικών ασφάλειας:

(1) Διαχειριστής ασφάλειας
(2) Τεχνικό προσωπικό
(3) Διαχειριστές μεγάλων ομάδων χρηστών μέσα στην οργάνωση (π.χ., επιχειρησιακά τμήματα, τμήμα πληροφορικής μέσα σε ένα πανεπιστήμιο, κ.λπ....)

(4) Ομάδα απάντησης ασφάλειας
(5) Αντιπρόσωποι των ομάδων χρηστών που επηρεάζονται από την πολιτική ασφάλειας
(6) Αρμόδια διαχείριση
(7) Νομικό συμβούλιο (εάν θεωρηθεί απαραίτητο)

Ο ανωτέρω κατάλογος είναι αντιπροσωπευτικός πολλών οργανώσεων.
Η ιδέα είναι να υπάρχει αντιπροσώπευση από τους βασικούς συμμέτοχους, τη διαχείριση, που έχει την αρχή προϋπολογισμών και πολιτικής, το τεχνικό προσωπικό που ξέρει τι μπορεί και δεν μπορεί να υποστηριχθεί, και το νομικό συμβούλιο που ξέρει τις νομικές επιπτώσεις των διάφορων πολιτικών επιλογών. Εάν θέλουμε να πετύχουν οι προκύπτουσες πολιτικές, με την ευρύτερη πιθανή αποδοχή, η ανάμειξη αυτής της ομάδας είναι σημαντική.
Πρέπει επίσης να αναφερθεί ότι ο ρόλος του νομικού συμβουλίου ποικίλει επίσης από χώρα σε χώρα.

2.2 Διαμόρφωση μιας σωστής πολιτικής ασφάλειας

Τα χαρακτηριστικά μιας σωστής πολιτικής ασφάλειας είναι:

(1) Πρέπει να είναι εκτελέσιμη μέσω των διαδικασιών διαχείρισης συστημάτων, της έκδοσης αποδεκτών οδηγιών χρήσης, ή άλλων κατάλληλων μεθόδων.
(2) Πρέπει να είναι δυνατόν να επιβληθεί με εργαλεία ασφάλειας, όπου απαιτείται, και με κυρώσεις, όπου η πρόληψη δεν είναι τεχνικά εφικτή.
(3) Πρέπει σαφώς να καθορίζει τους τομείς ευθύνης για τους χρήστες, τους διαχειριστές, και τη διοίκηση.

Τα συστατικά μιας σωστής πολιτικής ασφάλειας περιλαμβάνουν:

(1)Οδηγίες για αγορά τεχνολογίας υπολογιστών που διευκρινίζουν τα απαιτούμενα, ή επιθυμητά, χαρακτηριστικά γνωρίσματα ασφάλειας. Αυτές πρέπει να συμπληρώσουν τις υπάρχουσες πολιτικές και τις οδηγίες αγοράς.
(2) Μια πολιτική μυστικότητας που καθορίζει τις λογικές προσδοκίες της μυστικότητας σχετικά με ζητήματα όπως ζητήματα ελέγχου του ηλεκτρονικού ταχυδρομείου, καταγραφής των logins, και την πρόσβαση στα αρχεία των χρηστών.
(3) Μια πολιτική πρόσβασης που καθορίζει τα δικαιώματα πρόσβασης και τα προνόμια για να προστατεύσει τους πόρους από την απώλεια ή την κοινοποίηση με τη διευκρίνιση αποδεκτών οδηγιών χρήσης για τους χρήστες, το προσωπικό διαδικασιών, και τη διαχείριση. Πρέπει να παρέχει τις οδηγίες για τις μεταδόσεις στοιχείων μέσω εξωτερικών συνδέσεων, που συνδέουν συσκευές με ένα δίκτυο, και που προσθέτουν νέο λογισμικό στα συστήματα.
Πρέπει επίσης να διευκρινίσει οποιαδήποτε απαραίτητα μηνύματα ανακοίνωσης (π.χ. τα μηνύματα σύνδεσης πρέπει να παρέχουν προειδοποιήσεις για τον εξουσιοδοτημένο έλεγχο χρήσης και γραμμών, και να μην εμφανίζει απλά "Welcome").
(4) Μια πολιτική υπευθυνότητας που καθορίζει τις ευθύνες των χρηστών, του προσωπικού διαδικασιών, και της διαχείρισης. Πρέπει να διευκρινίσει μια ικανότητα ελέγχου καταγραφής, και να παρέχει οδηγίες διαχείρισης (δηλ., τι να κάνει και ποιοι να έρθουν σε επαφή εάν ανιχνεύεται μια πιθανή παραβίαση).

(5) Μια πολιτική επικύρωσης που καθιερώνει την εμπιστοσύνη μέσω μιας αποτελεσματικής πολιτικής κωδικού πρόσβασης, και με τον καθορισμό οδηγιών για την επικύρωση από απομακρυσμένη θέση και τη χρήση των συστημάτων επικύρωσης (π.χ., one-time κωδικοί πρόσβασης και τα συστήματα που τους παράγουν).
(6) Μια δήλωση διαθεσιμότητας που θέτει τις προσδοκίες των χρηστών για τη διαθεσιμότητα των πόρων. Πρέπει να αντιμετωπίσει τα ζητήματα πλεονασμού και αποκατάστασης, καθώς επίσης και να καθορίσει τις ώρες λειτουργίας και τις περιόδους διακοπής συντήρησης.
(7) Μια πολιτική συντήρησης συστημάτων & δικτύων που να περιγράφει πώς οι εσωτερικοί και οι εξωτερικοί υπεύθυνοι συντήρησης έχουν την άδεια να χειριστούν και να έχουν πρόσβαση στην τεχνολογία. Ένα σημαντικό θέμα που εξετάζεται εδώ είναι εάν η από απόσταση συντήρηση επιτρέπεται και πώς τέτοια πρόσβαση ελέγχεται.
(8)Παραβιάσεις που εκθέτουν την πολιτική ασφαλείας σε κινδύνους. (π.χ., μυστικότητα και ασφάλεια, εσωτερικούς και εξωτερικούς)
(9)Πληροφορίες που παρέχουν στους χρήστες, το προσωπικό, και τη διαχείριση, στοιχεία για κάθε τύπο πολιτικής παραβίασης, οδηγίες για το πώς να χειριστούν ένα γεγονός ασφάλειας, ή πληροφορίες που μπορούν να θεωρηθούν εμπιστευτικές ή ιδιόκτητες. Επίσης παρέχουν παραπομπές στις διαδικασίες ασφάλειας και τις σχετικές πληροφορίες, όπως οι πολιτικές επιχείρησης και οι κυβερνητικοί νόμοι και κανονισμοί.
Μπορεί να υπάρξουν ρυθμιστικές απαιτήσεις που έχουν επιπτώσεις σε μερικές πτυχές της πολιτικής ασφάλειάς (π.χ., έλεγχος γραμμής). Τουλάχιστον, η πολιτική πρέπει να αναθεωρηθεί από το νομικό συμβούλιο.
Μόλις καθιερωθεί η πολιτική ασφάλειάς πρέπει να κοινοποιηθεί με σαφή τρόπο στους χρήστες, το προσωπικό, και τη διαχείριση. Η υπογραφή μια δήλωσης που δείχνει ότι έχουν διαβάσει, κατανοήσει, και συμφωνήσει να τηρηθεί η πολιτική είναι ένα σημαντικό μέρος της διαδικασίας.
Τέλος, η πολιτική πρέπει να αναθεωρείτε ανά τακτά χρονικά διαστήματα για να παρατηρείται εάν υποστηρίζει επιτυχώς τις τρέχουσες ανάγκες ασφάλειας.

2.3 Κρατώντας «εύκαμπτη» την πολιτική

Για να είναι μια πολιτική ασφάλειας βιώσιμη για μακροπρόθεσμο διάστημα, απαιτείτε ευελιξία η οποία βασίζεται στην αρχιτεκτονική μιας πολιτικής ασφάλειας.
Μια πολιτική ασφάλειας πρέπει να είναι (κατά ένα μεγάλο μέρος) ανεξάρτητη από τις συγκεκριμένες καταστάσεις υλικού και λογισμικού

(δεδομένου ότι συγκεκριμένα συστήματα μπορεί να είναι σε φάση αντικατάστασης).
Οι μηχανισμοί για την αναθεώρηση της πολιτικής πρέπει να είναι ξεκάθαροι. Αυτό περιλαμβάνει τη διαδικασία, στην οποία αναμειγνύονται και τα σχετικά με την πολιτική ασφάλειας άτομα καθώς και τα άτομα που πρέπει να εγκρίνουν τις αλλαγές.
Είναι επίσης σημαντικό να αναγνωριστεί ότι υπάρχουν εξαιρέσεις σε κάθε κανόνα. Όποτε είναι δυνατόν, η πολιτική πρέπει να εξηγεί ποιες εξαιρέσεις υπάρχουν στην γενική πολιτική.
Παραδείγματος χάριν, ένας διαχειριστής ρυθμίζει σε ποια αρχεία επιτρέπεται να έχει πρόσβαση ένας χρήστης. Επίσης, μπορούν να υπάρξουν μερικές περιπτώσεις όπου πολλαπλοί χρήστες θα έχουν πρόσβαση στην ίδια ταυτότητα χρήστη.

Παραδείγματος χάριν, στα συστήματα με έναν χρήστη "root", οι πολλαπλοί διαχειριστές συστημάτων μπορούν να ξέρουν τον κωδικό πρόσβασης και να χρησιμοποιήσουν τον λογαριασμό του root.
Μια άλλη περίπτωση είναι το "Garbage Truck Syndrome." Αναφέρεται σε αυτό που θα συνέβαινε σε έναν οργανισμό εάν ένα βασικό πρόσωπο ήταν ξαφνικά μη διαθέσιμο για τη λειτουργία της εργασίας του (π.χ., ήταν ξαφνικά άρρωστος ή άφησε την επιχείρηση απροσδόκητα). Ενώ η μέγιστη ασφάλεια έγκειται στην ελάχιστη διάδοση των πληροφοριών, ο κίνδυνος απώλειας κρίσιμων πληροφοριών αυξάνεται όταν δεν μοιράζονται εκείνες οι πληροφορίες. Είναι σημαντικό να καθοριστεί πια είναι η κατάλληλη ισορροπία για έναν οργανισμό.

Κεφάλαιο 3. Αρχιτεκτονική

3.1 Στόχοι

3.1.1 Καθορισμένα σχέδια ασφάλειας

Όλοι οι οργανισμοί πρέπει να έχουν ένα περιεκτικό σχέδιο ασφάλειας. Αυτό το σχέδιο πρέπει να είναι σε πιο υψηλό επίπεδο από τις συγκεκριμένες πολιτικές που συζητήθηκαν στο κεφάλαιο 2, και πρέπει να κατασκευαστεί ως ένα σύνολο ευρειών οδηγιών στις οποίες οι συγκεκριμένες πολιτικές θα ταιριάξουν.
Είναι σημαντικό να υπάρχει αυτό το πλαίσιο σε ισχύ έτσι ώστε οι μεμονωμένες πολιτικές να μπορούν να είναι σύμφωνες με τη γενική αρχιτεκτονική ασφάλειας των οργανισμών.
Παραδείγματος χάριν, η κατοχή μιας ισχυρής πολιτικής όσον αφορά την πρόσβαση Διαδικτύου και η ύπαρξη μικρών περιορισμών στη χρήση modem είναι ασυμβίβαστες με μια γενική φιλοσοφία ισχυρών περιορισμών ασφάλειας στην εξωτερική πρόσβαση.
Ένα σχέδιο ασφάλειας πρέπει να καθορίζει: τον κατάλογο υπηρεσιών δικτύων που θα παρασχεθεί, ποιοι τομείς της οργάνωσης θα παράσχουν τις υπηρεσίες, ποιος θα έχει πρόσβαση σε εκείνες τις υπηρεσίες, πώς η πρόσβαση θα παρασχεθεί, ποιος θα διαχειριστεί εκείνες τις υπηρεσίες κ.λπ....
Το σχέδιο πρέπει επίσης να εξετάσει πώς θα αντιμετωπιστεί το γεγονός. Το κεφάλαιο 5 παρέχει μια σε βάθος ανάλυση του πώς πρέπει να χειριστούμε ένα γεγονός ασφάλειας, αλλά είναι σημαντικό για κάθε οργανισμό να καθοριστούν οι κατηγορίες γεγονότων και οι αντίστοιχες απαντήσεις.
Παραδείγματος χάριν, οι οργανισμοί που διαθέτουν firewall πρέπει να θέσουν ένα κατώτατο όριο στον αριθμό προσπαθειών που γίνονται εναντίον του οργανισμού πριν προκληθεί μια αντίδραση. Τα επίπεδα διαβάθμισης πρέπει να καθοριστούν και για τις επιθέσεις και για τις απαντήσεις.
Οι οργανισμοί χωρίς firewall θα πρέπει να καθορίσουν εάν μια ενιαία προσπάθεια για να συνδεθούν με έναν host(ξενιστή) αποτελεί ένα γεγονός.
Για τους οργανισμούς που συνδέονται με το Διαδίκτυο, η συνεχής ενίσχυση με μέσα σχετικά με την ασφάλεια του Διαδίκτυου μπορεί να επισκιάσει ένα (ενδεχομένως) σοβαρότερο εσωτερικό πρόβλημα ασφάλειας.
Επιπλέον, οι επιχειρήσεις που δεν έχουν συνδεθεί ποτέ με το Διαδίκτυο μπορούν να έχουν ισχυρές, καλά καθορισμένες, εσωτερικές πολιτικές αλλά αποτυγχάνουν να διαμορφώσουν επαρκώς μια εξωτερική πολιτική σύνδεσης.

3.1.2 Χωρισμός των υπηρεσιών

Υπάρχουν πολλές υπηρεσίες που ένας οργανισμός μπορεί να επιθυμεί να παρέχει στους χρήστες του, μερικές από τις οποίες μπορεί να είναι εξωτερικές. Υπάρχουν ποικίλοι λόγοι ασφάλειας για την προσπάθεια απομόνωσης των υπηρεσιών στους αφιερωμένους host (ξενιστής) υπολογιστές. Υπάρχουν επίσης λόγοι απόδοσης στις περισσότερες περιπτώσεις.
Οι υπηρεσίες που μπορεί να παρέχει ένας οργανισμός, στις περισσότερες περιπτώσεις, θα έχουν διαφορετικά επίπεδα αναγκών πρόσβασης και πρότυπα εμπιστοσύνης.
Οι υπηρεσίες που είναι ουσιαστικές για την ασφάλεια ή την ομαλή λειτουργία ενός οργανισμού θα ήταν καλύτερα αν τοποθετούνταν σε μια αφιερωμένη μηχανή με πολύ περιορισμένη πρόσβαση, παρά σε μια μηχανή που παρέχει μια υπηρεσία (ή τις υπηρεσίες)

που είναι παραδοσιακά λιγότερο ασφαλής. Είναι επίσης σημαντικό να υπάρχει διαχωρισμός μεταξύ των host (ξενιστών) που λειτουργούν μέσα σε διαφορετικά πρότυπα εμπιστοσύνης.
Είναι σημαντικό να αναφερθεί ότι η ασφάλεια είναι τόσο ισχυρή όσο ο πιο αδύνατος κρίκος στην αλυσίδα της πολιτικής ασφάλειας. Αρκετές από τις πιο γνωστές παραβιάσεις τα τελευταία χρόνια έγιναν μέσω της εκμετάλλευσης των αδυναμιών στα συστήματα ηλεκτρονικού ταχυδρομείου. Οι εισβολείς δεν προσπάθησαν να κλέψουν το ηλεκτρονικό ταχυδρομείο, αλλά χρησιμοποίησαν την αδυναμία σε εκείνη την υπηρεσία για να αποκτήσουν πρόσβαση σε άλλα συστήματα.
Εάν είναι δυνατόν, κάθε υπηρεσία πρέπει να τρέχει σε μια διαφορετική μηχανή της οποίας το μόνο καθήκον είναι να παρέχει μια συγκεκριμένη υπηρεσία. Αυτό βοηθά στην απομόνωση των εισβολέων και στον περιορισμό πιθανής ζημιάς.

3.1.3 Deny all - Allow all

Υπάρχουν δύο διαμετρικά αντίθετες φιλοσοφίες που μπορούν να υιοθετηθούν κατά το καθορισμό ενός σχεδίου ασφάλειας. Και οι δύο εναλλακτικές λύσεις είναι ομότιμες και η μεταξύ τους επιλογή θα εξαρτηθεί από τον οργανισμό και τις ανάγκες του για ασφάλεια.
Η πρώτη επιλογή είναι να κληθούν όλες οι υπηρεσίες και έπειτα επιλεκτικά να επιτραπούν οι υπηρεσίες όταν απαιτείται. Αυτό μπορεί να γίνει σε επίπεδο host (ξενιστή) ή δικτύων ανάλογα με την περίπτωση.
Αυτό το πρότυπο, το οποίο εδώ αναφέρεται ως "deny all" πρότυπο, είναι γενικά ασφαλέστερο από το πρότυπο που περιγράφεται στην επόμενη παράγραφο.
Περισσότερη προσπάθεια απαιτείται για να εφαρμοστεί επιτυχώς η "deny all" διαμόρφωση καθώς επίσης και μια καλύτερη κατανόηση των υπηρεσιών της.
Η άδεια μόνο των γνωστών υπηρεσιών επιτρέπει μια καλύτερη ανάλυση ενός ιδιαίτερου service/protocol και του σχεδίου ενός μηχανισμού ασφάλειας που ταιριάζει στο επίπεδο ασφάλειας του οργανισμού.
Το άλλο πρότυπο, το οποίο εδώ αναφέρεται ως "allow all" πρότυπο, είναι πολύ ευκολότερο να εφαρμοστεί, αλλά είναι γενικά λιγότερο ασφαλές από το "deny all".
Απλά ανοίγουμε όλες τις υπηρεσίες, συνήθως την προεπιλογή στο επίπεδο host (ξενιστή), και επιτρέπουμε σε όλα τα πρωτόκολλα να τρέχουν στα όρια δικτύων. Συνήθως η προεπιλογή γίνεται σε επίπεδο δρομολογητών.
Κάθε ένα από αυτά τα πρότυπα μπορεί να εφαρμοστεί σε διάφορα μέρη του οργανισμού, ανάλογα με τις απαιτήσεις λειτουργίας, το διοικητικό έλεγχο, την πολιτική περιοχών, κ.λπ....
Παραδείγματος χάριν, η πολιτική μπορεί να χρησιμοποιεί το "deny all" πρότυπο κατά το στήσιμο των τερματικών σταθμών για γενική χρήση, αλλά να υιοθετεί το "denny all" πρότυπο κατά το στήσιμο των κεντρικών υπολογιστών πληροφοριών, όπως ένα hub ηλεκτρονικού ταχυδρομείου. Επιπλέον, η "allow all" πολιτική μπορεί να υιοθετηθεί για κυκλοφορία μεταξύ των τοπικών LAN τα οποία είναι εσωτερικά στον οργανισμό, αλλά μια "deny all" πολιτική μπορεί να υιοθετηθεί μεταξύ του οργανισμού και του Διαδικτύου.
Πρέπει να υπάρχει προσοχή κατά την ανάμειξη φιλοσοφιών όπως αναφέρεται στα παραπάνω παραδείγματα. Πολλοί οργανισμοί είναι πρόθυμοι να πληρώσουν το κόστος της ασφάλειας για την εξωτερική πρόσβασή τους και να απαιτήσουν ισχυρά μέτρα ασφάλειας, αλλά είναι απρόθυμοι ή ανίκανοι να παρέχουν μια παρόμοια προστασία εσωτερικά.

Αυτό λειτουργεί εφ' όσον οι εξωτερικές άμυνες δεν παραβιάζονται ποτέ και οι εσωτερικοί χρήστες είναι έμπιστοι . Μόλις παραβιαστεί το εξωτερικό κέλυφος (firewall), η υπονόμευση του εσωτερικού δικτύου είναι σίγουρη.

3.1.4 Προσδιορισμός των πραγματικών αναγκών για τις υπηρεσίες

Υπάρχει μια μεγάλη ποικιλία υπηρεσιών που μπορεί να παρασχεθεί, και εσωτερικά και στο διαδίκτυο. Η διαχείριση της ασφάλειας είναι, από πολλές απόψεις, διαχείριση της πρόσβασης στις υπηρεσίες εσωτερικά στον οργανισμό και διαχείριση του πώς οι εσωτερικοί χρήστες έχουν πρόσβαση στις πληροφορίες απομακρυσμένων περιοχών .
Με την πάροδο των ετών πολλοί οργανισμοί έχουν καθιερώσει τους ανώνυμους κεντρικούς υπολογιστές FTP, τους κεντρικούς υπολογιστές gopher, τους κεντρικούς υπολογιστές wais, WWW κεντρικούς υπολογιστές, κ.λπ.. Η χρήση τους δεν είναι ιδιαίτερα ωφέλιμη σε όλους τους οργανισμούς.
Λαμβάνεται υπόψη ότι η πολυπλοκότητα ασφάλειας μπορεί να αυξηθεί εκθετικά με τον παρεχόμενο αριθμό υπηρεσιών . Οι δρομολογητές φιλτραρίσματος πρέπει να τροποποιηθούν για να υποστηρίξουν τα νέα πρωτόκολλα.
Μερικά πρωτόκολλα είναι δύσκολο στο να φιλτραριστούν ασφαλώς (π.χ., υπηρεσίες RPC και UDP), δημιουργώντας κατά συνέπεια περισσότερα κενά στο εσωτερικό δίκτυο. Οι υπηρεσίες που παρέχονται στην ίδια μηχανή μπορούν να αλληλεπιδράσουν με καταστροφικούς τρόπους.
Παραδείγματος χάριν, η ύπαρξη του ανώνυμου FTP στην ίδια μηχανή με ένα κεντρικό υπολογιστή WWW μπορεί να επιτρέψει σε έναν εισβολέα να τοποθετήσει ένα αρχείο στον ανώνυμο οργανισμό FTP και να αναγκάσει τον κεντρικό υπολογιστή HTTP να το εκτελέσει.

3.2 Διαμόρφωση δικτύων και υπηρεσιών

3.2.1 Προστασία της υποδομής

Πολλοί διαχειριστές δικτύων προβαίνουν σε ιδιαίτερα μέτρα για να προστατεύσουν τους host (ξενιστές) των δικτύων τους. Λίγοι διαχειριστές καταβάλλουν οποιαδήποτε προσπάθεια να προστατεύσουν τα ίδια τα δίκτυα . Υπάρχει κάποια λογική σε αυτό.
Παραδείγματος χάριν, είναι πολύ ευκολότερο να προστατευθεί ένας host (ξενιστής) παρά ένα δίκτυο. Επίσης, οι εισβολείς είναι πιθανό να επιζητούν δεδομένα που αφορούν τους host (ξενιστές), και η καταστροφή του δικτύου δεν θα εξυπηρετούσε τους σκοπούς τους. Υπάρχουν όμως ακόμα λόγοι για να προστατευθούν τα δίκτυα. Παραδείγματος χάριν, ένας εισβολέας μπορεί να εκτρέψει την κυκλοφορία του δικτύου μέσω ενός εξωτερικού host (ξενιστή) προκειμένου να δει τα δεδομένα (δηλ., αναζήτηση κωδικών πρόσβασης).
Επίσης, η υποδομή περιλαμβάνει περισσότερα πράγματα από τα δίκτυα και τους δρομολογητές που τους συνδέουν. Η υποδομή περιλαμβάνει επίσης τη διαχείριση δικτύων (π.χ., SNMP), τις υπηρεσίες (π.χ., DNS, NFS, NTP, WWW),και την ασφάλεια (δηλ., επικύρωση χρηστών και περιορισμοί πρόσβασης).
Η υποδομή χρειάζεται επίσης προστασία ενάντια στο ανθρώπινο λάθος. Όταν ένας διαχειριστής παραμετροποιήσει λάθος ένα host (ξενιστή), ο host (ξενιστής) μπορεί να προσφέρει υποβαθμισμένη υπηρεσία.

Αυτό έχει επιπτώσεις μόνο στους χρήστες που θέλουν πρόσβαση σε εκείνο το host (ξενιστή), εκτός αν εκείνος ο host (ξενιστής) είναι ένας αρχικός κεντρικός υπολογιστής, επομένως ο αριθμός των επηρεαζόμενων χρηστών θα περιοριστεί. Εντούτοις, εάν ένας δρομολογητής είναι κακώς παραμετροποιημένος, όλοι οι χρήστες του δικτύου θα επηρεαστούν.
Προφανώς, αυτός είναι ένας πολύ μεγαλύτερος αριθμός χρηστών από αυτούς που εξαρτώνται από οποιοδήποτε άλλο host (ξενιστή).

3.2.2 Προστασία του δικτύου

Υπάρχουν διάφορα προβλήματα στα οποία τα δίκτυα είναι τρωτά. Το κλασικό πρόβλημα είναι μια επίθεση "denial of service". Σε αυτήν την περίπτωση, το δίκτυο έρχεται σε μια κατάσταση στην οποία δεν μπορεί πλέον να ανακτήσει τα στοιχεία των νόμιμων χρηστών.
Υπάρχουν δύο κοινοί τρόποι με τους οποίους αυτό μπορεί να γίνει: με μια επίθεση στους δρομολογητές και με ένα «flood» του δικτύου με ξένη κυκλοφορία. Πρέπει να σημειωθεί ότι ο όρος "δρομολογητής" σε αυτό το τμήμα χρησιμοποιείται ως παράδειγμα μιας μεγαλύτερης κατηγορίας ενεργών τμημάτων διασύνδεσης δικτύων που περιλαμβάνει επίσης συστατικά όπως firewalls, proxy- servers, κτλ.
Μια επίθεση στο δρομολογητή έχει ως σκοπό να τον αναγκάσει να σταματήσει να διαβιβάζει τα πακέτα, ή να τα διαβιβάσει εσφαλμένα.
Η προηγούμενη περίπτωση μπορεί να οφείλεται σε μια κακή παραμετροποίηση, την έγχυση μιας πλαστής δρομολόγησης, ή μια "flood" επίθεση (δηλ., ο δρομολογητής βομβαρδίζεται με αδρομολόγητα πακέτα, οδηγώντας σε μείωση της απόδοσής του). Μια επίθεση flood σε ένα δίκτυο είναι παρόμοια με μια επίθεση flood σε έναν δρομολογητή, εκτός από το ότι τα πακέτα flood είναι συνήθως πακέτα μετάδοσης.
Μια ιδανική επίθεση flood θα ήταν η έγχυση ενός ενιαίου πακέτου που εκμεταλλεύεται κάποια γνωστό κενό στους κόμβους δικτύων και τους αναγκάζει να αναμεταδόσουν το πακέτο, ή να παράγουν πακέτα λάθους, κάθε ένα από τα οποία παίρνονται και επαναλαμβάνονται από έναν άλλο host (ξενιστή).
Ένα άλλο κλασικό πρόβλημα είναι το "spoofing." Σε αυτήν την περίπτωση, οι πλαστές δρομολογήσεις στέλνονται σε έναν ή περισσότερους δρομολογητές αναγκάζοντας τους να δρομολογήσουν άστοχα τα πακέτα.
Αυτό διαφέρει από μια επίθεση άρνησης υπηρεσιών. Στην περίπτωση άρνησης της υπηρεσίας, το αποτέλεσμα είναι να καταστεθεί ο δρομολογητής ακατάλληλος προς χρήση, κατάσταση που θα ανιχνευθεί γρήγορα από τους χρήστες. Στο spoofing, η πλαστή διαδρομή θα αναγκάσει τα πακέτα να καθοδηγηθούν σε έναν host (ξενιστή) από τον οποίο ένας εισβολέας μπορεί να ελέγξει τα στοιχεία των πακέτων.
Αυτά τα πακέτα επανακαθοδηγούνται έπειτα στους σωστούς προορισμούς τους. Εντούτοις, ο εισβολέας μπορεί να έχει αλλάξει το περιεχόμενο των πακέτων.
Η λύση στα περισσότερα από αυτά τα προβλήματα είναι να προστατευθούν τα πακέτα αναπροσαρμογών δρομολόγησης τα οποία στέλνονται από τα πρωτόκολλα δρομολόγησης που βρίσκονται σε χρήση (π.χ., RIP-2, OSPF).
Υπάρχουν τρία επίπεδα προστασίας: clear-text κωδικός πρόσβασης, κρυπτογραφικό checksum, και κρυπτογράφηση. Οι κωδικοί πρόσβασης προσφέρουν μόνο την ελάχιστη προστασία ενάντια στους εισβολείς που δεν έχουν άμεση πρόσβαση στα φυσικά δίκτυα.
Οι κωδικοί πρόσβασης προσφέρουν επίσης κάποια προστασία ενάντια στους κακώς παραμετροποιημένους δρομολογητές. Το πλεονέκτημα των κωδικών πρόσβασης είναι ότι

έχουν πολύ χαμηλό κόστος, τόσο σε εύρος ζώνης όσο και σε κατανάλωση CPU. Τα Checksums προστατεύουν από την έγχυση πλαστών πακέτων, ακόμα κι αν ο εισβολέας έχει άμεση πρόσβαση στο φυσικό δίκτυο. Συνδυασμένο με έναν αριθμό ακολουθίας, ή άλλο μοναδικό προσδιοριστικό, το checksum μπορεί επίσης να προστατεύσει από επαναλαμβανόμενες επιθέσεις, όπου μια παλαιά διαμόρφωση δρομολόγησης αναμεταδίδεται είτε από έναν εισβολέα είτε από έναν δρομολογητή με απρεπή συμπεριφορά.

Περισσότερη ασφάλεια παρέχεται από μια πλήρως αναθεωρημένη, κρυπτογραφημένη δρομολόγηση.

Αυτό αποτρέπει έναν εισβολέα από το να καθορίσει την τοπολογία του δικτύου. Το μειονέκτημα στην κρυπτογράφηση είναι το κόστος αναβαθμίσεων. Τα RIP-2, OSPF και οι δύο clear-text κωδικοί πρόσβασης διαμορφώνουν από την αρχή τις προδιαγραφές τους. Επιπλέον, υπάρχουν επεκτάσεις σε κάθε πρωτόκολλο που υποστηρίζουν την κρυπτογράφηση MD5.

Δυστυχώς, δεν υπάρχει καμία επαρκής προστασία ενάντια σε μια επίθεση flooding, ή ένα host (ξενιστή) που δεν λειτουργεί σωστά ή ένα δρομολογητή που «πλημμυρίζει» το δίκτυο. Ευτυχώς, αυτός ο τύπος επίθεσης γίνεται γρήγορα αντιληπτός και μπορεί συνήθως να αντιμετωπιστεί σχετικά εύκολα.

3.2.3 Προστασία των υπηρεσιών

Υπάρχουν πολλοί τύποι υπηρεσιών και κάθε ένας έχει τις απαιτήσεις ασφάλειάς του. Αυτές οι απαιτήσεις ποικίλουν ανάλογα με την προοριζόμενη χρήση της υπηρεσίας. Παραδείγματος χάριν, μια υπηρεσία που πρέπει μόνο να χρησιμοποιείται εσωτερικά (π.χ., NFS) μπορεί να απαιτήσει διαφορετικούς μηχανισμούς προστασίας από μια υπηρεσία που παρέχεται για εξωτερική χρήση.

Μπορεί να είναι ικανοποιητικό να προστατευθεί ο εσωτερικός κεντρικός υπολογιστής από την εξωτερική πρόσβαση, εντούτοις, ένας κεντρικός υπολογιστής WWW, που παρέχει μια αρχική σελίδα προοριζόμενη για πρόσβαση από τους χρήστες οπουδήποτε στο διαδίκτυο, απαιτεί ενσωματωμένη προστασία.

Δηλαδή το service/protocol/server πρέπει να παρέχει οποιαδήποτε ασφάλεια μπορεί να απαιτηθεί για να αποτρέψει την αναρμόδια πρόσβαση και την τροποποίηση της βάσης δεδομένων.

Οι εσωτερικές υπηρεσίες (δηλ., υπηρεσίες που χρησιμοποιούνται μόνο από χρήστες εντός του οργανισμού) και οι εξωτερικές υπηρεσίες (δηλ., υπηρεσίες που τίθενται σκόπιμα στην διάθεση των χρηστών έξω από έναν οργανισμό), γενικά, θα έχουν απαιτήσεις προστασίας που διαφέρουν.

Είναι επομένως σοφό να απομονωθούν οι εσωτερικές υπηρεσίες σε ένα σύνολο κεντρικών host (ξενιστών) υπολογιστών και οι εξωτερικές υπηρεσίες σε ένα άλλο σύνολο κεντρικών host (ξενιστών) υπολογιστών.

Δηλαδή οι εσωτερικοί και εξωτερικοί κεντρικοί υπολογιστές δεν πρέπει να συνδυαστούν στον ίδιο host (ξενιστή) υπολογιστή. Στην πραγματικότητα, πολλοί οργανισμοί εφαρμόζουν αυτή την τακτική όσον αφορά στην ύπαρξη ενός συνόλου υποδικτύων (ή ακόμα και διαφορετικών δικτύων) που να είναι προσιτά από τον εξωτερικό κεντρικό υπολογιστή και ένα άλλο σύνολο που μπορούν να προσεγγιστούν μόνο μέσα από τον οργανισμό .

Φυσικά, υπάρχει συνήθως ένα firewall που συνδέει αυτά τα χωρίσματα. Μεγάλη προσοχή πρέπει να ληφθεί για να εξασφαλιστεί ότι ένα τέτοιο firewall λειτουργεί κατάλληλα.

Υπάρχει αυξανόμενο ενδιαφέρον για χρησιμοποίηση intranets που θα συνδέουν τα διαφορετικά μέρη μιας οργάνωσης (π.χ., τμήματα μιας επιχείρησης).
Ενώ η παρούσα εργασία διαφοροποιείται γενικά μεταξύ εξωτερικού και εσωτερικού δικτύου (δημόσιου και ιδιωτικού), οι οργανισμοί που χρησιμοποιούν intranets πρέπει να γνωρίζουν ότι θα πρέπει να εξετάζουν τρεις διαχωρισμούς και να λάβουν κατάλληλα μέτρα κατά το σχεδιασμό και την προσφορά των υπηρεσιών. Οι υπηρεσίες που προσφέρονται σε ένα intranet δεν θα είναι δημόσιες, ούτε τόσο απόλυτα ιδιωτικές όσο μια υπηρεσία σε μια ενιαία οργανωτική υπό-μονάδα.
Μια μορφή εξωτερικής υπηρεσίας η οποία αξίζει κάποια ιδιαίτερη προσοχή, είναι η ανώνυμη, ή φιλοξενούμενη, πρόσβαση. Αυτό μπορεί να είναι είτε ανώνυμο FTP είτε πλαστή σύνδεση .
Είναι εξαιρετικά σημαντικό να εξασφαλιστεί ότι η ανώνυμη σύνδεση κεντρικών υπολογιστών και φιλοξενουμένων FTP userids είναι προσεκτικά απομονωμένη από οποιουσδήποτε host (ξενιστές) και συστήματα αρχείων από τους οποίους πρέπει να κρατούνται οι εξωτερικοί χρήστες.
Μια περίπτωση οργανισμού στην οποία πρέπει να δοθεί ιδιαίτερη προσοχή όσο αφορά την ανώνυμη πρόσβαση αναφέρεται παρακάτω.
Ένας οργανισμός μπορεί να είναι νόμιμα αρμόδιος για το περιεχόμενο των δημόσια διαθέσιμων πληροφοριών, τόσο που να ενθαρρύνεται ένας προσεκτικός έλεγχος των πληροφοριών που κατατίθενται από τους ανώνυμους χρήστες.
Τώρα θα εξεταστούν μερικές από τις δημοφιλέστερες υπηρεσίες:name service, password/key service, authentication/proxy service, electronic mail, WWW, file transfer και NFS.
Δεδομένου ότι αυτές είναι οι πιο συχνά χρησιμοποιημένες υπηρεσίες, είναι και τα προφανέστερα σημεία επίθεσης.

3.2.3.1 Name Servers (DNS και NIS(+))

Το Διαδίκτυο χρησιμοποιεί το σύστημα ονόματος περιοχών (DNS) για να εκτελέσει το polling διευθύνσεων για τα ονόματα των host (ξενιστών) και των δικτύων. Οι υπηρεσίες πληροφοριών δικτύων (NAK) και NIS + δεν χρησιμοποιούνται στο Διαδίκτυο, αλλά υπόκεινται στους ίδιους κινδύνους με έναν DNS κεντρικό υπολογιστή. Το polling Name-to-address είναι κρίσιμο για την ασφαλή λειτουργία οποιουδήποτε δικτύου.
Ένας επιτιθέμενος μπορεί επιτυχώς να ελέγξει ή να προσποιηθεί ένα DNS κεντρικό υπολογιστή και μπορεί να επαναδρομολογήσει την κίνηση για να υπονομεύσει την ασφάλεια.
Παραδείγματος χάριν, η κυκλοφορία ρουτίνας μπορεί να εκτραπεί σε ένα παραβιασμένο σύστημα που ελέγχεται ή οι χρήστες μπορούν να εξαπατηθούν στην παροχή των μυστικών επικύρωσης.
Παραδοσιακά, το DNS δεν είχε καμία δυνατότητα ασφάλειας. Ειδικότερα, οι πληροφορίες που επιστρέφονται από μια ερώτηση δεν μπορούν να ελεγχθούν για τροποποίηση ή να ελέγξουν ότι είχε προέλθει από τον κεντρικό υπολογιστή .

3.2.3.2 Password/Key Servers (NIS(+) και KDC)

Οι Password και key κεντρικοί υπολογιστές προστατεύουν γενικά τις ζωτικής σημασίας πληροφορίες τους (δηλ., τους κωδικούς πρόσβασης και τα κλειδιά) με αλγορίθμους κρυπτογράφησης.
Εντούτοις, ακόμη και ένας μονόδρομα (one-way) κρυπτογραφημένος κωδικός πρόσβασης μπορεί να παραβιασθεί από μια επίθεση λεξικών (όπου οι κοινές λέξεις κρυπτογραφούνται για να δουν εάν ταιριάζουν με την αποθηκευμένη κρυπτογράφηση).
Είναι επομένως απαραίτητο να εξασφαλιστεί ότι αυτοί οι κεντρικοί υπολογιστές δεν είναι προσβάσιμοι από τους host (ξενιστές) και δεν τους χρησιμοποιούν για την υπηρεσία. Ακόμη οι host (ξενιστές) πρέπει να είναι σε θέση να έχουν πρόσβαση στην υπηρεσία (δηλ., γενικές υπηρεσίες, όπως Telnet και FTP δεν πρέπει να έχουν άδεια από κανένα άλλο εκτός από τους διαχειριστές).

3.2.3.3 Authentication/Proxy Servers (SOCKS, FWTK)

Ένας proxy server ισχυροποιεί την ασφάλεια. Επιτρέπει στους οργανισμούς να συγκεντρώνουν υπηρεσίες μέσω ενός συγκεκριμένου host (ξενιστή) για να επιτρέπετε η παρακολούθηση της εσωτερικής δομής, κ.λπ....
Αυτό το σύνολο υπηρεσιών αποτελεί έναν ελκυστικό στόχο για έναν πιθανό εισβολέα. Ο τύπος προστασίας που απαιτείται για έναν proxy server εξαρτάται πολύ από το πρωτόκολλο που χρησιμοποιείται. Ο γενικός κανόνας περιορισμού της πρόσβασης μόνο σε εκείνους τους host (ξενιστές) που χρειάζονται τις υπηρεσίες είναι μια καλή αρχή.

3.2.3.4 Ηλεκτρονικό ταχυδρομείο

Τα συστήματα ηλεκτρονικού ταχυδρομείου (ηλεκτρονικό ταχυδρομείο) είναι από καιρό μια πηγή για διαρρήξεις επειδή τα πρωτόκολλα ηλεκτρονικού ταχυδρομείου είναι σχετικά παλιά.
Επίσης, ένας κεντρικός υπολογιστής ηλεκτρονικού ταχυδρομείου απαιτεί πρόσβαση στον εξωτερικό κόσμο. Οι περισσότεροι κεντρικοί υπολογιστές ηλεκτρονικού ταχυδρομείου δέχονται εισαγωγές από οποιαδήποτε πηγή.
Ένας κεντρικός υπολογιστής ηλεκτρονικού ταχυδρομείου αποτελείται γενικά από δύο μέρη: ένα πράκτορα λήψης-αποστολής και ένα πράκτορα επεξεργασίας.
Δεδομένου ότι το ηλεκτρονικό ταχυδρομείο παραδίδεται σε όλους τους χρήστες, και είναι συνήθως ιδιωτικό, ο πράκτορα επεξεργασίας απαιτεί τα προνόμια συστημάτων (root) για να παραδώσει το ταχυδρομείο.
Οι περισσότερες εφαρμογές ηλεκτρονικού ταχυδρομείου εκτελούν και τα δυο μέρη της υπηρεσίας, το οποίο σημαίνει ότι ο λαμβάνων πράκτορας έχει επίσης τα προνόμια συστημάτων.
Υπάρχουν μερικές διαθέσιμες εφαρμογές που διαχωρίζουν τους δύο πράκτορες.
Τέτοιες εφαρμογές θεωρούνται γενικά ασφαλέστερες, αλλά απαιτούν προσεκτική εγκατάσταση έτσι ώστε να αποφευχθεί ένα πρόβλημα ασφάλειας.

3.2.3.5 World Wide Web (WWW)

Η δημοτικότητα του WWW αυξάνεται λόγω της ευκολίας χρήσης και της δυνατότητας συγκέντρωσης πολλών πληροφοριών.
Οι περισσότεροι κεντρικοί υπολογιστές WWW δέχονται κατευθύνσεις και ενέργειες από τα πρόσωπα που έχουν πρόσβαση στις υπηρεσίες τους.
Το πιο κοινό παράδειγμα είναι ένα αίτημα από έναν μακρινό χρήστη που εισάγει πληροφορίες σε ένα πρόγραμμα που τρέχει στον κεντρικό υπολογιστή για να επεξεργαστεί το αίτημα.
Μερικά από αυτά τα προγράμματα δεν γράφονται με την ασφάλεια κατά νου και μπορούν να δημιουργήσουν κενά ασφάλειας. Εάν ένας κεντρικός υπολογιστής δικτύου είναι διαθέσιμος στην κοινότητα του Διαδικτύου, είναι ιδιαίτερα σημαντικό ότι οι εμπιστευτικές πληροφορίες δεν πρέπει να συνδυαστούν στον ίδιο host (ξενιστή) με εκείνο του κεντρικού υπολογιστή.
Συνιστάται ο κεντρικός υπολογιστής να έχει έναν αφιερωμένο host (ξενιστή) που "δεν εμπιστεύεται" άλλους εσωτερικούς host (ξενιστές).
Πολλοί οργανισμοί μπορεί να θέλουν να συνδυάσουν την υπηρεσία FTP με την υπηρεσία WWW αλλά αυτό πρέπει μόνο να εμφανιστεί για τους ανώνυμους κεντρικούς υπολογιστές FTP που παρέχουν μόνο τις πληροφορίες (FTP-get).
Το ανώνυμο FTP, σε συνδυασμό με το WWW, μπορεί να είναι και καθιστά τις ανάγκες ασφάλειας διαφορετικές για κάθε υπηρεσία.

3.2.3.6 Μεταφορά αρχείων (FTP, TFTP)

Το FTP και TFTP επιτρέπουν στους χρήστες να λάβουν και να στείλουν ηλεκτρονικά αρχεία από σημείο σε σημείο. Εντούτοις, το FTP απαιτεί επικύρωση ενώ TFTP δεν απαιτεί τίποτα. Για αυτόν τον λόγο, το TFTP πρέπει να αποφευχθεί όσο το δυνατόν περισσότερο.
Οι εσφαλμένα διαμορφωμένοι κεντρικοί υπολογιστές FTP μπορούν να επιτρέψουν στους εισβολείς να αντιγράψουν, να αντικαταστήσουν και να διαγράψουν τα αρχεία, οπουδήποτε σε έναν host (ξενιστή), έτσι είναι πολύ σημαντικό να διαμορφωθεί αυτή η υπηρεσία σωστά. Η πρόσβαση στους κρυπτογραφημένους κωδικούς πρόσβασης και τα ιδιόκτητα στοιχεία, και η εισαγωγή Trojan horses είναι ακριβώς μερικά από τα πιθανά κενά ασφάλειας που μπορούν να εμφανιστούν όταν διαμορφώνεται ανακριβώς η υπηρεσία. Οι κεντρικοί υπολογιστές FTP πρέπει να είναι εγκατεστημένοι στον host (ξενιστή) τους.
Μερικοί οργανισμοί επιλέγουν να συνδυάσουν το FTP με έναν κεντρικό υπολογιστή δικτύου, δεδομένου ότι τα δύο πρωτόκολλα μοιράζονται κοινές ανάγκες ασφάλειας εντούτοις, η πρακτική αυτή δεν συστήνεται, ειδικά όταν η υπηρεσία FTP επιτρέπει την κατάθεση των αρχείων. Όπως αναφέρεται στην παράγραφο 3.2.3 οι υπηρεσίες που προσφέρονται εσωτερικά στον οργανισμό δεν πρέπει να συνδυαστούν με τις εξωτερικές υπηρεσίες. Κάθε ένας πρέπει να έχει τον host (ξενιστή) του.
Το TFTP δεν υποστηρίζει την ίδια σειρά λειτουργιών με το FTP, και δεν έχει καμία ασφάλεια. Αυτή η υπηρεσία πρέπει μόνο να εξεταστεί για εσωτερική χρήση, και έπειτα πρέπει να διαμορφωθεί με έναν περιορισμένο τρόπο έτσι ώστε ο κεντρικός υπολογιστής να έχει μόνο πρόσβαση σε ένα σύνολο προκαθορισμένων αρχείων. Πιθανώς η πιο κοινή χρήση του TFTP είναι για τη μεταφόρτωση των αρχείων διαμόρφωσης δρομολογητών σε έναν δρομολογητή.

Το TFTP πρέπει να είναι εγκατεστημένο στον host (ξενιστή) του, και δεν πρέπει να εγκατασταθεί στους host (ξενιστές) που υποστηρίζουν την εξωτερική πρόσβαση FTP ή WWW.

3.2.3.7 NFS

Η υπηρεσία Network File επιτρέπει στους host (ξενιστές) να μοιράζονται κοινούς δίσκους. Το NFS χρησιμοποιείται συχνά από τους diskless hosts (ξενιστές) που εξαρτώνται από έναν κεντρικό υπολογιστή δίσκων για όλες τις ανάγκες αποθήκευσής τους.
Δυστυχώς, το NFS δεν έχει καμία ενσωματωμένη ασφάλεια. Είναι επομένως απαραίτητο ο κεντρικός υπολογιστής NFS να είναι προσβάσιμος μόνο από εκείνους τους host (ξενιστές) που τον χρησιμοποιούν για την υπηρεσία.
Αυτό επιτυγχάνεται με τη διευκρίνιση μέσω ποιου host (ξενιστή) το σύστημα αρχείων εξάγεται και με ποιο τρόπο (π.χ., μόνο ανάγνωση, ανάγνωση-γραφή, κ.λπ.).
Τα αρχεία συστήματος δεν πρέπει να εξαχθούν σε οποιουσδήποτε host (ξενιστές) έξω από το τοπικό δίκτυο δεδομένου ότι αυτό θα απαιτούσε η υπηρεσία NFS να είναι προσιτή εξωτερικά.
Ιδανικά, η εξωτερική πρόσβαση στην υπηρεσία NFS πρέπει να μπλοκάρεται από firewall.

3.2.4 Προστασία της ασφάλειας

Είναι καταπληκτικό πόσο συχνά ένας οργανισμός αγνοεί την προφανέστερη αδυναμία στην ασφάλειά του με την παραχώρηση ενός ανοικτού σε επίθεση κεντρικού υπολογιστή ασφάλειας.
Με βάση τις ανάγκες που συζητήθηκαν προηγουμένως, πρέπει να είναι σαφές ότι : ο κεντρικός υπολογιστής ασφάλειας δεν πρέπει να είναι προσιτός από τον έξω κόσμο, πρέπει να προσφέρει την ελάχιστη δυνατή πρόσβαση, εκτός από τη λειτουργία επικύρωσης, στους εσωτερικούς χρήστες και δεν πρέπει να συνδυαστεί με οποιουσδήποτε άλλους κεντρικούς υπολογιστές.

3.3 Η έννοια του firewall του Internet

Αν και η τεχνολογία της κρυπτογράφησης βοηθά να επιλυθούν πολλά προβλήματα της ασφάλειας, χρειάζεται και μια δεύτερη τεχνολογία. Η τεχνολογία αυτή, που ονομάζεται *Internet firewall,* βοηθά στην προστασία των υπολογιστών και των δικτύων ενός οργανισμού από ανεπιθύμητη κυκλοφορία του Internet. Όπως και ένα συμβατικό firewall, ένα firewall του Internet είναι σχεδιασμένο να εμποδίζει να εξαπλώνονται προβλήματα του Internet στους υπολογιστές ενός οργανισμού.
Ένα firewall τοποθετείται μεταξύ ενός οργανισμού και του υπόλοιπου Internet αυτό φαίνεται στην Εικόνα 1.

ΕΙΚΟΝΑ 1: Firewall που χρησιμοποιείται για να προστατεύει ένα οργανισμό από ανεπιθύμητες αλληλεπιδράσεις με το Internet.

Αν ένας οργανισμός έχει πολλές συνδέσεις με το Internet, πρέπει να τοποθετηθεί ένα firewall σε κάθε σύνδεση, και όλα τα firewall πρέπει να είναι διευθετημένα έτσι ώστε να επιβάλλουν την πολιτική ασφάλειας του οργανισμού. Ακόμα, το ίδιο το firewall πρέπει να είναι ασφαλές. Δηλαδή: Όλη η κυκλοφορία που εισέρχεται στον οργανισμό να περνά από το firewall .Όλη η κυκλοφορία που εξέρχεται από τον οργανισμό να περνά από το firewall. Το firewall να υλοποιεί την πολιτική ασφάλειας του οργανισμού, και να απορρίπτει οποιαδήποτε κυκλοφορία δεν είναι σύμφωνη με αυτή. Το ίδιο το firewall να είναι άτρωτο σε επιθέσεις κατά της ασφάλειας.

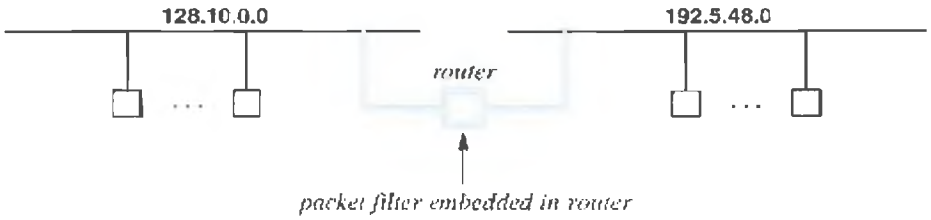
Το firewall είναι το πιο σημαντικό εργαλείο ασφάλειας που χρησιμοποιείται για να χειρίζεται τις δικτυακές συνδέσεις μεταξύ δύο οργανισμών που δεν εμπιστεύονται ο ένας τον άλλο. Τοποθετώντας ένα firewall σε κάθε εξωτερική σύνδεση δικτύου, ένας οργανισμός μπορεί να ορίσει μια *ασφαλή περίμετρο (secure perimeter)* η οποία εμποδίζει τους ξένους να αναμιγνύονται με τους υπολογιστές του. Ειδικότερα, με τον περιορισμό της πρόσβασης σε ένα μικρό σύνολο υπολογιστών, ένα firewall μπορεί να εμποδίζει τους ξένους να βολιδοσκοπούν όλους τους υπολογιστές ενός οργανισμού, κατακλύζοντας τα δίκτυα με ανεπιθύμητη κυκλοφορία, ή να επιτίθενται σε έναν υπολογιστή στέλνοντας μια ακολουθία αυτοδύναμων πακέτων IP (IP datagrams) η οποία είναι γνωστό ότι θα προκαλέσει στο υπολογιστικό σύστημα ανεπιθύμητη συμπεριφορά (π.χ. κατάρρευσης)

Ένα firewall μπορεί να μειώσει το κόστος της ασφάλειας. Χωρίς ένα firewall για να εμποδίζει την πρόσβαση, οι ξένοι μπορούν να στέλνουν πακέτα σε οποιουσδήποτε υπολογιστές ενός οργανισμού. Επομένως, για να παρέχει ασφάλεια ένας οργανισμός, θα πρέπει να κάνει ασφαλείς όλους τους υπολογιστές του. Με ένα firewall, όμως, ένας διαχειριστής μπορεί να περιορίσει τα εισερχόμενα πακέτα σε ένα μικρό σύνολο υπολογιστών. Στην πιο ακραία περίπτωση, το σύνολο αυτό μπορεί να αποτελείται από ένα

μόνο υπολογιστή. Αν και οι υπολογιστές αυτού ταυ συνόλου πρέπει να είναι *ασφαλείς, οι* άλλοι υπολογιστές του οργανισμού δε χρειάζεται να είναι ασφαλείς. Έτσι, ένας οργανισμός μπορεί να εξοικονομήσει χρήματα, επειδή είναι λιγότερο δαπανηρό να εγκαταστήσει ένα firewall παρά να κάνει ασφαλή όλα τα υπολογιστικά συστήματα.

3.3.1 Διαλογή πακέτων

Ο κύριος μηχανισμός που χρησιμοποιείται για τη δημιουργία ενός firewall ονομάζεται *φίλτρο πακέτων (packet filter}.* Όπως φαίνεται στην Εικόνα 2, ένα φίλτρο πακέτων είναι ενσωματωμένο σε ένα δρομολογητή (router). Το φίλτρο αποτελείται από λογισμικό που μπορεί να εμποδίζει κάποια πακέτα να περνούν από το δρομολογητή σε μια διαδρομή από ένα δίκτυο σε ένα άλλο. Ο διαχειριστής πρέπει να διευθετήσει το φίλτρο πακέτων για να καθορίσει ποια πακέτα επιτρέπεται να περνούν από το δρομολογητή και ποια πρέπει να μπλοκάρονται.



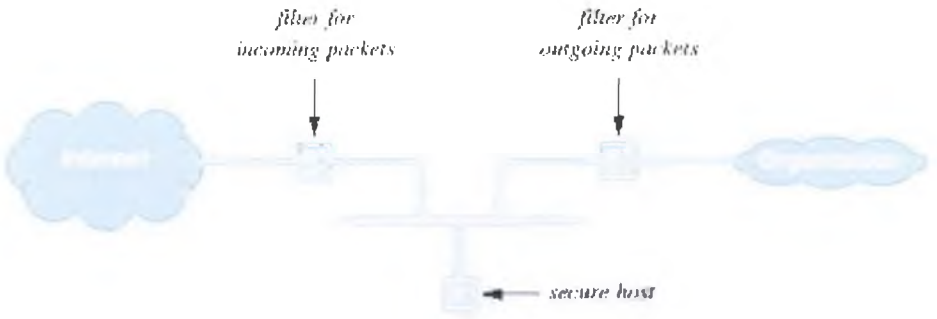
ΕΙΚΟΝΑ 2 : Η θέση ενός φίλτρου πακέτων. Το λογισμικό του φίλτρου είναι διευθετημένο να απορρίπτει τα καθορισμένα πακέτα καθώς περνούν από το ένα δίκτυο στο άλλο.

Ένα φίλτρο πακέτων λειτουργεί εξετάζοντας πεδία της κεφαλίδας του κάθε πακέτου. Το φίλτρο μπορεί να διευθετηθεί έτσι ώστε να καθοριστεί ποια πεδία κεφαλίδων θα εξετάζονται και πώς θα ερμηνεύονται οι τιμές. Για να ελέγχει ο διαχειριστής ποιοι υπολογιστές του δικτύου μπορούν να επικοινωνούν με υπολογιστές ενός άλλου δικτύου, ορίζει ότι το φίλτρο θα πρέπει να εξετάζει τα πεδία *αφετηρίας (source)* και *προορισμού (destination)* της κάθε κεφαλίδας αυτοδύναμου πακέτου.
Στην εικόνα, για να μην επιτρέπεται σε έναν υπολογιστή του δεξιού δικτύου με διεύθυνση IP *192.5.48.27* να επικοινωνεί με οποιουσδήποτε υπολογιστές του αριστερού δικτύου, ο διαχειριστής ορίζει ότι το φίλτρο θα πρέπει να μπλοκάρει όλα τα πακέτα που έχουν διεύθυνση αφετηρίας ίση με *192.5.48.27.* Παρόμοια, για να μην επιτρέπεται σε έναν υπολογιστή του αριστερού δικτύου με διεύθυνση *128.10.0.32* να λαμβάνει οποιαδήποτε πακέτα από το δεξιό δίκτυο, ο διαχειριστής ορίζει ότι το φίλτρο θα πρέπει να μπλοκάρει όλα τα πακέτα που έχουν διεύθυνση προορισμού ίση με *128.10.0.32.*
Εκτός από τη χρήση των διευθύνσεων IP αφετηρίας και προορισμού, ένα φίλτρο πακέτων μπορεί να εξετάζει το πρωτόκολλο του πακέτου ή την υπηρεσία υψηλού επιπέδου στην

οποία αυτό αντιστοιχεί. Η δυνατότητα να μπλοκάρονται επιλεκτικά τα πακέτα μιας συγκεκριμένης υπηρεσίας σημαίνει ότι ο διαχειριστής μπορεί να εμποδίζει την κυκλοφορία για μια υπηρεσία ενώ επιτρέπει την κυκλοφορία για μια άλλη. Για παράδειγμα, ο διαχειριστής μπορεί να διευθετήσει ένα φίλτρο πακέτων έτσι ώστε να μπλοκάρει όλα τα πακέτα που μεταφέρουν επικοινωνίες του Παγκόσμιου Ιστού (WWW), ενώ επιτρέπει να περνούν τα πακέτα που μεταφέρουν κυκλοφορία e-mail.
Ένας μηχανισμός φίλτρου πακέτων επιτρέπει στο διαχειριστή να ορίζει σύνθετους συνδυασμούς διευθύνσεων αφετηρίας και προορισμού και υπηρεσιών. Συνήθως, το λογισμικό του φίλτρου πακέτων επιτρέπει στο διαχειριστή να ορίζει λογικούς συνδυασμούς αφετηρίας, προορισμού, και τύπου υπηρεσίας. Έτσι, ο διαχειριστής μπορεί να ελέγχει την πρόσβαση για κάποιες συγκεκριμένες υπηρεσίες σε κάποιους συγκεκριμένους υπολογιστές. Για παράδειγμα, ένας διαχειριστής μπορεί να επιλέξει να μπλοκάρει όλη την κυκλοφορία που προορίζεται για την υπηρεσία FTP στον υπολογιστή *128.10.2.14,* όλη την κυκλοφορία Παγκόσμιου Ιστού που προέρχεται από τον υπολογιστή *192.5.48.33,* και όλη την κυκλοφορία e-mail που προέρχεται από τον υπολογιστή *192.5.48.34.* Το φίλτρο μπλοκάρει μόνο τους καθορισμένους συνδυασμούς, ενώ αφήνει να περνά η κυκλοφορία που προορίζεται για άλλους υπολογιστές και η κυκλοφορία άλλων υπηρεσιών στους καθορισμένους υπολογιστές.

3.3.2 Χρήση φίλτρων πακέτων για τη δημιουργία firewall

Στην πράξη, ένα firewall του διαδικτύου αποτελείται τουλάχιστον από τρία συστήματα. Ένα φίλτρο πακέτων περιορίζει τα αυτοδύναμα πακέτα που φτάνουν από το διαδίκτυο. Ένα ξεχωριστό φίλτρο πακέτων περιορίζει τα αυτοδύναμα πακέτα που φεύγουν από το ενδοδίκτυο του οργανισμού. Τέλος, ένα ασφαλές υπολογιστικό σύστημα στο firewall εκτελεί λογισμικό εφαρμογών. Η αρχιτεκτονική αυτή παρουσιάζεται στην Εικόνα 3.



Εικόνα 3 Η αρχιτεκτονική ενός firewall με ένα ασφαλή υπολογιστή ανάμεσα σε δυο φίλτρα πακέτων. Το ένα φίλτρο περιορίζει τα εισερχόμενα πακέτα, και το άλλο περιορίζει τα εξερχόμενα πακέτα

Όπως φαίνεται στην εικόνα, ο ασφαλής υπολογιστής υπηρεσίας είναι τοποθετημένος στο δίκτυο που συνδέει και τους δρομολογητές. Λογικά, ο ασφαλής υπολογιστής υπηρεσίας είναι τοποθετημένος "ανάμεσα" στα δύο φίλτρα πακέτων - τα φίλτρα πακέτων είναι διευθετημένα να κατευθύνουν τα πακέτα στον υπολογιστή υπηρεσίας. Δηλαδή, το φίλτρο στο δρομολογητή ri είναι διευθετημένο να απορρίπτει όλα τα εισερχόμενα πακέτα εκτός από εκείνα που προορίζονται για συγκεκριμένες εφαρμογές οι οποίες εκτελούνται στον ασφαλή υπολογιστή υπηρεσίας. Παρόμοια, το φίλτρο στο δρομολογητή R2 είναι διευθετημένο να απορρίπτει όλα τα εξερχόμενα πακέτα εκτός από εκείνα που προορίζονται για εφαρμογές που εκτελούνται στον ασφαλή υπολογιστή υπηρεσίας. Έτσι, όλες οι επικοινωνίες μεταξύ υπολογιστών του οργανισμού και του παγκόσμιου διαδικτύου, του Internet, περνούν από τον ασφαλή υπολογιστή υπηρεσίας.

Τι λογισμικό είναι διαθέσιμο στον ασφαλή υπολογιστή υπηρεσίας;

Ένας ασφαλής υπολογιστής υπηρεσίας εκτελεί ειδικά προγράμματα-εφαρμογές τα οποία λέγονται πύλες επιπέδου εφαρμογών (application-layer gateways) ή μεσολαβητές (proxies), που παρέχουν ασφαλείς υπηρεσίες για το Internet. Για παράδειγμα, ας υποθέσουμε ότι ένα χρήστης μέσα στον οργανισμό θέλει να χρησιμοποιήσει το FTP για να αποκτήσει ένα αρχείο. Όταν ο χρήστης κάνει μια αίτηση, το λογισμικό-πελάτης στον υπολογιστή του έρχεται σε επαφή με έναν μεσολαβητή FTP στον ασφαλή υπολογιστή υπηρεσίας. Όταν ο πελάτης στέλνει μια αίτηση για ένα αρχείο, ο μεσολαβητής επαληθεύει αν η αίτηση επιτρέπεται από την πολιτική ασφάλειας του οργανισμού, αποκτά ένα αντίγραφο του αρχείου από ένα διακομιστεί του Internet, ελέγχει το αντίγραφο για ιούς, και έπειτα μεταβιβάζει το αντίγραφο πίσω στον υπολογιστή του χρήστη. Το λογισμικό πύλης εφαρμογών μπορεί επίσης να κρατά μια καταγραφή όλων των αιτήσεων για να μπορούν να ελέγχονται εκτός σύνδεσης.

Υπάρχουν σημαντικά οφέλη ασφάλειας που μπορούν να προκύψουν από τη χρησιμοποίηση των κεντρικών υπολογιστών proxy. Είναι δυνατό να προστεθούν κατάλογοι ελέγχου πρόσβασης στα πρωτόκολλα, που απαιτούν από τους χρήστες ή τα συστήματα να παρέχουν κάποιο επίπεδο επικύρωσης προτού να χορηγηθεί η πρόσβαση. Οι εξυπνότεροι κεντρικοί υπολογιστές proxy, αποκαλούμενοι μερικές φορές και πύλες στρώματος εφαρμογής (ALGs), μπορούν να καταλαβαίνουν τα συγκεκριμένα πρωτόκολλα και μπορούν να διαμορφωθούν για να εμποδίσουν μόνο τις υπό-ενότητες του πρωτοκόλλου.

Παραδείγματος χάριν, ένα ALG για το FTP μπορεί να δείξει τη διαφορά μεταξύ της "put" εντολής και "get" εντολής. Μια οργάνωση μπορεί να θελήσει να επιτρέψει στους χρήστες να " πάρουν" τα αρχεία από το Διαδίκτυο, αλλά να μην είναι σε θέση να "βάλει" τα εσωτερικά αρχεία σε έναν μακρινό κεντρικό υπολογιστή. Σε αντίθεση, ένας δρομολογητής φιλτραρίσματος θα μπορούσε να εμποδίσει όλη την πρόσβαση FTP ή ακόμα και καμία πρόσβαση FTP, αλλά όχι ένα υποσύνολο.

Οι κεντρικοί υπολογιστές proxy μπορούν επίσης να κρυπτογραφήσουν δεδομένα βασισμένοι σε διάφορες παραμέτρους.

Μια οργάνωση μπορεί να χρησιμοποιήσει αυτό το χαρακτηριστικό γνώρισμα για να επιτρέψει κρυπτογραφημένες συνδέσεις μεταξύ δύο θέσεων των οποίων τα μόνα σημεία πρόσβασης είναι στο διαδίκτυο.

Τα κόστος των firewall αρχίζει από περίπου $10.000US και υπερβαίνει τα $250.000US. Υπάρχουν επίσης και firewall μικρού κόστους[Norton Personal Firewall]

Πρέπει να αναφερθεί ότι η σωστή οργάνωση ενός firewall (εμπορικού ή αυτοσχέδιου) απαιτεί μεγάλη ικανότητα και γνώση του TCP/IP. Και οι δύο τύποι

απαιτούν συντήρηση, εγκατάσταση των επιδιορθώσεων λογισμικού και των αναβαθμίσεων, καθώς και έλεγχο. Κατά την σύνταξη προϋπολογισμού για ένα firewall, αυτές οι συμπληρωματικές δαπάνες πρέπει να εξεταστούν εκτός από το κόστος των φυσικών στοιχείων του firewall.
Όπως με όλα τα μέτρα ασφάλειας, είναι σημαντικό να παρθούν αποφάσεις σχετικά με την απειλή, την αξία των πόρων που προστατεύονται, και των δαπανών για την εφαρμογή της ασφάλειας.
Τα firewall μπορούν να παρέχουν μεγάλη βοήθεια κατά την εφαρμογή της ασφάλειας ενός οργανισμού και προστατεύουν από μια μεγάλη ποικιλία επιθέσεων.
Αλλά είναι σημαντικό να ληφθεί υπόψη ότι είναι μόνο ένα μέρος της λύσης. Δεν μπορούν να προστατεύσουν έναν οργανισμό από όλους τους τύπους επιθέσεων.

Κεφάλαιο 4. Υπηρεσίες & διαδικασίες ασφάλειας

4.1 Καθορισμός όρων

Οι ορισμοί που παρουσιάζονται εδώ είναι εστιασμένοι στα θέματα που συζητούνται στην παρούσα εργασία.

Πιστοποίηση: Η χορήγηση δικαιωμάτων πρόσβασης βασισμένων σε μια επικυρωμένη ταυτότητα.

Εμπιστευτικότητα: Η προστασία των πληροφοριών έτσι ώστε κάποιος μη-εξουσιοδοτημένος, χρήστης που θα αποκτήσει πρόσβαση σε πληροφορίες, να μην μπορεί να τις διαβάσει ακόμα κι αν μπορεί να δει το δοχείο των πληροφοριών (π.χ., αρχείο υπολογιστών ή δίκτυο).

Ακεραιότητα των δεδομένων (Data Integrity): Η ακεραιότητα αναφέρεται στην προστασία από αλλαγές: Είναι τα δεδομένα που έρχονται σε έναν παραλήπτη ακριβώς τα ίδια με τα δεδομένα που έχουν σταλεί;

Εξουσιοδότηση: Η επαλήθευση της ταυτότητας της πηγής πληροφοριών.

Κρυπτογράφηση: Ένας μηχανισμός που χρησιμοποιείται συχνά για να παρέχει εμπιστευτικότητα.

Ενεργός επίθεση: Μια προσπάθεια να τροποποιηθούν εσφαλμένα τα στοιχεία, να αποκτήσουν επικύρωση, ή να αποκτήσουν πιστοποίηση με την εισαγωγή ψεύτικων πακέτων στο ρεύμα στοιχείων ή με την τροποποίηση των πακέτων που μεταφέρουν το ρεύμα των στοιχείων. (Βλ. παθητικές επιθέσεις και επιθέσεις επανάληψης.)

Ασύμμετρη κρυπτογραφία: Ένα σύστημα κρυπτογράφησης που χρησιμοποιεί διαφορετικά κλειδιά, για την κρυπτογράφηση και την αποκρυπτογράφηση. Τα δύο κλειδιά έχουν εγγενής μαθηματική σχέση το ένα με το άλλο. Επίσης αποκαλείτε Public-Key-Cryptography. (Βλ. συμμετρικό σύστημα κρυπτογραφίας)

Βασικό πιστοποιητικό: Μια δομή δεδομένων που αποτελείται από ένα δημόσιο κλειδί, ταυτότητα του προσώπου, του συστήματος, ή του ρόλου που συνδέεται με αυτό το κλειδί, και πληροφορίες που επικυρώνουν και το κλειδί και την ένωση μεταξύ της ταυτότητας και του δημόσιου κλειδιού. Τα κλειδιά που χρησιμοποιούνται από PEM είναι ένα παράδειγμα βασικού πιστοποιητικου.

Παθητική επίθεση: Μια επίθεση σε ένα σύστημα επικύρωσης που δεν παρεμβάλλει κανένα στοιχείο στο ρεύμα, αλλά άντ' αυτού είναι σε θέση να ελέγχει παθητικά πληροφορίες που στέλνονται μεταξύ άλλων συμβαλλόμενων μερών. Αυτές οι πληροφορίες θα μπορούσαν να χρησιμοποιηθούν πιο μετά μαζί με αυτό που εμφανίζεται σαν μια έγκυρη σύνοδος.

Σαφές-κείμενο: Κείμενο μη-κρυπτογραφημένο.

Επίθεση επανάληψης: Μια επίθεση σε ένα σύστημα επικύρωσης καταγράφοντας και επαναλαμβάνοντας τα προηγούμενα σταλμένα έγκυρα μηνύματα (ή μέρη μηνυμάτων). Οποιεσδήποτε σταθερές πληροφορίες επικύρωσης, όπως ο κωδικός πρόσβασης ή τα ηλεκτρονικά διαβιβασθέντα βιομετρικά στοιχεία, μπορούν να καταγραφούν και να χρησιμοποιηθούν αργότερα για να πλαστογραφηθούν τα μηνύματα ώστε να μοιάζουν ως αυθεντικά.

Συμμετρικό σύστημα κρυπτογραφίας: Ένα σύστημα κρυπτογράφησης που χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Μερικές φορές αναφέρεται ως Secret-Key-Cryptography.

4.2 Πιστοποίηση

Για πολλά έτη, η πιο κοινή μέθοδος για την επικύρωση χρηστών ήταν μέσω της χρήσης τυποποιημένων και επαναχρησιμοποιήσιμων κωδικών πρόσβασης. Αρχικά, αυτοί οι κωδικοί πρόσβασης χρησιμοποιήθηκαν από τους χρήστες στα τερματικά για να επικυρώνονται σε έναν κεντρικό υπολογιστή.
Σε προηγούμενες περιόδους, δεν υπήρχε κανένα δίκτυο (εσωτερικό ή εξωτερικό), έτσι ο κίνδυνος κοινοποίησης του κωδικού πρόσβασης ήταν ελάχιστος. Σήμερα, τα συστήματα συνδέονται μέσω τοπικών δικτύων, και αυτά τα τοπικά δίκτυα συνδέονται περαιτέρω και με το Διαδίκτυο.
Οι χρήστες συνδέονται από όλη τη γη. Οι επαναχρησιμοποιήσιμοι κωδικοί πρόσβασής τους διαβιβάζονται συχνά στα ίδια δίκτυα σε σαφές κείμενο και μπορούν να αναχαιτιστούν από πιθανούς εισβολείς.
Και πράγματι, το CERT Coordination Center και άλλες ομάδες έχουν παρατηρήσει έναν τεράστιο αριθμό γεγονότων που περιλαμβάνουν sniffers πακέτων οι οποίοι συλλαμβάνουν τους κωδικούς πρόσβασης.
Με την εμφάνιση νεώτερων τεχνολογιών όπως οι one-time κωδικοί πρόσβασης (π.χ., s/key), PGP, και οι σε token-βασισμένες συσκευές επικύρωσης, οι άνθρωποι χρησιμοποιούν ακολουθίες που μοιάζουν με κωδικούς πρόσβασης σε μορφή token και pins.
Εάν αυτά τα μυστικά tokens και pins δεν επιλέγονται και προστατεύονται κατάλληλα, η επικύρωση μπορεί εύκολα να υπονομευτεί.

4.2.1 One-Time κωδικοί πρόσβασης

Λαμβάνοντας υπόψη τα σημερινά δικτυωμένα περιβάλλοντα, συνιστάται στους οργανισμούς που ενδιαφέρονται για την ασφάλεια και την ακεραιότητα των συστημάτων και των δικτύων τους, να αναθεωρούν τους τυποποιημένους, επαναχρησιμοποιήσιμους κωδικούς πρόσβασης.
Έχουν υπάρξει πολλές περιπτώσεις Trojan προγραμμάτων (π.χ., Telnet και rlogin) και sniffing προγραμμάτων τα οποία συλλαμβάνουν το σαφές κείμενο name/account name/password triplets.
Οι εισβολείς μπορούν να χρησιμοποιήσουν τις συλληφθείσες πληροφορίες για να αποκτήσουν πρόσβαση σε εκείνους τους host (ξενιστές) και λογαριασμούς. Αυτό είναι δυνατό επειδή:

1) Ο κωδικός πρόσβασης χρησιμοποιείται επανειλημμένως (ως εκ τούτου ο όρος "επαναχρησιμοποιήσιμος")
2) Οι κωδικοί πρόσβασης περνούν μέσω του δικτύου σε σαφές κείμενο.

Έχουν αναπτυχθεί διάφορες τεχνικές επικύρωσης που εξετάζουν αυτό το πρόβλημα. Μεταξύ αυτών των τεχνικών είναι οι τεχνολογίες πρόκλησης-απάντησης που παρέχουν τους κωδικούς πρόσβασης που χρησιμοποιούνται μόνο μία φορά (συνήθως αποκαλούμενοι one-time κωδικοί πρόσβασης).
Υπάρχουν διάφορα διαθέσιμα προϊόντα που οι οργανισμοί πρέπει να λάβουν υπόψιν τους. Η απόφαση να χρησιμοποιηθεί ένα προϊόν είναι ευθύνη κάθε οργάνωσης, και κάθε οργάνωση πρέπει να εκτελέσει την αξιολόγηση και την επιλογή του.

4.2.2 Kerberos

Το Kerberos είναι ένα διανεμημένο σύστημα ασφάλειας δικτύων που προσφέρει επικύρωση σε μη ασφαλή δίκτυα. Εάν απαιτείται από την εφαρμογή, η ακεραιότητα και η κρυπτογράφηση μπορούν επίσης να παρασχεθούν.
Το Kerberos αναπτύχθηκε αρχικά στο ίδρυμα της Μασαχουσέτης τεχνολογίας (MIT) στα μέσα της δεκαετίας του '80. Υπάρχουν δύο σημαντικές εκδόσεις Kerberos, η έκδοση 4 και 5, οι οποίες είναι για πρακτικούς λόγους, ασύμβατες.
Το Kerberos στηρίζεται σε μια συμμετρική βάση δεδομένων χρησιμοποιώντας ένα βασικό κέντρο διανομής (KDC) που είναι γνωστό ως κεντρικός υπολογιστής Kerberos. Σε έναν χρήστη ή σε μια υπηρεσία (γνωστό ως "principals") χορηγούνται ηλεκτρονικά "εισιτήρια" μετά από την επικοινωνία με το KDC. Αυτά τα εισιτήρια χρησιμοποιούνται για την επικύρωση μεταξύ των principals.
Όλα τα εισιτήρια περιλαμβάνουν ένα χρονικό γραμματόσημο που περιορίζει το χρονικό διάστημα για το οποίο το εισιτήριο ισχύει. Επομένως, οι πελάτες του Kerberos και ο κεντρικός υπολογιστής πρέπει να έχουν μια ασφαλή χρονική πηγή
Η πρακτική πλευρά του Kerberos είναι η ολοκλήρωσή του με το επίπεδο εφαρμογής. Οι χαρακτηριστικές εφαρμογές όπως το FTP, Telnet, POP, και NFS έχουν ενσωματωθεί στο σύστημα Kerberos.

4.2.3 Επιλογή και προστασία των μυστικών Tokens και PINs

Κατά την επιλογή των μυστικών tokens, πρέπει να δοθεί ιδιαίτερη προσοχή. Δηλαδή δεν πρέπει να είναι μεμονωμένες λέξεις οι οποίες να είναι κοινές. Ιδανικά, θα είναι μεγαλύτερα παρά μικρότερα και θα αποτελούνται από φράσεις που συνδυάζουν ψηφία και άλλους χαρακτήρες.
Η προστασία αυτών των μυστικών σημείων γίνεται πολύ σημαντική μόλις επιλεχτεί. Μερικά χρησιμοποιούνται ως pins στις συσκευές υλικού (όπως οι token κάρτες) και δεν πρέπει να γραφτούν ή να τοποθετηθούν στην ίδια θέση με τη συσκευή με την οποία συνδέονται.
Ένα αρκετά καλό κλειδί μυστικότητας (PGP), πρέπει να προστατευθεί από αναρμόδια πρόσβαση. Κατά τη χρησιμοποίηση προϊόντων κρυπτογράφησης, όπως το PGP, πρέπει να δοθεί προσοχή στον καθορισμό του κατάλληλου μήκους και να εξασφαλιστεί επιπλέον ότι οι χρήστες έχουν εκπαιδευτεί για να το κάνουν.

Καθώς η τεχνολογία μεγαλώνει, το ελάχιστο ασφαλές βασικό μήκος συνεχίζει να αυξάνεται.
Πρέπει να υπάρχει σιγουριά ότι ο οργανισμός συμβαδίζει με τις τελευταίες τεχνολογικές εξελίξεις έτσι ώστε να μπορεί να εξασφαλιστεί ότι οποιαδήποτε χρησιμοποιούμενη κρυπτογραφία παρέχει την προστασία που χρειάζεται.

4.2.4 Διαβεβαίωση κωδικού πρόσβασης

Ενώ είναι πολύ σημαντικό να αποβληθεί η χρήση των τυποποιημένων, επαναχρησιμοποιήσιμων κωδικών πρόσβασης, αναγνωρίζεται ότι μερικές οργανώσεις μπορεί ακόμα να τους χρησιμοποιούν.
Ενώ συνιστάται μετάβαση αυτών των οργανώσεων σε χρήση καλύτερης τεχνολογίας, στο μεταξύ, υπάρχουν οι ακόλουθες συμβουλές που βοηθούν στην επιλογή και τη συντήρηση παραδοσιακών κωδικών πρόσβασης.
Πρέπει όμως να αναφερθεί, ότι κανένα από αυτά τα μέτρα δεν παρέχει προστασία ενάντια στην κοινοποίηση λόγω των προγραμμάτων sniffer.

(1) Η σημασία των δυνατών κωδικών πρόσβασης

Στις πιο πολλές (εάν όχι τις περισσότερες) περιπτώσεις παραβίασης συστημάτων, ο εισβολέας πρέπει να αποκτήσει πρόσβαση σε έναν λογαριασμό του συστήματος.
Ένας τρόπος ολοκλήρωσης μιας εισβολής είναι μέσω της εικασίας του κωδικού πρόσβασης ενός νόμιμου χρήστη. Αυτό ολοκληρώνεται συχνά με την εκτέλεση ενός αυτοματοποιημένου προγράμματος σπασίματος κωδικού πρόσβασης, που χρησιμοποιεί ένα πολύ μεγάλο λεξικό.
Ο μόνος τρόπος άμυνας ενάντια στους κωδικούς πρόσβασης που αποκαλύπτονται με αυτόν τον τρόπο είναι μέσω της προσεκτικής επιλογής κωδικών πρόσβασης που δεν μπορούν να μαντευθούν εύκολα (δηλ., συνδυασμοί αριθμών, γραμμάτων, και χαρακτήρων στίξης).Οι κωδικοί πρόσβασης πρέπει επίσης να είναι τόσο μεγάλοι όσο το σύστημα υποστηρίζει και όσο μπορούν να ανεχτούν οι χρήστες συστημάτων.

(2) Αλλάζοντας τους αρχικούς κωδικούς

Πολλά λειτουργικά συστήματα και προγράμματα εφαρμογής εγκαθίστανται με τους αρχικούς λογαριασμούς και κωδικούς πρόσβασης .Αυτοί πρέπει να αλλάξουν αμέσως σε κάτι που δεν μπορεί να μαντευθεί ή να σπαστεί.

(3) Περιορίζοντας την πρόσβαση στο αρχείο κωδικού πρόσβασης

Ειδικότερα, ένας οργανισμός θέλει να προστατεύσει την κρυπτογραφημένη μερίδα κωδικού πρόσβασης του αρχείου έτσι ώστε οι εισβολείς να μην μπορούν να τους σπάσουν.
Μια αποτελεσματική τεχνική είναι να χρησιμοποιηθούν οι shadow κωδικοί πρόσβασης όπου ο τομέας κωδικού πρόσβασης του τυποποιημένου αρχείου περιέχει έναν πλαστό ή ψεύτικο κωδικό πρόσβασης. Το αρχείο που περιέχει τους νόμιμους κωδικούς πρόσβασης προστατεύεται αλλού στο σύστημα.

(4) Κωδικός πρόσβασης που παλιώνει

Το πότε και πώς πρέπει να λήξουν οι κωδικοί πρόσβασης αποτελεί ακόμα ένα αντικείμενο διαμάχης μεταξύ της κοινότητας ασφάλειας.
Γενικά είναι αποδεκτό ότι ένας κωδικός πρόσβασης δεν πρέπει να διατηρηθεί αν δεν είναι πλέον σε χρήση ένας λογαριασμός, αλλά συζητείται εάν ένας χρήστης πρέπει να αναγκαστεί να αλλάξει έναν καλό κωδικό πρόσβασης που βρίσκεται σε χρήση.
Τα επιχειρήματα για τους μεταβαλλόμενους κωδικούς πρόσβασης αφορούν την πρόληψη της συνεχούς χρήσης των παραβιασμένων λογαριασμών.
Εντούτοις, η αντίθετη άποψη υποστηρίζει ότι οι συχνές αλλαγές κωδικού πρόσβασης οδηγούν τους χρήστες στο να γράφουν τους κωδικούς πρόσβασής τους σε ορατές περιοχές (όπως η συγκόλληση τους σε ένα τερματικό),ή στο να επιλέγουν πολύ απλούς κωδικούς πρόσβασης που είναι εύκολο να μαντευτούν.
Πρέπει επίσης να αναφερθεί ότι ένας εισβολέας πιθανώς θα βρει έναν κωδικό πρόσβασης σύντομα οπότε σε αυτή την περίπτωση ο κωδικός πρόσβασης που παλιώνει παρέχει λίγη εάν όχι καθόλου προστασία.
Ενώ δεν υπάρχει καμία οριστική απάντηση σε αυτό το δίλημμα, πρέπει το ζήτημα να αντιμετωπίσει άμεσα μέσω μιας πολιτικής κωδικού πρόσβασης και να παρέχει οδηγίες για το πόσο συχνά ένας χρήστης πρέπει να αλλάζει τον κωδικό πρόσβασης.
Βεβαίως, μια ετήσια αλλαγή στον κωδικό πρόσβασής δεν είναι συνήθως δύσκολη για τους περισσότερους χρήστες.
Συνιστάται οι κωδικοί πρόσβασης να αλλάζουν τουλάχιστον όποτε ένας προνομιούχος λογαριασμός παραβιάζεται, ή σε περίπτωση που υπάρχει μια κρίσιμη αλλαγή στο προσωπικό (ειδικά εάν είναι διαχειριστής), ή όταν παραβιαστεί ένας λογαριασμός.
Επιπλέον, εάν ένας προνομιούχος κωδικός πρόσβασης λογαριασμού παραβιαστεί, όλοι οι κωδικοί πρόσβασης στο σύστημα πρέπει να αλλάξουν.

(5) Φράξιμο κωδικού πρόσβασης-λογαριασμού

Μερικοί οργανισμοί το βρίσκουν χρήσιμο να θέσουν εκτός λειτουργίας τους λογαριασμούς μετά από έναν προκαθορισμένο αριθμό αποτυχημένων προσπαθειών για επικύρωση.
Εάν ο οργανισμός αποφασίζει να χρησιμοποιήσει αυτόν τον μηχανισμό, συνιστάται ο μηχανισμός να μην "διαφημίζει" τον εαυτό του κατόπιν της απενεργοποίησης, ακόμα κι αν παρουσιάζεται ο σωστός κωδικός πρόσβασης, Το μήνυμα που επιδεικνύεται πρέπει να παραμείνει μια αποτυχημένη προσπάθεια σύνδεσης.
Η εφαρμογή αυτού του μηχανισμού απαιτεί από τους νόμιμους χρήστες να έρχονται σε επαφή με τον διαχειριστή των συστημάτων για να ζητήσουν να επανενεργοποιηθεί ο λογαριασμός τους.

4.3 Προσεγγίσεις για την πιστοποίηση μηνύματος

Ένα μήνυμα, αρχείο, έγγραφο ή άλλη συλλογή από δεδομένα θεωρείται αυθεντική όταν είναι γνήσια και έρχεται από την ισχυριζόμενη πηγή της. Η πιστοποίηση μηνύματος είναι μία διαδικασία που επιτρέπει στις επικοινωνούσες ομάδες να επαληθεύσουν πως τα ληφθέντα μηνύματα είναι αυθεντικά. Οι δύο σημαντικές όψεις είναι να επαληθευτεί πως δεν έχουν μεταβληθεί τα περιεχόμενα του μηνύματος και

πως η πηγή είναι αυθεντική. Μπορεί επίσης να επιθυμούμε να επαληθεύσουμε την επικαιρότητα του μηνύματος (δεν είναι τεχνητά καθυστερημένο ή επανεκτελέσιμο) και την ακολουθία σχετικά με άλλα μηνύματα που ρέουν μεταξύ των δύο ομάδων.

4.3.1 Πιστοποίηση χρησιμοποιώντας συμβατική κρυπτογράφηση

Είναι δυνατό να εκτελέσουμε πιστοποίηση απλά με τη χρήση συμβατικής κρυπτογράφησης. Εάν θεωρήσουμε ότι διαμοιράζονται ένα κλειδί μόνον ο αποστολέας και ο παραλήπτης (το οποίο έτσι θα πρέπει να είναι), τότε μόνον ο γνήσιος αποστολέας θα είναι ικανός να κρυπτογραφήσει επιτυχώς ένα μήνυμα για τον άλλο συμμετέχοντα. Επιπλέον, εάν το μήνυμα περιλαμβάνει ένα κώδικα ανίχνευσης σφαλμάτων και έναν αριθμό ακολουθίας, ο παραλήπτης διαβεβαιώνεται πως δεν
έχουν γίνει αλλαγές και η ακολουθία είναι κατάλληλη. Εάν το μήνυμα περιλαμβάνει επίσης μία χρονοσήμανση, ο παραλήπτης διαβεβαιώνεται πως το μήνυμα δεν έχει καθυστερηθεί πέραν αυτού που φυσιολογικά αναμένεται για τη διάσχιση του δικτύου

4.3.1.1 Πιστοποίηση ταυτότητας με ψηφιακές υπογραφές

Ένας μηχανισμός κρυπτογράφησης μπορεί επίσης να χρησιμοποιείται για την πιστοποίηση της ταυτότητας του αποστολέα ενός μηνύματος. Η τεχνική αυτή ονομάζεται *ψηφιακή υπογραφή (digital signature).* Για να υπογράψει ένα μήνυμα, ο αποστολέας κρυπτογραφεί το μήνυμα χρησιμοποιώντας ένα κλειδί που είναι γνωστό μόνο σε αυτόν. Ο αποδέκτης χρησιμοποιεί την αντίστροφη συνάρτηση για να αποκρυπτογραφήσει το μήνυμα. Ο αποδέκτης γνωρίζει ποιος έστειλε το μήνυμα, επειδή μόνο ο αποστολέας έχει το κλειδί που χρειάζεται για να πραγματοποιηθεί η κρυπτογράφηση. Για να εξασφαλιστεί ότι τα κρυπτογραφημένα μηνύματα δεν μπορούν να αντιγραφούν και να ξανασταλθούν αργότερα, το αρχικό μήνυμα μπορεί να περιέχει την ημερομηνία και την ώρα που δημιουργήθηκε.
Ας εξετάσουμε πώς μπορεί να χρησιμοποιηθεί ένα σύστημα δημόσιου κλειδιού για να παρέχει ψηφιακή υπογραφή. Για να υπογράψει ο χρήστης ένα μήνυμα, το κρυπτογραφεί χρησιμοποιώντας το ιδιωτικό κλειδί του. Για να επαληθεύσει την υπογραφή ο αποδέκτης, βρίσκει το δημόσιο κλειδί του χρήστη και το χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα. Επειδή μόνο ο χρήστης γνωρίζει το ιδιωτικό κλειδί, μόνο αυτός μπορεί να κρυπτογραφήσει ένα μήνυμα που να μπορεί να αποκωδικοποιηθεί με το δημόσιο κλειδί.
Είναι ενδιαφέρον ότι μπορούν να χρησιμοποιηθούν δύο επίπεδα κρυπτογράφησης για να εξασφαλιστεί ότι ένα μήνυμα είναι και αυθεντικό και εμπιστευτικό. Πρώτον, για να υπογραφεί το μήνυμα, χρησιμοποιείται το ιδιωτικό κλειδί του αποστολέα για την κρυπτογράφηση του. Δεύτερον, το κρυπτογραφημένο μήνυμα κρυπτογραφείται ξανά με το δημόσιο κλειδί του αποδέκτη. Μαθηματικά, η διπλή κρυπτογράφηση μπορεί να εκφραστεί έτσι

$$X = encrypt\ (pub\text{-}u2,\ encrypt(prv\text{-}ul,\ M))$$

όπου το *M* αντιπροσωπεύει το μήνυμα που στέλνεται, το X αντιπροσωπεύει το αλφαριθμητικό που προκύπτει από τη διπλή κρυπτογράφηση, το *prv-ul*

αντιπροσωπεύει το ιδιωτικό κλειδί του αποστολέα, και το *pub-u2* αντιπροσωπεύει το δημόσιο κλειδί του αποδέκτη.
Στην πλευρά του αποδέκτη, η διαδικασία αποκρυπτογράφησης είναι η αντίστροφη της διαδικασίας κρυπτογράφησης. Πρώτον, ο αποδέκτης χρησιμοποιεί το ιδιωτικό κλειδί του για να αποκρυπτογραφήσει το μήνυμα. Η αποκρυπτογράφηση αφαιρεί ένα επίπεδο κρυπτογράφησης, αλλά αφήνει το μήνυμα με ψηφιακή υπογραφή. Δεύτερον, ο αποδέκτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει ξανά το μήνυμα. Η διαδικασία αυτή μπορεί να εκφραστεί ως

M =decrypt (pub-ul, decrypt(prv-u2, X))

όπου το *X* αντιπροσωπεύει το κρυπτογραφημένο αλφαριθμητικό που μεταφέρθηκε μέσω του δικτύου, το *M* αντιπροσωπεύει το αρχικό μήνυμα, το *prv-u2* αντιπροσωπεύει το ιδιωτικό κλειδί του αποδέκτη, και το *pub-ul* αντιπροσωπεύει το δημόσιο κλειδί του αποστολέα.
Αν προκύψει από τη διπλή αποκρυπτογράφηση ένα μήνυμα που έχει νόημα, το μήνυμα αυτό θα πρέπει να είναι εμπιστευτικό και αυθεντικό. Το μήνυμα πρέπει να έχει φτάσει στον αποδέκτη για τον οποίο προοριζόταν, επειδή μόνο ο αποδέκτης έχει το σωστό ιδιωτικό κλειδί που χρειάζεται για να αφαιρεθεί η εξωτερική κρυπτογράφηση. Το μήνυμα πρέπει να είναι αυθεντικό, επειδή μόνο ο αποστολέας έχει το ιδιωτικό κλειδί που χρειάζεται για να κρυπτογραφήσει έτσι ώστε το δημόσιο κλειδί του αποστολέα να το αποκρυπτογραφεί σωστά.

4.3.2 Πιστοποίηση μηνύματος χωρίς συμβατική κρυπτογράφηση

Σε αυτό το τμήμα, θα εξεταστούν διάφορες προσεγγίσεις για την πιστοποίηση μηνύματος που δε βασίζονται στην κρυπτογράφηση. Σε όλες αυτές τις προσεγγίσεις, παράγεται μία ετικέτα πιστοποίησης και προσαρτάται σε κάθε μήνυμα προς μετάδοση. Το ίδιο το μήνυμα δεν είναι κρυπτογραφημένο και μπορεί να διαβαστεί στον προορισμό ανεξάρτητα από τη συνάρτηση πιστοποίησης στον προορισμό. Επειδή οι προσεγγίσεις που εξετάζονται σε αυτό το μέρος δεν κρυπτογραφούν μήνυμα, δεν παρέχεται εμπιστευτικότητα μηνύματος. Επειδή η συμβατική κρυπτογράφηση θα παρέχει πιστοποίηση και επειδή είναι ευρέως χρησιμοποιούμενη με άμεσα διαθέσιμα προϊόντα, γιατί να μη χρησιμοποιήσουμε απλά μία τέτοια προσέγγιση, η οποία παρέχει τόσο εμπιστευτικότητα όσο και πιστοποίηση; Υπάρχουν τρεις περιστάσεις στις οποίες είναι προτιμητέα η πιστοποίηση μηνύματος χωρίς εμπιστευτικότητα:
Υπάρχει ένας αριθμός από εφαρμογές στις οποίες το ίδιο μήνυμα εκπέμπεται σε έναν αριθμό από προορισμούς (για παράδειγμα, ειδοποίηση στους χρήστες πως το δίκτυο είναι τώρα μη διαθέσιμο ή ένα σήμα συναγερμού σε ένα κέντρο ελέγχου). Είναι φτηνότερο και περισσότερο αξιόπιστο να υπάρχει μόνον ένας προορισμός υπεύθυνος για την αυθεντικότητα παρακολούθησης. Έτσι, το μήνυμα πρέπει να εκπεμφθεί σε μη κωδικοποιημένο κείμενο με ένα συνδεδεμένο μήνυμα ετικέτας πιστοποίησης. Το υπεύθυνο σύστημα εκτελεί την πιστοποίηση. Εάν προκύψει κάποια παραβίαση, προειδοποιούνται τα υπόλοιπα συστήματα προορισμού από ένα γενικό συναγερμό.
Ένα άλλο δυνατό σενάριο είναι μία συναλλαγή στην οποία η μία πλευρά έχει ένα υψηλό φορτίο και δεν μπορεί να αντέξει το χρόνο να αποκρυπτογραφεί όλα τα

εισερχόμενα μηνύματα. Η πιστοποίηση εκτελείται σε μία επιλεκτική βάση, με μηνύματα να επιλέγονται τυχαία για έλεγχο.
Η πιστοποίηση σε ένα πρόγραμμα υπολογιστή σε καθαρό κείμενο είναι μία ενδιαφέρουσα υπηρεσία. Το πρόγραμμα του υπολογιστή μπορεί να εκτελεστεί χωρίς να χρειάζεται να αποκρυπτογραφείται κάθε φορά, το οποίο θα ήταν σπάταλο για πόρους επεξεργασίας. Ωστόσο, εάν επισυναπτόταν ένα μήνυμα ετικέτα πιστοποίησης στο πρόγραμμα, θα μπορούσε να ελεγχθεί οποτεδήποτε απαιτείται διαβεβαίωση της ακεραιότητας του προγράμματος.
Έτσι, υπάρχει χώρος τόσο για την πιστοποίηση όσο και για την κρυπτογράφηση στην ικανοποίηση των απαιτήσεων ασφαλείας.

4.3.2.1 Κώδικας πιστοποίησης μηνύματος

Μία τεχνική πιστοποίησης περιλαμβάνει τη χρήση ενός μυστικού κλειδιού για να παράγει ένα μικρό τμήμα δεδομένων, γνωστό ως κώδικας πιστοποίησης μηνύματος, το οποίο προσαρτάται στο μήνυμα. Αυτή η τεχνική υποθέτει πως οι δύο ι κοινωνούσες ομάδες, έστω Α και Β, διαμοιράζονται ένα κοινό μυστικό κλειδί. Όταν η Α έχει να στείλει ένα μήνυμα στη Β, υπολογίζει τον κώδικα πιστοποίησης μηνύματος ως μία συνάρτηση του μηνύματος και του κλειδιού: $MAC_M = F(K\ M)$. Το μήνυμα συν το κώδικα μεταδίδονται στον προοριζόμενο παραλήπτη. Ο παραλήπτης εκτελεί τον ίδιο υπολογισμό στο ληφθέν μήνυμα, χρησιμοποιώντας το ίδιο μυστικό κλειδί, για να παράγει ένα νέο κώδικα πιστοποίησης μηνύματα ληφθέν κώδικας συγκρίνεται με τον υπολογισμένο κώδικα. Εάν υποτεθεί πως μόνον ο παραλήπτης και ο αποστολέας γνωρίζουν την ταυτότητα του μυστικού κλειδιού και ο ληφθέν κώδικας ταιριάζει με τον υπολογισμένο κώδικα, τότε:

- Ο παραλήπτης διαβεβαιώνεται πως το μήνυμα δεν έχει αλλαχθεί. Εάν ένας επιτιθέμενος αλλάξει το μήνυμα αλλά δεν αλλάξει τον κώδικα, τότε ο υπολογισμός του παραλήπτη για τον κώδικα θα διαφέρει από το ληφθέν κώδικα. Επειδή υποθέτεται πως ο επιτιθέμενος δε γνωρίζει το μυστικό κλειδί, αυτός δε μπορεί να αλλάξει τον κώδικα για να ανταποκρίνεται στις μεταβολές στο μήνυμα.
- Ο παραλήπτης διαβεβαιώνεται πως το μήνυμα είναι από τον ισχυριζόμενο αποστολέα. Επειδή κανένας άλλος δε γνωρίζει το μυστικό κλειδί, κανένας άλλος δε θα μπορούσε να προετοιμάσει ένα μήνυμα με έναν κατάλληλο κώδικα, p. Εάν το μήνυμα περιλαμβάνει έναν αριθμό ακολουθίας (όπως χρησιμοποιείται με το X.25, HDLC και το TCP), τότε ο παραλήπτης μπορεί να βεβαιωθεί για την κατάλληλη ακολουθία, επειδή ένας επιτιθέμενος δε μπορεί να αλλάξει επιτυχώς τον αριθμό ακολουθίας.

Για να παραχθεί ο κώδικας, θα μπορούσε να χρησιμοποιηθεί ένας αριθμός από αλγορίθμους. Το Εθνικό Ινστιτούτο Προτύπων, στην έκδοση του *Τύποι Λειτουργίας DES,* συστήνει τη χρήση του DEA. Ο DEA χρησιμοποιείται για να παράγει μία κρυπτογραφημένη έκδοση του μηνύματος και τα τελευταία bit στο κρυπτογραφημένο κείμενο χρησιμοποιούνται ως κώδικας. Συνηθισμένος είναι ένας 16- ή 32-bit [κώδικας.]
Η διαδικασία που μόλις περιγράφηκε είναι παρόμοια με την κρυπτογράφηση. Μία διαφορά είναι πως ο αλγόριθμος πιστοποίησης δεν είναι απαραίτητο να είναι αντιστρέψιμος, όπως πρέπει να είναι για την αποκρυπτογράφηση. Αποδεικνύεται

χρησιμοποιείται στους εξυπηρετητές πρόσβασης (access servers) και είναι πολύ δημοφιλές στους παρόχους δικτυακών υπηρεσιών και της μεγάλες εταιρίες.
Οι εξυπηρετητές πρόσβασης παρέχουν τη δυνατότητα απομακρυσμένης σύνδεσης στο διαδίκτυο ή το εσωτερικό δίκτυο εταιρίας ή οργανισμού μέσω modem συνήθως. Η καταγραφή στοιχείων σχετικά με τις συνδέσεις των χρηστών και τις δραστηριότητές τους είναι πολύ σημαντική για την
ασφάλεια, τη χρέωση και την ποιότητα των υπηρεσιών που προσφέρει ο πάροχος δικτυακών υπηρεσιών. Επίσης, το RADIUS παρέχει τα δυνατότητα ορισμού συγκεκριμένων ρυθμίσεων ανά χρήστη ενώ η πιστοποίησή τους γίνεται με τη βοήθεια βάσης δεδομένων, γεγονός που βοηθάει σημαντικά σε θέματα διαχείρισης. Κάθε μια από τις τρεις υπηρεσίες του RADIUS μορούν να χρησιμοποιηθούν και ανεξάρτητα.
Στην καταγραφή στοιχείων (accounting), γίνεται καταγραφή των δεδομένων στην αρχή και το τέλος της συνόδου. Τα δεδομένα αυτά αναφέρονται στους πόρους του δικτύου που χρησιμοποιήθηκαν (χρόνος σύνδεσης, πακέτα, bytes, ιστορικό ενεργειών κτλ) Το πρωτόκολλο RADIUS βασίζεται στο μοντέλο πελάτη – εξυπηρετητή.
Ο εξυπηρετητής RADIUS, ο οποίος είτε καταγράφει στατιστικά στοιχεία, είτε υλοποιεί την πιστοποίηση και εξουσιοδότηση του χρήστη, δίνοντας την εντολή στον εξυπηρετητή πρόσβασης δικτύου να αποδεχθεί ή να απορρίψει τη σύνδεση. Επίσης, διατηρεί τη βάση δεδομένων των χρηστών και των ρυθμίσεών τους. Το RADIUS μπορεί να χρησιμοποιηθεί και για τη χρέωση και έλεγχο εφαρμογών VoIP.
Ο έλεγχος του RADIUS, αναπτύχθηκε ως πρόσθετο τμήμα στο πρωτόκολλο επικύρωσης RADIUS.. Κατά συνέπεια, ο έλεγχος του RADIUS μοιράζεται την προσέγγιση της επικύρωσης RADIUS, χωρίς υποστήριξη για επεξεργασία κατά δέσμες ή polling. Σαν αποτέλεσμα αυτού του γεγονότος, οι κλίμακες ελέγχου RADIUS με τον αριθμό γεγονότων ελέγχου αντί του αριθμού συσκευών και οι μεταφορές ελέγχου είναι ανεπαρκής.
Μιας και ο έλεγχος RADIUS είναι βασισμένος σε UDP και timeout-retry οι παράμετροι δεν διευκρινίζονται, και εφαρμογές ποικίλλουν ευρέως στην προσέγγιση της αξιοπιστίας. Μερικές από τις εφαρμογές επαναλαμβάνουν τις προσπάθειες σύνδεσης μέχρι την επίτευξη της παράδοσης ή την εξάντληση των προσωρινών αποθηκευτών (buffers), ενώ άλλες χάνουν στοιχεία ελέγχου μετά από μερικές επαναπροωθήσεις. Μιας και ο έλεγχος RADIUS δεν προβλέπει την ανάγνωση του στρώματος εφαρμογής ή των μηνυμάτων λάθους, μια απάντηση έλεγχου RADIUS είναι ισοδύναμη με μια αναγνώριση στρώματος μεταφοράς και δεν παρέχει καμία προστασία ενάντια στις δυσλειτουργίες του στρώματος εφαρμογής. Λόγω της έλλειψης αξιοπιστίας, δεν είναι δυνατό να γίνει ταυτόχρονος έλεγχος χρήσης βασισμένος στον έλεγχο RADIUS και μόνο. Τυπικά απαιτείται μια άλλη πηγή στοιχείων συσκευών, όπως το polling μιας συνόδου MIB ή μιας συνόδου Telnet.
Οι εφαρμογές ελέγχου RADIUS είναι τρωτές στην απώλεια πακέτων όπως και σε αποτυχίες του στρώματος εφαρμογής, αποτυχίες δικτύων και επανεκκινήσεις συσκευών. Αυτές οι ανεπάρκειες ενισχύονται στον έλεγχο inter-domain όπως απαιτεί η περιαγωγή (roaming). Αφ' ετέρου, η κατά-γεγονός προσέγγιση του ελέγχου RADIUS είναι χρήσιμη όπου απαιτείται καθυστέρηση επεξεργασίας, όπως η διαχείριση πιστωτικού κινδύνου ή η ανίχνευση απάτης.
Ενώ ο έλεγχος RADIUS παρέχει hop-by-hop επικύρωση, προστασία ακεραιότητας, και IPSEC, μπορεί να υιοθετηθεί για να παρέχεί hop-by-hop εμπιστευτικότητα, ενώ η ασφάλεια αντικειμένου στοιχείων δεν υποστηρίζεται, και έτσι τα συστήματα που

βασίζονται σε έλεγχο RADIUS δεν είναι σε θέση να αναπτυχθούν με τα μη-έμπιστα proxies, ή σε καταστάσεις που απαιτούν παρακολούθηση
Ενώ το RADIUS δεν υποστηρίζει τη συμπίεση, η συμπίεση IP, μπορεί να υιοθετηθεί. Ενώ σε γενικές γραμμές υπάρχει η δυνατότητα καθορισμού νέων ιδιοτήτων, το RADIUS πάσχει από περιορισμένο χώρο ιδιοτήτων (256 ιδιότητες).

4.3.4 TACACS+

Ένα άλλο πρωτόκολλο παρόμοιο με το RADIUS είναι το TACACS (Terminal Access Control Access Control System). Έχουν την ίδια λειτουργικότητα και η βασική τους διαφορά είναι στον τρόπο επικοινωνίας του εξυπηρετητή πρόσβασης δικτύου και τον εξυπηρετητή TACACS. Στην περίπτωση του RADIUS χρησιμοποιείται το πρωτόκολλο UDP (connectionless), ενώ το TACACS χρησιμοποιεί το TCP (connection oriented), γεγονός που το καθιστά περισσότερο αξιόπιστο.
(RFC 2975)Το TACACS + προσφέρει ένα πρότυπο ελέγχου με αρχή, stop και ενδιάμεσα μηνύματα αναπροσαρμογής. Δεδομένου ότι το TACACS + είναι βασισμένο στο TCP, οι εφαρμογές είναι ελαστικές ενάντια στην απώλεια πακέτων και τα βραχυχρόνια χωρίσματα δικτύου. Μιας και το TACACS + τρέχει πάνω στο TCP, προσφέρει υποστήριξη τόσο για το στρώμα μεταφορών όσο και για το στρώμα εφαρμογής, και είναι κατάλληλο για ταυτόχρονο έλεγχο χρήσης και χειρισμό των γεγονότων ελέγχου που απαιτούν μέτρια αλλά όχι και τη χαμηλότερη καθυστέρηση επεξεργασίας.
Το TACACS + επιτρέπει την επικύρωση και την ακεραιότητα hop-by-hop καθώς επίσης και την hop-by-hop εμπιστευτικότητα. Η ασφάλεια των στοιχείων αντικείμενου δεν υποστηρίζεται, και επομένως συστήματα βασισμένα στον έλεγχο TACACS + δεν μπορούν να αναπτυχθούν με την παρουσία μη-έμπιστων proxies. Ενώ το TACACS+ δεν υποστηρίζει συμπίεση, η συμπίεση IP, μπορεί να υιοθετηθεί.

4.4 Εμπιστευτικότητα

Ένας οργανισμός έχει στην διάθεσή του πόρους που θα θελήσει να τους προστατεύσει από την κοινοποίηση σε αναρμόδιες οντότητες.
Τα λειτουργικά συστήματα έχουν συχνά ενσωματωμένους μηχανισμούς προστασίας αρχείων που επιτρέπουν σε έναν διαχειριστή να ελέγχει ποιος μπορεί να έχει πρόσβαση στο σύστημα, ή "να δει," το περιεχόμενο ενός δεδομένου αρχείου.
Ένας ισχυρότερος τρόπος να παρασχεθεί η εμπιστευτικότητα είναι μέσω της κρυπτογράφησης..
Οι εξουσιοδοτημένοι παραλήπτες και ο ιδιοκτήτης των πληροφοριών κατέχουν τα αντίστοιχα κλειδιά αποκρυπτογράφησης που τους επιτρέπουν εύκολα να φτιάξουν το κείμενο σε μια αναγνώσιμη μορφή.
Η χρησιμοποίηση κρυπτογράφησης είναι επιθυμητή για την παροχή εμπιστευτικότητας και την προστασία πολύτιμων πληροφοριών.
Η χρήση της κρυπτογράφησης ελέγχεται μερικές φορές από τους κυβερνητικούς κανονισμούς, έτσι πρέπει να ενθαρρύνονται οι διαχειριστές ώστε να είναι ενημερωμένοι για τους νόμους ή τις πολιτικές που ρυθμίζουν τη χρήση της πριν την υιοθέτηση της.

Ενθαρρύνουμε επίσης τους πάντες να διαθέσουν χρόνο για να καταλάβουν την ισχύ της κρυπτογράφησης σε οποιοδήποτε αλγόριθμο/ προϊόν πριν το χρησιμοποιήσουν.

4.4.1 Κρυπτογράφηση και εμπιστευτικότητα

Για να εξασφαλιστεί ότι το περιεχόμενο ενός μηνύματος θα παραμείνει εμπιστευτικό ακόμα και αν γίνει υποκλοπή, το μήνυμα πρέπει να *κρυπτογραφηθεί (encrypted).* Ουσιαστικά, η κρυπτογράφηση αλλοιώνει τα bit του μηνύματος με τέτοιον τρόπο ώστε μόνο ο τελικός αποδέκτης να μπορεί να τα αποκαταστήσει. Κάποιος που υποκλέπτει ένα αντίγραφο του κρυπτογραφημένου μηνύματος δε θα μπορέσει να εξαγάγει τις πληροφορίες.
Υπάρχουν πολλές τεχνολογίες κρυπτογράφησης. Σε μερικές τεχνολογίες, ο αποστολέας και ο παραλήπτης πρέπει να έχουν και οι δύο αντίγραφο ενός *κλειδιού κρυπτογράφησης (encryption key),* το οποίο κρατούν μυστικό. Ο αποστολέας χρησιμοποιεί το κλειδί για να δημιουργήσει ένα κρυπτογραφημένο μήνυμα, το οποίο στη συνέχεια στέλνει μέσω δικτύου. Ο παραλήπτης χρησιμοποιεί το κλειδί για να αποκωδικοποιήσει το κρυπτογραφημένο μήνυμα. Δηλαδή, η συνάρτηση κρυπτογράφησης *encrypt* που χρησιμοποιείται από τον αποστολέα δέχεται δύο ορίσματα: ένα κλειδί, *K,* και ένα μήνυμα για κρυπτογράφηση, Μ. Η συνάρτηση παράγει μια κρυπτογραφημένη έκδοση του μηνύματος, *E.*
E = encrypt(K, M)
Η συνάρτηση αποκρυπτογράφησης *decrypt* αντιστρέφει τη συνάρτηση και δίνει το αρχικό μήνυμα:
M = *decrypt(K, E)*
Από μαθηματική άποψη, η συνάρτηση *decrypt* είναι η αντίστροφη της *encrypt:*
M - decrypt(K, encrypt(K, M))

4.4.1.1 Κρυπτογράφηση δημόσιου κλειδιού

Σε *πολλές* μεθόδους κρυπτογράφησης, το κλειδί πρέπει να διατηρείται μυστικό για να αποφευχθεί η παραβίαση της ασφάλειας. Μια ιδιαίτερα ενδιαφέρουσα τεχνική κρυπτογράφησης είναι να αποδίδονται σε κάθε χρήστη δύο κλειδιά. Το ένα από τα κλειδιά του χρήστη, το λεγόμενο *ιδιωτικό κλειδί (private key),* διατηρείται μυστικό, ενώ το άλλο, το λεγόμενο *δημόσιο κλειδί (public key),* δημοσιοποιείται μαζί με το όνομα του χρήστη, ώστε όλοι να γνωρίζουν την τιμή του. Η συνάρτηση κρυπτογράφησης έχει τη μαθηματική ιδιότητα ότι ένα μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί δεν μπορεί να αποκρυπτογραφηθεί εύκολα παρά μόνο με το ιδιωτικό κλειδί, και ένα μήνυμα κρυπτογραφημένο με το ιδιωτικό κλειδί δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το δημόσιο κλειδί.
Οι σχέσεις μεταξύ της κρυπτογράφησης και της αποκρυπτογράφησης με τα δύο κλειδιά μπορεί να εκφραστεί μαθηματικά. Έστω *M* ένα μήνυμα, *pub-u1* το δημόσιο κλειδί του χρήστη 1, και priv--*u1* το ιδιωτικό κλειδί του χρήστη *1.* Τότε

M = *decrvpt (pub-ul, encrvpt(prv-ul, M))* και

M = decrypt (prv-ul, encrypt(pub-ul, M))

Η αποκάλυψη του δημόσιου κλειδιού είναι ασφαλής επειδή οι συναρτήσεις που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση έχουν την ιδιότητα να είναι *μονόδρομες (one way).* Δηλαδή, αν δοθεί σε κάποιον το δημόσιο κλειδί, αυτό δεν του επιτρέπει να πλαστογραφήσει ένα μήνυμα που να φαίνεται σαν να έχει κρυπτογραφηθεί με το ιδιωτικό κλειδί.
Η κρυπτογράφηση δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί για να εξασφαλίσει την εμπιστευτικότητα. Ένας αποστολέας που θέλει να παραμείνει ένα μήνυμα εμπιστευτικό χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να το κρυπτογραφήσει. Αν κάποιος αποκτήσει ένα αντίγραφο του μηνύματος καθώς περνά από το δίκτυο δε θα μπορέσει να διαβάσει το περιεχόμενο του, επειδή για την αποκρυπτογράφηση απαιτείται το ιδιωτικό κλειδί του παραλήπτη. Επομένως, ο μηχανισμός αυτός εξασφαλίζει ότι τα δεδομένα παραμένουν εμπιστευτικά, επειδή μόνο ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα.

4.5 Ακεραιότητα

Ο διαχειριστής θέλει να είναι σίγουρος για την ακεραιότητα των πληροφοριών του οργανισμού(π.χ., αρχεία λειτουργικών συστημάτων, στοιχεία επιχείρησης, κ.λπ....) που δεν έχουν αλλαχτεί με μια αρμόδια μέθοδο.
Αυτό σημαίνει ότι θα πρέπει να παρέχετε κάποια διαβεβαίωση ως προς την ακεραιότητα των πληροφοριών στο σύστημα .
Ένας τρόπος είναι να παραχθεί ένα checksum του αμετάβλητου αρχείου, να αποθηκευθεί το checksum offline, και περιοδικά (ή όταν επιδιώκεται) να γίνεται έλεγχος για να σιγουρευτεί ότι το checksum του online αρχείου δεν έχει αλλάξει.
Μερικά λειτουργικά συστήματα προσφέρονται με προγράμματα, όπως το πρόγραμμα sum Unix. Εντούτοις, αυτά μπορεί να μην παρέχουν την προστασία που χρειάζεται πραγματικά. Τα αρχεία μπορεί να τροποποιηθούν με τέτοιο τρόπο ώστε να συντηρηθεί το αποτέλεσμα του προγράμματος sum Unix.
Επομένως, πρέπει να χρησιμοποιηθεί ένα κρυπτογραφικά ισχυρό πρόγραμμα, όπως το message digesting program MD5, για να παραχθούν τα checksums που θα χρησιμοποιηθούν για τη βεβαίωση της ακεραιότητας.
Υπάρχουν ακόμα άλλες εφαρμογές όπου η ακεραιότητα θα πρέπει να βεβαιωθεί, όπως κατά τη διαβίβαση ενός μηνύματος ηλεκτρονικού ταχυδρομείου μεταξύ δύο συμβαλλόμενων μερών.
Υπάρχουν προϊόντα διαθέσιμα που μπορούν να παρέχουν αυτή την δυνατότητα.

4.5.1 Μηχανισμοί ακεραιότητας

Έχουν χρησιμοποιηθεί πολλοί μηχανισμοί για να εξασφαλίζεται η ακεραιότητα τω μηνυμάτων από σκόπιμες αλλαγές. Γενικά, αυτές οι μέθοδοι κωδικοποιούν τα μεταδιδόμενα δεδομένα με έναν *κώδικα πιστοποίησης μηνύματος (message authentication code, MAC),* το οποίο δεν μπορεί να σπάσει ή να πλαστογραφήσει ένας εισβολέας. Οι τυπικές μέθοδοι κωδικοποίησης χρησιμοποιούν μηχανισμούς *κρυπτογραφικού κατακερματισμού (cryptographi hashing).* Για παράδειγμα, μια μέθοδος κρυπτογραφικού κατακερματισμού χρησιμοποιεί ένα *απόρρητο κλειδί (secret key)* το οποίο είναι γνωστό μόνο στον αποστολέα και τον παραλήπτη. Όταν ο αποστολέας κωδικοποιεί το μήνυμα, η συνάρτηση κρυπτογραφικού κατακερματισμού

χρησιμοποιεί το απόρρητο κλειδί για να ανακατέψει τη θέση των byte μέσα στο μήνυμα καθώς και να κωδικοποιήσει τα δεδομένα. Μόνο ο παραλήπτης μπορεί να αποκωδικοποιήσει τα δεδομένα. Ένας εισβολέας που δεν έχει το απόρρητο κλειδί δεν μπορεί να αποκωδικοποιήσει το μήνυμα χωρίς να προκαλέσει λάθος. Έτσι, ο παραλήπτης γνωρίζει ότι όποιο μήνυμα μπορεί να αποκωδικοποιηθεί σωστά είναι αυθεντικό

4.6 Εξουσιοδότηση

Η εξουσιοδότηση αναφέρεται στη διαδικασία απόκτησης προνομιών στις υπηρεσίες και, τελικά, στους χρήστες. Αυτό διαφέρει από την επικύρωση δεδομένου. Η επικύρωση είναι η διαδικασία που χρησιμοποιείται για να προσδιοριστεί ένας χρήστης.
Μόλις προσδιοριστούν, τα προνόμια, τα δικαιώματα, η ιδιοκτησία, και οι επιτρεπόμενες ενέργειες του χρήστη στη συνέχεια δίνεται πρόσβαση.
Η απαρίθμηση των εξουσιοδοτημένων δραστηριοτήτων κάθε χρήστη (και διαδικασίες χρηστών) όσον αφορά όλους τους πόρους (αντικείμενα) είναι αδύνατη σε ένα λογικό σύστημα.
Σε ένα πραγματικό σύστημα ορισμένες τεχνικές χρησιμοποιούνται για να απλοποίηση της διαδικασίας έγκρισης. Μια προσέγγιση, που εφαρμόζεται σε συστήματα Unix, είναι να οριστεί κάθε αντικείμενο σε τρεις κατηγορίες χρήστη: ιδιοκτήτης, ομάδα και κοινό.
Ο ιδιοκτήτης είναι ο δημιουργός του αντικειμένου ή ο χρήστης που διορίζεται ως ιδιοκτήτης από τον super-χρήστη. Οι άδειες ιδιοκτητών (που διαβάζονται read, write and execute,) ισχύουν μόνο για τον ιδιοκτήτη. Μια ομάδα είναι ένα σύνολο χρηστών που μοιράζονται τα δικαιώματα πρόσβασης σε ένα αντικείμενο.
Οι άδειες ομάδας (που διαβάζονται, read, write and execute) ισχύουν για όλους τους χρήστες μιας ομάδας (εκτός από τον ιδιοκτήτη).
Το κοινό είναι όλοι οι άλλοι με πρόσβαση στο σύστημα.
Οι παγκόσμιες άδειες (που διαβάζονται, read, write and execute) ισχύουν για όλους τους χρήστες (εκτός από τον ιδιοκτήτη και τα μέλη της ομάδας).

4.6.1 Τεχνολογίες εξουσιοδότησης

Υπάρχουν διάφορες κατηγορίες εξουσιοδότησης. Διάφοροι μηχανισμοί εξουσιοδότησης είναι κατάλληλοι για την εξέταση διάφορων ειδών προβλημάτων εξουσιοδότησης.

4.6.1.1 Καμία εξουσιοδότηση

Το πιο απλό σύστημα εξουσιοδότησης είναι να μην υπάρχει καθόλου εξουσιοδότηση. Ένα μη-δικτυωμένο PC σε μια ιδιωτική (ασφαλή) θέση είναι ένα παράδειγμα όπου δεν χρειάζεται καμία εξουσιοδότηση. Μια άλλη περίπτωση είναι ένας αυτόνομος δημόσιος τερματικός σταθμός, όπως οι "mail reading" τερματικοί σταθμοί που παρέχονται σε μερικές διασκέψεις, στον οποίο τα δεδομένα δεν είναι ευαίσθητα στην κοινοποίηση ή την τροποποίηση.

4.6.1.2 Μηχανισμοί εξουσιοδότησης που είναι ευάλωτοι στις παθητικές επιθέσεις

Ο απλός έλεγχος κωδικού πρόσβασης είναι η πιο κοινή μορφή εξουσιοδότησης. Οι απλοί έλεγχοι εξουσιοδότησης υπάρχουν σε πολλές μορφές: το κλειδί μπορεί να είναι ένας κωδικός πρόσβασης που απομνημονεύεται από το χρήστη, μπορεί να είναι ένα φυσικό ή ηλεκτρονικό στοιχείο που κατέχει ο χρήστης, ή μπορεί να είναι ένα μοναδικό βιολογικό χαρακτηριστικό γνώρισμα.
Τα απλά συστήματα εξουσιοδότησης συνήθως χαρακτηρίζονται ως "αποκαλύψιμα" επειδή εάν το κλειδί διαβιβάζεται μέσω του δικτύου, είναι πιθανό να ανακαλυφθεί από πιθανούς εισβολείς.
Έχουν υπάρξει αναφορές επιτυχών παθητικών επιθέσεων στο Διαδίκτυο χρησιμοποιώντας τα ήδη παραβιασμένα συστήματα για να συμμετέχουν σε παθητική επίθεση ενάντια σε άλλα συστήματα .
Οι αποκαλυπτικοί μηχανισμοί εξουσιοδότησης είναι ευάλωτοι στις επιθέσεις επανάληψης. Τα κλειδιά πρόσβασης μπορούν να αποθηκευτούν στο σύστημα στόχος, οπότε σ' αυτή την περίπτωση ένας εισβολέας που παραβιάζει την ασφάλεια συστημάτων μπορεί να αποκτήσει πρόσβαση σε όλους τους κωδικούς πρόσβασης. Εναλλακτικά, όπως στα περισσότερα συστήματα, τα στοιχεία που αποθηκεύονται στο σύστημα μπορεί να είναι αρκετά ώστε να επιβεβαιώνουν τους κωδικούς πρόσβασης αλλά όχι να τους παράγουν.

4.6.1.3 Ευάλωτοι μηχανισμοί εξουσιοδότησης στις ενεργές επιθέσεις

Τα συστήματα μη-αποκάλυψης του κωδικού πρόσβασης έχουν σχεδιαστεί για να αποτρέπουν επιθέσεις επανάληψης. Έχουν εφευρεθεί διάφορα συστήματα για να παράγουν κωδικούς πρόσβασης μη-αποκάλυψης . Παραδείγματος χάριν, η κάρτα SecurID από την Security Dynamics χρησιμοποιεί συγχρονισμένα ρολόγια για την παροχή πληροφοριών εξουσιοδότησης Η κάρτα παράγει μια οπτική ένδειξη όταν είναι στην κατοχή του προσώπου που επιδιώκει την εξουσιοδότηση.
Το S/Key (TM) σύστημα εξουσιοδότησης που αναπτύχθηκε από την Bellcore, παράγει πολλαπλούς κωδικούς πρόσβασης μιας χρήσεως από ένα ενιαίο μυστικό κλειδί. Δεν χρησιμοποιεί φυσικό token, έτσι είναι επίσης κατάλληλο για μηχανή προς μηχανή εξουσιοδότηση . Επιπλέον υπάρχουν συστήματα απάντησης στα οποία ένα πρόγραμμα συσκευών ή υπολογιστών χρησιμοποιείται για να παράγει μια επαληθεύσιμη απάντηση από μια μη επαναλαμβανόμενη πρόκληση . Η S/Key εξουσιοδότηση δεν απαιτεί αποθήκευση του μυστικού κλειδιού του χρήστη, το οποίο είναι ένα πλεονέκτημα κατά τη εξέταση μη έμπιστων συστημάτων υπολογισμού.
Στη τρέχουσα μορφή του, το σύστημα S/Key είναι ευάλωτο σε μια επίθεση λεξικών σε ένα κωδικό πρόσβασης που είναι κακώς επιλεγμένος. Το Point-to- Point (βασισμένο σε πρωτόκολλο CHAP)challenge-response σύστημα είναι μη αποκαλύψιμο αλλά χρήσιμο τοπικά.
Αυτά τα συστήματα ποικίλλουν ανάλογα με την ευαισθησία των πληροφοριών που αποθηκεύονται στον host(ξενιστή) εξουσιοδότησης, και ποικίλλουν ανάλογα με στις απαιτήσεις ασφάλειας σε εκείνο τον host(ξενιστή).

4.6.1.4 Ανθεκτικοί μηχανισμοί εξουσιοδότησης σε ενεργές επιθέσεις

Η αυξανόμενη χρήση δικτυωμένων υπολογιστικών περιβαλλόντων έχει οδηγήσει στη ανάγκη για ισχυρότερη εξουσιοδότηση. Στα ανοικτά δίκτυα, πολλοί χρήστες μπορούν να αποκτήσουν πρόσβαση σε οποιεσδήποτε πληροφορίες που υπάρχουν μέσα στο δίκτυο, και με πρόσθετη προσπάθεια, ένας χρήστης μπορεί να στείλει πληροφορίες και να τις κάνει να εμφανίζονται από έναν άλλο χρήστη.
Τα περισσότερα συστήματα εξουσιοδότησης χρησιμοποιούν την υπολογιστική δύναμη και των δύο εξουσιοδοτούμενων μερών.
Μερικά συστήματα εξουσιοδότησης χρησιμοποιούν κρυπτογραφικές τεχνικές και καθιερώνουν (ως μέρος της διαδικασίας εξουσιοδότησης) ένα κοινό μυστικό (π.χ., κλειδί συνόδου) το οποίο μπορεί να χρησιμοποιηθεί για τις περαιτέρω ανταλλαγές. Παραδείγματος χάριν, ένας χρήστης, μετά την ολοκλήρωση της διαδικασίας εξουσιοδότησης, μπορεί να χορηγήσει ένα πιστοποιητικό έγκρισης που μπορεί να χρησιμοποιηθεί για να λάβει άλλες υπηρεσίες χωρίς περαιτέρω εξουσιοδότηση. Αυτά τα συστήματα εξουσιοδότησης επίσης παρέχουν εμπιστευτικότητα (που χρησιμοποιεί την κρυπτογράφηση) σε επισφαλή δίκτυα σε περίπτωση ανάγκης.

4.7 Πρόσβαση

4.7.1 Φυσική πρόσβαση

Περιορίζουμε τη φυσική πρόσβαση στους host (ξενιστές), επιτρέποντας την πρόσβαση μόνο σε εκείνους που είναι εξουσιοδοτημένοι να χρησιμοποιούν τους host (ξενιστές). Οι host (ξενιστές) περιλαμβάνουν "εμπιστευμένα" τερματικά (δηλ., τερματικά που επιτρέπουν την πλαστή χρήση όπως οι κονσόλες συστημάτων, τα τερματικά χειριστών και τα τερματικά που αφιερώνονται σε ειδικούς στόχους), τους μεμονωμένους μικροϋπολογιστές και τους τερματικούς σταθμούς, ειδικά εκείνους που συνδέονται με το δίκτυο. Ο χώρος εργασίας πρέπει να ταιριάζει με τους περιορισμούς πρόσβασης διαφορετικά μπορεί να βρεθεί τρόπος να παρακαμφθεί η φυσική ασφάλεια .
Αρχικά πρέπει να κρατηθούν εφεδρικά αντίγραφα των στοιχείων και προγραμμάτων. Εκτός από την κράτηση τους σε καλή κατάσταση για εφεδρικούς λόγους, πρέπει να προστατευθούν και από την κλοπή.
Είναι σημαντικό να κρατηθούν backups σε διαφορετικό χώρο από τα πρωτότυπα, όχι μόνο για περιπτώσεις ζημίας, αλλά και για ασφάλεια ενάντια στις κλοπές.
Οι φορητοί hosts (ξενιστές) αποτελούν ένα ιδιαίτερο κίνδυνο. Πρέπει να υπάρχει σιγουριά ότι δεν θα προκληθεί πρόβλημα εάν ένας από τους φορητούς υπολογιστές του προσωπικού κλαπεί.
Οι οδηγίες για τα είδη των δεδομένων που επιτρέπετε να εγκατασταθούν σε δίσκους φορητών υπολογιστών καθώς επίσης και τα δεδομένα, πρέπει να προστατευθούν (π.χ., κρυπτογράφηση) όταν είναι σε έναν φορητό υπολογιστή.
Άλλα μέρη όπου η φυσική πρόσβαση πρέπει να περιοριστεί είναι τα ντουλάπια καλωδίωσης και σημαντικά στοιχεία δικτύων όπως οι κεντρικοί υπολογιστές αρχείων, οι hosts (ξενιστές) κεντρικών υπολογιστών ονόματος, και οι δρομολογητές.

4.7.2 Walk-up συνδέσεις δικτύων

Με τις "walk-up" συνδέσεις, επισημαίνουμε τα σημεία σύνδεσης δικτύων τα οποία παρέχουν έναν κατάλληλο τρόπο στους χρήστες ώστε να συνδέσουν έναν φορητό host (ξενιστή) με το δίκτυο.
Εξετάζετε αν πρέπει να παρέχετε αυτή η υπηρεσία, λαμβάνοντας υπόψη ότι επιτρέπει σε οποιοδήποτε χρήστη να συνδέσει έναν αναρμόδιο host (ξενιστή) με το δίκτυο. Αυτό αυξάνει τον κίνδυνο επιθέσεων μέσω τεχνικών όπως το spoofing διευθύνσεων IP, το sniffing πακέτων,κ.λ.π. Οι χρήστες και οι διαχειριστές των οργανισμών πρέπει να εκτιμήσουν τους σχετικούς κινδύνους .
Εάν αποφασισθεί η παροχή walk-up συνδέσεων, η υπηρεσία πρέπει να προγραμματισθεί προσεκτικά και να καθοριστεί ακριβώς που θα παράσχετε έτσι ώστε να είναι δυνατή η εξασφάλιση της απαραίτητης φυσικής ασφάλειας πρόσβασης.
Ένας walk-up host (ξενιστής) πρέπει να επικυρωθεί προτού να επιτραπεί στον χρήστη του πρόσβαση στους πόρους του δικτύου. Μια εναλλακτική λύση, είναι να ελεγχθεί η φυσική πρόσβαση.
Παραδείγματος χάριν, εάν η υπηρεσία πρόκειται να χρησιμοποιηθεί από σπουδαστές, μπορεί να παρέχετε walk-up σύνδεση σε sockets στα εργαστήρια σπουδαστών.
Εάν επιτρέπετε walk-up πρόσβαση στους επισκέπτες για να συνδεθούν με τα εγχώρια δίκτυά τους (π.χ., ανάγνωση ηλεκτρονικού ταχυδρομείου, κ.λπ....) πρέπει να χρησιμοποιηθεί ένα χωριστό υποδίκτυο που δεν έχει καμία συνδεσιμότητα με το εσωτερικό δίκτυο.
Οποιοσδήποτε οργανισμός που παρέχει ανεξακρίβωτη πρόσβαση στο δίκτυο πρέπει να παρακολουθείτε.

4.7.3 Άλλες τεχνολογίες δικτύων

Οι εξεταζόμενες εδώ τεχνολογίες περιλαμβάνουν τα X.25, ISDN, SMDS, DDS και Frame Relay. Όλα παρέχονται μέσω των φυσικών συνδέσεων που περνούν από τις τηλεφωνικές ανταλλαγές και που παρέχουν τη δυνατότητα εκτροπής.
Οι crackers ενδιαφέρονται κυρίως για τους τηλεφωνικούς switches καθώς επίσης και για τα δίκτυα δεδομένων.
Στην σύγχρονη τεχνολογία, χρησιμοποιούνται τα μόνιμα εικονικά κυκλώματα ή κλειστές ομάδες χρηστών όποτε αυτό είναι δυνατό.
Οι τεχνολογίες που παρέχουν επικύρωση ή και κρυπτογράφηση (όπως το IPv6) εξελίσσονται γρήγορα. Χρησιμοποιούνται σε συνδέσεις όπου η ασφάλεια είναι σημαντική.

4.7.4 Modems

4.7.4.1 Διαχείριση των γραμμών Modem

Αν και παρέχουν κατάλληλη πρόσβαση στους χρήστες ενός οργανισμού, μπορούν επίσης να παρέχουν μια αποτελεσματική παράκαμψη γύρω από τα firewall. Για αυτόν τον λόγο είναι ουσιαστικό να διατηρηθεί ο κατάλληλος έλεγχος των modem.
Δεν πρέπει να επιτρέπετε στους χρήστες να εγκαταστήσουν μια γραμμή modem χωρίς την κατάλληλη έγκριση. Αυτό συμπεριλαμβάνει τις προσωρινές εγκαταστάσεις (π.χ., που συνδέουν ένα modem με μια ολονύκτια τηλεφωνική γραμμή).
Πρέπει να διατηρείτε ένας κατάλογος όλων των γραμμών modem και να τηρείτε αυτός ο κατάλογος ενημερωμένος. Πρέπει να διεξάγονται συχνοί (ιδανικά αυτοματοποιημένοι) έλεγχοι για αναρμόδια modem.

4.7.4.2 Οι Dial-in χρήστες πρέπει να επικυρώνονται

Πρέπει να ολοκληρωθεί ένας έλεγχος ονόματος χρήστη και του κωδικού πρόσβασης του προτού να μπορεί να έχει πρόσβαση στο δίκτυο. Οι τηλεφωνικές γραμμές μπορούν να παραβιασθούν, και είναι αρκετά εύκολο να αναχαιτιστούν μηνύματα από κινητά τηλέφωνα.
Τα σύγχρονα μεγάλης ταχύτητας, modem χρησιμοποιούν περιπλοκότερες τεχνικές διαμόρφωσης, οι οποίες τα καθιστούν κάπως δυσκολότερο να ελεγχθούν, αλλά είναι γνωστό ότι οι χάκερ ξέρουν πώς να κρυφακούν τις γραμμές. Για αυτόν τον λόγο, πρέπει να χρησιμοποιούνται one-time κωδικοί πρόσβασης .
Είναι χρήσιμο να υπάρξει ένα ενιαίο dial-in σημείο έτσι ώστε όλοι οι χρήστες να επικυρώνονται με τον ίδιο τρόπο.
Οι χρήστες περιστασιακά θα πληκτρολογούν ένα κωδικό πρόσβασης. Θέτουμε μια σύντομη καθυστέρηση - δύο δευτερόλεπτα - μετά από τον πρώτο και το δεύτερο αποτυχημένο login, και τους αναγκάζουμε να αποσυνδεθούν μετά από το τρίτο.
Αυτό επιβραδύνει τις αυτοματοποιημένες επιθέσεις κωδικού πρόσβασης.

4.7.4.3 Ικανότητα επανάκλησης

Μερικοί dial-in κεντρικοί υπολογιστές προσφέρουν call-back παροχές (δηλ., ο χρήστης dials-in επικυρώνεται, κατόπιν το σύστημα αποσυνδέει την κλήση και καλεί ξανά το συγκεκριμένο αριθμό).
Η επανάκληση είναι χρήσιμη εάν κάποιος επρόκειτο να μαντέψει ένα όνομα χρήστη και έναν κωδικό πρόσβασης. Το σύστημα κατόπιν καλεί ξανά τον πραγματικό χρήστη του οποίου ο κωδικός πρόσβασης έχει παραβιαστεί.
Οι τυχαίες κλήσεις από έναν κεντρικό υπολογιστή είναι συνήθως ύποπτες. Αυτό σημαίνει ότι οι χρήστες μπορούν να συνδεθούν μόνο από μια θέση (όπου ο κεντρικός υπολογιστής διαμορφώνεται για να τους συνδέει ξανά),και φυσικά μπορούν να υπάρξουν τηλεφωνικές δαπάνες που συνδέονται με τη θέση επανάκλησης.
Αυτό το χαρακτηριστικό γνώρισμα πρέπει να χρησιμοποιηθεί με προσοχή γιατί μπορεί να παρακαμφθεί εύκολα. Τουλάχιστον, πρέπει να υπάρχει βεβαιότητα ότι η επιστρεφόμενη κλήση δεν γίνεται ποτέ από το ίδιο modem με το εισερχόμενο.

Συνολικά, αν και η επανάκληση μπορεί να βελτιώσει την ασφάλεια του modem, δεν πρέπει να εξαρτάται από αυτήν και μόνο.

4.7.4.4 Όλα τα Logins πρέπει να καταγράφονται

Όλα τα logins, είτε επιτυχή είτε ανεπιτυχή πρέπει να καταγράφονται. Εντούτοις, δεν πρέπει να κρατούνται οι σωστοί κωδικοί πρόσβασης στο αρχείο καταγραφής αλλά πρέπει να καταγράφονται απλά ως επιτυχής προσπάθειες σύνδεσης.
Δεδομένου ότι οι περισσότεροι ''κακοί'' κωδικοί πρόσβασης πληκτρολογούνται λάθος από εξουσιοδοτημένους χρήστες, ποικίλλουν συνήθως μόνο κατά έναν ενιαίο χαρακτήρα από τον πραγματικό κωδικό πρόσβασης.
Επομένως εάν δεν μπορεί να ενημερωθεί ένα τέτοιο αρχείο με ασφάλεια, δεν πρέπει να καταγράφετε καθόλου.
Εάν ο προσδιορισμός καλούσας γραμμής είναι διαθέσιμος, πρέπει να γίνει καταγραφή του καλώντος αριθμού για κάθε προσπάθεια σύνδεσης.
Πρέπει να υπάρχει ευαισθησία στα ζητήματα γύρω από τον προσδιορισμό της καλούσας γραμμής .
Επίσης πρέπει να γνωρίζουμε ότι ο προσδιορισμός της καλούσας γραμμής δεν είναι άξιος εμπιστοσύνης.(δεδομένου ότι οι εισβολείς είναι γνωστό ότι σπάζουν τους τηλεφωνικούς switches και προωθούν τηλεφωνικούς αριθμούς ή κάνουν άλλες αλλαγές)

4.7.4.5 Προσεκτική επιλογή του Opening Banner

Πολλοί οργανισμοί χρησιμοποιούν μια προεπιλογή του συστήματος που περιλαμβάνεται σε ένα μήνυμα αρχείου ημέρας για το opening banner τους.
Δυστυχώς, αυτό περιλαμβάνει συχνά τον τύπο υλικού των host (ξενιστών) ή του λειτουργικού συστήματος του παρόντος host (ξενιστή). Αυτό μπορεί να παρέχει πολύτιμες πληροφορίες σε έναν πιθανό εισβολέα.
Άντ' αυτού, κάθε οργανισμός πρέπει να δημιουργήσει το συγκεκριμένο login banner του, που περιλαμβάνει μόνο τις απαραίτητες πληροφορίες.
Μπορεί να παρέχετε ένα short banner, αλλά δεν πρέπει να προσφέρεται ένα "inviting" όνομα (π.χ., πανεπιστήμιο XYZ, σύστημα αρχείων σπουδαστών).
Άντ' αυτού, μπορεί να δοθεί σε έναν οργανισμό, μια σύντομη προειδοποίηση ότι οι σύνοδοι μπορεί να παρακολουθούνται Πρέπει επίσης να γίνει έλεγχος για πιθανά νομικά ζητήματα σχετικά με το κείμενο που μπαίνει στο banner .
Για τις εφαρμογές υψηλής-ασφάλειας, πρέπει να χρησιμοποιηθεί ένας "blind" κωδικός πρόσβασης (δηλ., δεν πρέπει να δοθεί καμία απάντηση σε μια εισερχόμενη κλήση έως ότου να δακτυλογραφήσει ο χρήστης έναν κωδικό πρόσβασης).Αυτό μιμείται αποτελεσματικά ένα νεκρό modem.

4.7.4.6 Επικύρωση Dial-out

Οι Dial-out χρήστες πρέπει επίσης να επικυρωθούν, δεδομένου ότι ένας οργανισμός θα πρέπει να πληρώνει τις τηλεφωνικές δαπάνες τους.

Δεν πρέπει να επιτρέπετε ποτέ dial-out από μια πλαστή dial-in κλήση, και πρέπει να εξετάζετε εάν θα επιτρέπετε από μια επικυρωμένη.
Ο στόχος είναι να αποτραπούν οι επισκέπτες που χρησιμοποιούν το σύνολο των modem ως τμήμα μιας αλυσίδας logins.
Αυτό μπορεί να είναι δύσκολο να ανιχνευθεί, ιδιαίτερα εάν ένας χάκερ περάσει μέσω διάφορων hosts (ξενιστών) ενός οργανισμού.
Στην χειρότερη περίπτωση, δεν πρέπει να επιτρέπετε στα ίδια τα modem και τις τηλεφωνικές γραμμές να χρησιμοποιούνται και από dial-in και από dial-out.
Αυτό μπορεί να εφαρμοστεί εύκολα εάν τρέχουν χωριστά οι dial-in και dial-out modem pools.

4.7.4.7 Ενδυνάμωση του προγραμματισμού του modem "Bullet-proof"

Πρέπει να υπάρχει βεβαιότητα ότι τα modem δεν μπορούν να επαναπρογραμματιστούν ενώ βρίσκονται σε λειτουργία.
Το modem πρέπει να προγραμματιστεί ώστε να επαναρυθμίζετε στην τυποποιημένη διαμόρφωση στην έναρξη κάθε νέας κλήσης. Διαφορετικά, πρέπει να επαναρυθμίζετε στο τέλος κάθε κλήσης.
Αυτή η προφύλαξη θα παρέχει προστασία από τον τυχαίο επαναπρογραμματισμό των modem.
Η επαναρύθμιση στο τέλος και στην αρχή κάθε κλήσης θα παρέχει ένα ακόμα πιο υψηλό επίπεδο εμπιστοσύνης και ότι ένας νέος επισκέπτης δεν θα κληρονομήσει τη σύνοδο ενός προηγούμενου επισκέπτη.
Το modem πρέπει να ολοκληρώνει τις κλήσεις καθαρά. Όταν ένας χρήστης αποσυνδέεται από έναν κεντρικό υπολογιστή πρόσβασης, πρέπει να γίνεται έλεγχος αν ο κεντρικός υπολογιστής κλείνει την τηλεφωνική γραμμή κατάλληλα.

4.8 Υπηρεσίες καταγραφής και ανάλυσης δικτυακής δραστηριότητας

4.8.1 Εισαγωγή

Στο σημερινό επιχειρησιακό περιβάλλον, όπου υπάρχει μία αυξανόμενη έμφαση στην αποδοτικότητα, τα δίκτυα εμφανίζονται όλο και περισσότερο ως μέσα για τη μείωση του κόστους και την αύξηση των εσόδων και της παραγωγικότητας. Για να επιτευχθεί αυτό, απαιτείται ο έλεγχο και η γνώση για την κυκλοφορίας μέσα στο δίκτυό της επιχείρησης ή του οργανισμού. Οι λύσεις καταγραφής και ανάλυσης δικτυακής δραστηριότητας (network accounting) βοηθούν τους παρόχους δικτυακών υπηρεσιών στο σχεδιασμό, στη παρακολούθηση και στη χρέωση διαφόρων υπηρεσιών, χωρίς συμβιβασμούς στην αφθονία των δυνατοτήτων, στην απόδοση των υπηρεσιών, στην προτεραιότητα των πακέτων, και στη κλιμάκωση των δικτύων τους. Ανάλογα με τις ιδιαιτερότητες των δικτύων, τις απαιτήσεις των πελατών, και το επιχειρησιακό μοντέλο, η μία τεχνολογία μπορεί να είναι καλύτερη από άλλη ή ένας συνδυασμός τεχνολογιών μπορεί να είναι η απάντηση στο σύνθετο αυτό θέμα.
Στα κεφαλαία που ακολουθούν παρουσιάζονται τρόποι και λόγοι χρήσης εφαρμογών network accounting, καθώς και οι πιο διαδεδομένες τεχνολογίες για την υλοποίηση των συστημάτων αυτών.

4.8.2 Παρουσίαση εφαρμογών network accounting

Ανάλογα με το πλαίσιο και τη χρήση, ο όρος "καταγραφή και ανάλυση δικτυακής δραστηριότητας (Network Accounting)" μπορεί να σημαίνει οτιδήποτε από τη χρέωση βάσει της χρήσης του δικτύου μέχρι τον χαρακτηρισμό και κατηγοριοποίηση της κίνησης του δικτύου.
Σε αυτό το κείμενο, ο όρος καταγραφή και ανάλυση δικτυακής δραστηριότητας χρησιμοποιείται με την ευρύτερη έννοιά του, για να περιλάβει τον σχεδιασμό (planning) δικτύων, την διαχείριση της
κίνησης, την παρακολούθηση δικτύων, την παρακολούθηση εφαρμογών, την παρακολούθηση χρηστών, τη χρέωση με βάση την υπηρεσία και τον όγκο κίνησης, τις συμφωνίες μεταξύ ομότιμων οντοτήτων (peering agreements) και την ανάλυση της ασφάλειας δικτύων.

Τεχνολογίες Λύσεις	BGPPolicy Accounting /DSB/	CDR	IP Accounting	NetFlow	RADIUS & TACACS+	RMON	Service Assurance Agent	SNMP
Traffic Characterization			X	X		X		X
Security Analysis				X				
Application specific accounting				X	X	X	X	
Voice over IP		X			X		X	
Usage-based billing	X	X	X	X	X	X		X
Peering and transit	X		X	X				X

Αντιστοίχηση λύσεων με τεχνολογίες Network Accounting
Πίνακας 1

Οι διάφορες λύσεις που παρέχει το network accounting περιγράφονται παρακάτω. Ο ακόλουθος πίνακας παρουσιάζει μία επισκόπηση των μεθόδων network accounting που παρέχουν χρήσιμες πληροφορίες για τους διάφορους σκοπούς της διαχείρισης ενός δικτύου. Ο Πίνακας 1 συνοψίζει τις λύσεις και τις τεχνολογίες που καλύπτονται σε αυτό το κείμενο και μπορεί να χρησιμοποιηθεί ως αρχικό σημείο για την εξερεύνηση των κατάλληλων λύσεων και τεχνολογιών.

4.8.3 Διοικητικοί στόχοι ελέγχου

Η διαχείριση ελέγχου περιλαμβάνει τη συλλογή στοιχείων για την κατανάλωση των πόρων για σκοπούς ανάλυσης ικανότητας και τάσης, καθώς και κατανομής κόστους και έλεγχου. Κάθε ένας από αυτούς τους στόχους έχει διαφορετικές απαιτήσεις.

4.8.3.1 Ανάλυση τάσης και προγραμματισμός δυνατοτήτων

Στην ανάλυση τάσης και τον προγραμματισμό δυνατοτήτων, ο στόχος είναι η πρόβλεψη της μελλοντικής χρήσης. Δεδομένου ότι τέτοιες προβλέψεις είναι εγγενώς ατελής, τυπικά δεν απαιτείται υψηλή αξιοπιστία, και μια μέτρια απώλεια πακέτων μπορεί να γίνει ανεκτή. Όπου είναι δυνατό να χρησιμοποιηθούν στατιστικές τεχνικές δειγματοληψίας ώστε να μειωθούν οι απαιτήσεις συλλογής δεδομένων ,ενώ παρέχεται μια πρόβλεψη με την επιθυμητή στατιστική ακρίβεια, μπορεί να είναι δυνατή η ανοχή υψηλής απώλειας πακέτων εφόσον δεν οδηγεί σε μια μη αποδεκτή στατιστική απόκλιση.
Οι απαιτήσεις ασφάλειας για την ανάλυση τάσης και τον προγραμματισμό δυνατοτήτων εξαρτάται από τις περιστάσεις της συλλογής δεδομένων και την ευαισθησία των στοιχείων. Μπορεί να απαιτούνται πρόσθετες υπηρεσίες ασφάλειας όταν το στοιχείο μεταφέρεται μεταξύ διαχειριστικών περιοχών. Παραδείγματος χάριν, όταν πληροφορίες συλλέγονται και αναλύονται μέσα στον ίδιο οργανισμό διαχείρισης, μπορούν να χρησιμοποιηθούν μηχανισμοί προστασίας ακεραιότητας και επικύρωσης προκειμένου να υπάρξει προστασία ενάντια στη συλλογή αβάσιμων στοιχείων.
Σε inter-domain εφαρμογές πρέπει να υπάρχει εμπιστευτικότητα ώστε να παρέχεται προστασία ενάντια σε τρίτους.

4.8.3.2 Accounting

Με την αύξηση των δαπανών επιχειρηματικής δικτύωσης, αυξάνεται και το ενδιαφέρον για έλεγχο. Ο έλεγχος, ο οποίος είναι η πράξη της επαλήθευσης μιας διαδικασίας, στηρίζεται συνήθως στα στοιχεία καταγραφής.
Οι εργασίες ελέγχου μπορούν να περιλαμβάνουν την επαλήθευση της ακρίβειας ενός τιμολογίου που έχει υποβληθεί από έναν φορέα παροχής υπηρεσιών, την επαλήθευση της συμμόρφωσης στη πολιτική που χρησιμοποιείτε, συμφωνίες επιπέδου υπηρεσιών και οδηγίες ασφάλειας. Για να υπάρχει ένας αξιόπιστος έλεγχος, η διαδικασία συλλογής δεδομένων ελέγχου πρέπει να είναι τουλάχιστον τόσο αξιόπιστη όσο η διαδικασία έλεγχου που χρησιμοποιείται από την οντότητα που ελέγχεται. Ομοίως, οι πολιτικές ασφάλειας έλεγχου πρέπει να είναι τουλάχιστον τόσο αυστηρές όσο εκείνες που χρησιμοποιούνται κατά την προετοιμασία της αρχικής ρύθμισης. Λόγω των οικονομικών και νομικών απαιτήσεων, απαιτούνται συχνά για αυτή την εφαρμογή πρακτικές αρχειακού έλεγχου.
Όπου χρησιμοποιούνται διαδικασίες ελέγχου μπορεί να απαιτούνται υπηρεσίες ασφάλειας για να ελεγχθεί η προσαρμογή στη χρήση των πολιτικών ασφάλειας,. Σε αυτή την περίπτωση τυπικά θα περιληφθεί προστασία επικύρωσης, ακεραιότητας,

εμπιστευτικότητας και ακεραιότητας στοιχείων αντικειμένου. Προκειμένου να επιτρέπετε απάντηση σε υπό εξέλιξη γεγονότα ασφάλειας, χρησιμοποιούνται εφαρμογές έλεγχου οι οποίες λειτουργούν με χαμηλή καθυστέρηση επεξεργασίας.

4.8.4 Τι πρέπει να συλλεχθεί

Τα στοιχεία ελέγχου πρέπει να καταγράφουν οποιαδήποτε προσπάθεια επίτευξης ενός διαφορετικού επιπέδου ασφάλειας από οποιοδήποτε πρόσωπο, επεξεργασία, ή άλλη οντότητα στο δίκτυο.
Αυτό περιλαμβάνει τη σύνδεση και την αποσύνδεση, την παραγωγή ticket (Kerberos, παραδείγματος χάριν), και οποιαδήποτε άλλη αλλαγή της πρόσβασης ή της θέσης.
Είναι ιδιαίτερα σημαντικό να σημειωθεί η "ανώνυμη" ή η πρόσβαση "guest" στους δημόσιους κεντρικούς υπολογιστές.
Τα πραγματικά στοιχεία που πρέπει να συλλεχθούν διαφέρουν για διάφορους οργανισμούς και για διαφορετικούς τύπους αλλαγών πρόσβασης μέσα σε έναν οργανισμό.
Γενικά, οι πληροφορίες που πρέπει να συλλεχθούν περιλαμβάνουν: όνομα χρήστη και host name (όνομα ξενιστή) για τη σύνδεση και την αποσύνδεση, παλιά και νέα δικαιώματα πρόσβασης, μια αλλαγή των δικαιωμάτων πρόσβασης και ένα timestamp.
Φυσικά, υπάρχουν πολύ περισσότερες πληροφορίες που μπορούν να συγκεντρωθούν, ανάλογα με αυτό που παρέχει το σύστημα και πόσο διάστημα είναι διαθέσιμο για αποθήκευση πληροφοριών.
Μια πολύ σημαντική σημείωση είναι ότι δεν πρέπει να συλλέγονται κωδικοί πρόσβασης.
Αυτό δημιουργεί μια μεγάλη πιθανότητα παραβίασης ασφάλειας εάν προσεγγιστούν εσφαλμένα τα αρχεία ελέγχου.
Δεν πρέπει να συλλέγονται ανακριβείς κωδικοί πρόσβασης ακόμα και αν διαφέρουν συχνά από τους έγκυρους κωδικούς πρόσβασης από μόνο έναν χαρακτήρα.

4.8.5 Διαδικασία συλλογής

Η διαδικασία συλλογής πρέπει να ξεκινά από τον host (ξενιστή) ή τον πόρο που προσεγγίζεται. Ανάλογα με τη σημασία των δεδομένων, τα στοιχεία θα μπορούσαν να κρατηθούν τοπικά στον πόρο μέχρι να χρειαστεί να διαβιβαστούν στην αποθήκευση μετά από κάθε γεγονός.
Υπάρχουν βασικά τρεις τρόποι να αποθηκευτούν τα αρχεία ελέγχου: σε ένα read/write αρχείο σε έναν host (ξενιστή), σε μια write-once/read-many συσκευή (π.χ., ένα CD-ROM ή ένα ειδικά διαμορφωμένο tape drive), ή σε μια write-only συσκευή (π.χ., ένας line printer).
Κάθε μέθοδος έχει πλεονεκτήματα και μειονεκτήματα.
Η αναγραφή συστημάτων αρχείων είναι η λιγότερο απαιτητική σε πόρους εκ των τριών μεθόδων και η ευκολότερη στη διαμόρφωση.
Επιτρέπει στιγμιαία πρόσβαση στα αρχεία για ανάλυση, η οποία μπορεί να είναι σημαντική εάν μια επίθεση είναι υπό εξέλιξη. Η αναγραφή συστημάτων αρχείων είναι επίσης η λιγότερη αξιόπιστη μέθοδος.

Εάν ο logging host (ξενιστής) έχει παραβιαστεί, το σύστημα αρχείων είναι συνήθως το πρώτο πράγμα που θα χτυπήσει ένας εισβολέας. Θα μπορούσε εύκολα να καλύψει τα ίχνη της παραβίασης.
Η συλλογή των στοιχείων ελέγχου καταγραφής όσον αφορά τη write-once συσκευή θέλει ελαφρώς περισσότερη προσπάθεια διαμόρφωσης από ένα απλό αρχείο, αλλά έχει το σημαντικό πλεονέκτημα της αυξανόμενης ασφάλειας επειδή ένας εισβολέας δεν μπορεί να αλλάξει τα στοιχεία που δείχνουν ότι μια παραβίαση έχει εμφανιστεί.
Τα μειονεκτήματα αυτής της μεθόδου είναι η ανάγκη να διατηρηθεί ένας ανεφοδιασμός των μέσων απομνημόνευσης και το κόστος εκείνων των μέσων. Επίσης, τα στοιχεία μπορεί να μην είναι άμεσα διαθέσιμα.
Το Line printer logging είναι χρήσιμο στο σύστημα όταν απαιτούνται μόνιμα και άμεσα αρχεία. Ένα σύστημα πραγματικού χρόνου είναι ένα παράδειγμα ,όπου το ακριβές σημείο μιας αποτυχίας ή μιας επίθεσης πρέπει να καταγραφεί. Ένας εκτυπωτής λέιζερ, ή άλλη συσκευή που αποθηκεύει δεδομένα σε buffers (π.χ., ένας print server), μπορεί να χάσει δεδομένα εάν οι buffers περιέχουν τα αναγκαία δεδομένα σε μια κρίσιμη στιγμή.
Το μειονέκτημα των "paper trails" είναι η ανάγκη απασχόλησης του εκτυπωτή και η ανάγκη να ανιχνευθούν τα αρχεία με το χέρι.
Υπάρχει επίσης το ζήτημα αποθήκευσης, ενδεχομένως, του τεράστιου όγκου εγγράφων που μπορεί να παραχθεί.
Για κάθε μια από τις μεθόδους αναγραφών που περιγράφονται, υπάρχει επίσης το ζήτημα της εξασφάλισης της πορείας μεταξύ της συσκευής που παράγει την καταγραφή και της πραγματικής logging συσκευής (δηλ., ο file server, tape/CD-ROM drive, printer).
Εάν εκείνο το μονοπάτι παραβιαστεί, το logging μπορεί να σταματήσει ή να υπάρξει spoofing ή και τα δύο. Σε έναν ιδανικό κόσμο, η logging συσκευή θα ήταν άμεσα συνδεδεμένη από ένα ενιαίο, απλό, point-to-point καλώδιο.
Δεδομένου ότι αυτό είναι συνήθως μη πρακτικό, το μονοπάτι πρέπει να περνάει μέσω του ελάχιστου αριθμού δικτύων και δρομολογητών.
Ακόμα κι όταν τα αρχεία καταγραφής μπορούν να εμποδιστούν, το spoofing μπορεί να αποτραπεί με κρυπτογραφικά checksums.

4.8.6 Φόρτος συλλογής στοιχείων

Η συλλογή των στοιχείων του ελέγχου καταγραφής μπορεί να οδηγήσει σε μια γρήγορη συσσώρευση bytes έτσι ώστε η διαθεσιμότητα αποθήκευσης αυτών των πληροφοριών να πρέπει να εξεταστεί εκ των προτέρων.
Υπάρχουν τρόποι μείωσης του απαραίτητου διαστήματος αποθήκευσης. Ένας τρόπος είναι η συμπίεση των δεδομένων, χρησιμοποιώντας μια από τις πολλές μεθόδους που υπάρχουν. Συχνά, ένα γεγονός εξελίσσεται για κάποια χρονική περίοδο που θα το παρατηρήσει ένας οργανισμός και αρχίζει να το ερευνά.
Σε εκείνο το χρονικό σημείο, είναι πολύ χρήσιμο να υπάρχουν λεπτομερώς διαθέσιμα αρχεία ελέγχου καταγραφής.

4.8.7 Χειρισμός και συντήρηση των στοιχείων ελέγχου

Τα στοιχεία ελέγχου καταγραφής πρέπει να είναι από τα πιο εξασφαλισμένα στοιχεία επί του οργανισμού και στα backups. Εάν ένας εισβολέας επρόκειτο να αποκτήσει

πρόσβαση στα στοιχεία ελέγχου καταγραφής, τα συστήματα τα ίδια, εκτός από τα στοιχεία, θα διέτρεχαν κίνδυνο.
Τα στοιχεία ελέγχου καταγραφής μπορούν επίσης να είναι βασικός κρίκος στην έρευνα, τη σύλληψη, και τη δίωξη του δράστη.
Για αυτόν τον λόγο, είναι ενδεδειγμένο να ζητηθούν οι συμβουλές του νομικού συμβουλίου κατά την απόφαση πώς τα στοιχεία ελέγχου καταγραφής πρέπει να αντιμετωπιστούν.
Αυτό πρέπει να συμβεί προτού να εμφανιστεί ένα γεγονός.

4.8.8 Νομικά ζητήματα

Λόγω του περιεχομένου των στοιχείων ελέγχου καταγραφής, προκύπτουν διάφορα νομικά ζητήματα που θα πρέπει να εξεταστούν από το νομικό συμβούλιο.
Εάν σωθούν τα στοιχεία ελέγχου καταγραφής, πρέπει να είμαστε προετοιμασμένοι για τις συνέπειες που προκύπτουν και από την ύπαρξή τους και από το περιεχόμενό τους.
Μια περίπτωση είναι η μυστικότητα των ατόμων. Σε ορισμένες περιπτώσεις, τα στοιχεία ελέγχου καταγραφής μπορούν να περιέχουν προσωπικές πληροφορίες.
Το ψάξιμο των στοιχείων, ακόμη και για έναν στερεότυπο έλεγχο της ασφάλειας του συστήματος, θα μπορούσε να αντιπροσωπεύσει μια παραβίαση της μυστικότητας.
Ένας δεύτερος τομέας ανησυχίας είναι η ύπαρξη κακόβουλης συμπεριφοράς που προέρχεται από τον ίδιο τον οργανισμό.
Εάν μια οργάνωση κρατά τα στοιχεία ελέγχου καταγραφής, είναι αρμόδια για την εξέταση τους ;
Εάν ένας host (ξενιστής) σε μια οργάνωση χρησιμοποιείται ως σημείο προώθησης για μια επίθεση ενάντια σε μια άλλη οργάνωση, μπορεί η δεύτερη οργάνωση να χρησιμοποιήσει τα στοιχεία ελέγχου καταγραφής της πρώτης οργάνωσης για να αποδείξει την αμέλεια εκ μέρους εκείνης της οργάνωσης;
Τα παραπάνω παραδείγματα είναι περιεκτικά, αλλά πρέπει να ωθήσουν την οργάνωσή στην εξέταση των νομικών ζητημάτων που αφορούν τα στοιχεία ελέγχου καταγραφής.

4.8.9 Εκτιμήσεις ασφάλειας και Tunneling

Αυτή η ενότητα εξετάζει τα ζητήματα ασφάλειας που προκύπτουν από την εισαγωγή διαφοροποιημένων υπηρεσιών, πρώτιστα της άρνηση υπηρεσιών, και δεύτερον της σχετικής δυνατότητας για κλοπή της υπηρεσίας από αναρμόδια κυκλοφορία.
Επιπλέον, συζητείται η λειτουργία διαφοροποιημένων υπηρεσιών, η παρουσία του IPsec επίσης καθώς επίσης και οι απαιτήσεις ελέγχου. Αυτή η ενότητα εξετάζει τα ζητήματα που παρουσιάζονται κατά τη χρήση και των IPsec και των μη -IPsec tunnels.

4.8.9.1 Κλοπή και άρνηση υπηρεσίας

Ο αρχικός στόχος των διαφοροποιημένων υπηρεσιών είναι να επιτρέπονται διάφορα επίπεδα υπηρεσίας για traffic streams σε μια κοινή υποδομή δικτύων. Για να γίνει αυτό, χρησιμοποιούνται ποικίλες τεχνικές διαχείρισης των πόρων, αλλά το τελικό αποτέλεσμα είναι μερικά πακέτα να λαμβάνουν διαφορετική (π.χ., καλύτερη) υπηρεσία από άλλα.
Η χαρτογράφηση της κυκλοφορίας δικτύων σύμφωνα με τις συγκεκριμένες συμπεριφορές που οδηγούν σε διαφορετική (π.χ., καλύτερη ή χειρότερη) υπηρεσία φαίνεται πρώτιστα από τον τομέα DS, και ως εκ τούτου ένας αντίπαλος μπορεί να είναι σε θέση να λάβει καλύτερη υπηρεσία με την τροποποίηση του τομέα DS.
Φτάνοντας στα όριά της, αυτή η κλοπή υπηρεσίας γίνεται μια επίθεση άρνησης υπηρεσιών όταν η τροποποιημένη κυκλοφορία μειώνει τους διαθέσιμους πόρους για να τους διαβιβάσει και σε άλλα ρεύματα κυκλοφορίας.
Η άμυνα ενάντια σε μια τέτοια κλοπή - επίθεση υπηρεσιών είναι ο συνδυασμός βελτίωσης κυκλοφορίας στους κόμβους ορίου DS μαζί με την ασφάλεια και την ακεραιότητα του δικτύου μέσα σε έναν οργανισμό DS.
Οι κόμβοι εισόδου DS πρέπει να ρυθμίσουν όλη την κυκλοφορία που εισάγεται σε έναν οργανισμό DS για να εξασφαλιστεί ότι έχει αποδεκτά DS codepoints. Αυτό σημαίνει ότι τα codepoints πρέπει να προσαρμοστούν στα εφαρμόσιμα TCA(s) και στη πολιτική των υπηρεσιών του οργανισμού. Ως εκ τούτου, οι εισαγωγικοί κόμβοι είναι η αρχική γραμμή άμυνας ενάντια στην κλοπή - άρνηση υπηρεσιών η οποία στηρίζεται στα τροποποιημένα DS codepoints (π.χ., codepoints στα οποία η κυκλοφορία δεν έχει δικαίωμα).Μια επιτυχημένη επίθεση είναι η παραβίαση του εφαρμόσιμου TCA(s) ή και της πολιτικής παροχής υπηρεσιών .
Μια σημαντική περίπτωση ενός κόμβου εισόδου είναι ότι οποιαδήποτε μετάδοση, δημιουργημένη από κόμβο σε έναν οργανισμό DS ,είναι ο κόμβος εισόδου για εκείνη την κυκλοφορία, και πρέπει να εξασφαλιστεί ότι όλες οι μεταδόσεις φέρουν αποδεκτά DS codepoints.
Και η πολιτική παροχής υπηρεσιών ενός οργανισμού και τα TCAs μπορούν να απαιτήσουν, από τους κόμβους εισόδου να αλλάξουν τα DS codepoint σε μερικά εισαγμένα πακέτα (π.χ., ένας δρομολογητής εισόδου μπορεί να θέσει το DS codepoint της κυκλοφορίας ενός πελάτη σύμφωνα με το κατάλληλο SLA). Οι κόμβοι εισόδου πρέπει να ρυθμίζουν όλη την εισερχόμενη κυκλοφορία για να εξασφαλίσουν ότι τα DS codepoints είναι αποδεκτά. Τα πακέτα που έχουν μη αποδεκτά codepoints πρέπει είτε να απορρίπτονται είτε πρέπει τα DS codepoints τους να έχουν αποδεκτές τιμές πριν διαβιβαστούν. Παραδείγματος χάριν, ένας κόμβος εισόδου που λαμβάνει κυκλοφορία από έναν οργανισμό με τον οποίο δεν υπάρχει συμφωνία υπηρεσίας, μπορεί να επαναριθμήσει τα DS codepoint στην προεπιλογή PHB codepoint.
Η επικύρωση κυκλοφορίας μπορεί να απαιτεί επικύρωση χρήσης κάποιου DS codepoint (π.χ., εκείνα που αντιστοιχούν σε ενισχυμένες υπηρεσίες), και τέτοια επικύρωση μπορεί να εκτελεσθεί με τεχνικά μέσα (π.χ., IPsec) ή και με μη τεχνικά μέσα.
Μια inter-domain συμφωνία μπορεί να μειώσει ή να εξαλείψει την ανάγκη για βελτίωση κυκλοφορίας κόμβων εισόδου με την δημιουργία ενός upstream οργανισμού η οποία θα είναι εν μέρει ή ολοκληρωτικά υπεύθυνη για την εξασφάλιση ότι η κυκλοφορία έχει αποδεκτά DS codepoints στον downstream οργανισμό. Σε αυτήν την περίπτωση, ο κόμβος εισόδου μπορεί ακόμα να εκτελέσει περιττούς

ελέγχους κυκλοφορίας για να μειώσει την εξάρτηση στον upstream οργανισμό (π.χ., τέτοιοι έλεγχοι μπορούν να αποτρέψουν τη διάδοση επιθέσεων – κλοπών υπηρεσιών πέρα από το όριο των οργανισμών).
Εάν ένας τέτοιος έλεγχος αποτυγχάνει επειδή ο upstream οργανισμός δεν εκπληρώνει τις ευθύνες του, η αποτυχία αυτή είναι ένα γεγονός που μπορεί να παρατηρηθεί και η παραγόμενη καταγραφή ελέγχου πρέπει να περιλαμβάνει την ημερομηνία-χρόνο, το πακέτο που παραλήφθηκε, τις διευθύνσεις πηγής και προορισμού IP και τα DS codepoint που προκάλεσαν την αποτυχία.
Πρακτικά τα περιορισμένα κέρδη από τέτοιους ελέγχους πρέπει να συγκριθούν με τον πιθανό αντίκτυπο που μπορεί να υπάρχει στην ταχύτητα ώστε να διαπιστωθεί αν και ποιοι έλεγχοι πρέπει να γίνουν υπό αυτές τις συνθήκες.
Οι εσωτερικοί κόμβοι σε έναν οργανισμό DS μπορούν να στηριχθούν στον τομέα DS έτσι ώστε να παρέχουν διαφοροποιημένες υπηρεσίες κυκλοφορίας με συμπεριφορές που χρησιμοποιούνται για να εφαρμόσουν ενισχυμένες υπηρεσίες. Οποιοσδήποτε κόμβος που ενεργεί με αυτό τον τρόπο, εξαρτάται από τη σωστή λειτουργία του οργανισμού DS για να αποτρέψει την άφιξη κυκλοφορίας με μη αποδεκτά DS codepoints.
Οι εύλογες ανησυχίες υπαγορεύουν ότι η άφιξη πακέτων με μη αποδεκτά DS codepoints δεν πρέπει να προκαλέσουν αποτυχία (π.χ., συντριβή) των κόμβων δικτύων.
Οι εσωτερικοί κόμβοι δεν είναι αρμόδιοι για την επιβολή της παρεχόμενης πολιτικής υπηρεσιών (ή μεμονωμένα SLAs) και ως εκ τούτου δεν απαιτείται να ελέγχουν DS codepoints πριν να τα χρησιμοποιήσουν. Οι εσωτερικοί κόμβοι μπορούν να εκτελέσουν κάποιους ελέγχους κυκλοφορίας στα DS codepoints (π.χ., έλεγχος για DS codepoints που δεν χρησιμοποιήθηκαν ποτέ για κυκλοφορία σε μια συγκεκριμένη σύνδεση) για να βελτιωθεί η ασφάλεια (π.χ., αντίσταση στις επιθέσεις - κλοπές υπηρεσιών με βάση τα τροποποιημένα DS codepoint).
Οποιαδήποτε ανιχνευμένη αποτυχία ενός τέτοιου έλεγχου είναι ένα γεγονός άξιο καταγραφής και αυτή η καταγραφή πρέπει να περιλαμβάνει το χρόνο παραλαβής του πακέτου, τη πηγή και τις διευθύνσεις προορισμού IP και το DS codepoint που προκάλεσε την αποτυχία.
Πρακτικά τα περιορισμένα κέρδη από τέτοιους ελέγχους πρέπει να συγκριθούν με τον πιθανό αντίκτυπο που μπορεί να υπάρχει στην ταχύτητα ώστε να διαπιστωθεί αν και ποιοι έλεγχοι πρέπει να γίνουν υπό αυτές τις συνθήκες σε εσωτερικούς κόμβους.
Οποιαδήποτε σύνδεση που δεν μπορεί να εξασφαλιστεί επαρκώς ενάντια στην τροποποίηση των DS codepoints ή την εισαγωγή κυκλοφορίας από τους αντιπάλους πρέπει να αντιμετωπιστεί ως μια οριακή σύνδεση
Η τοπική πολιτική ασφάλειας παρέχει τον ορισμό "επαρκώς εξασφαλισμένος," και ένας τέτοιος ορισμός μπορεί να περιλαμβάνει έναν προσδιορισμό ότι οι κίνδυνοι και οι συνέπειες των τροποποιημένων DS codepoint δεν δικαιολογούν οποιαδήποτε πρόσθετα μέτρα ασφάλειας για μια σύνδεση.
Η ασφάλεια σύνδεσης μπορεί να ενισχυθεί μέσω των φυσικών ελέγχων ή ελέγχων λογισμικού όπως τα tunnels που εξασφαλίζουν ακεραιότητα πακέτων.

4.8.9.2 Εφαρμογές του IPSec

Το IPSec παρέχει τη δυνατότητα να ασφαλίζει τις επικοινωνίες κατά μήκος ενός τοπικού δικτύου, κατά μήκος ιδιωτικών και δημόσιων δικτύων ευρείας περιοχής και

κατά μήκος του Διαδικτύου. Παραδείγματα της χρήσης του περιλαμβάνουν τα ακόλουθα:

• **Ασφάλιση συνδεσιμότητας υποκαταστημάτων πάνω στο Διαδίκτυο:** Μία εταιρεία μπορεί να οικοδομήσει ένα ασφαλές νοητό ιδιωτικό δίκτυο πάνω από το Διαδίκτυο ή πάνω από κάποιο δημόσιο δίκτυο ευρείας περιοχής. Αυτό επιτρέπει σε μία επιχείρηση να βασίζεται ισχυρά στο Διαδίκτυο μειώνοντας την ανάγκη της για ιδιωτικά δίκτυα, γλιτώνοντας κόστος και επιβάρυνση διαχείρισης δικτύου.
• **Ασφαλή απομακρυσμένη πρόσβαση πάνω στο Διαδίκτυο:** Ένας τερματικός χρήστης του οποίου το σύστημα είναι εφοδιασμένο με πρωτόκολλα ασφαλείας IP μπορεί να κάνει μία τοπική κλήση σε έναν παροχέα υπηρεσίας Διαδικτύου (ISP) και να επιτύχει ασφαλή πρόσβαση σε ένα εταιρικό δίκτυο. Αυτό μειώνει το κόστος των χρεώσεων διοδίων για τους ταξιδεύοντες εργαζόμενους.
• **Αποκατάσταση εξωδικτυακής και ενδοδικτυακής συνδεσιμότητας με συνεταίρους:** Το IPSec μπορεί να χρησιμοποιηθεί για να ασφαλίσει την επικοινωνία με άλλους οργανισμούς, εξασφαλίζοντας πιστοποίηση και εμπιστευτικότητα και παρέχοντας ένα μηχανισμό ανταλλαγής κλειδιού.
• **Εμπλουτισμός ασφάλειας ηλεκτρονικού εμπορίου:** Έστω και εάν κάποιες εφαρμογές του διαδικτύου και ηλεκτρονικού εμπορίου έχουν ενσωματωμένα πρωτόκολλα ασφαλείας, η χρήση του IPSec εμπλουτίζει αυτήν την ασφάλεια.

Το βασικό χαρακτηριστικό του IPSec που του επιτρέπει να υποστηρίζει αυτές τις ποικίλες εφαρμογές είναι ότι μπορεί να κρυπτογραφήσει και/ή να πιστοποιήσει *όλη* την κίνηση στο επίπεδο IP. Έτσι, μπορούν να ασφαλιστούν όλες οι κατανεμημένες εφαρμογές, συμπεριλαμβάνοντας το απομακρυσμένο logon, εφαρμογές client/ server, ηλεκτρονικό ταχυδρομείο, μεταφορά αρχείων, πρόσβαση στο διαδίκτυο και ούτω καθεξής.

4.8.9.3 Ο Σκοπός του IPSec

Το IPSec παρέχει τρεις κύριες ευκολίες: μία λειτουργία μόνο πιστοποίησης αναφερόμενη ως Επικεφαλίδα Πιστοποίησης (AH), μία συνδυασμένη λειτουργία πιστοποίησης-κρυπτογράφησης ονομαζόμενη Ενθυλακωμένο Φορτίο Ασφαλείας (ESP) και μία λειτουργία ανταλλαγής κλειδιού. Για τα νοητά ιδιωτικά δίκτυα, είναι συνήθως επιθυμητή τόσο η πιστοποίηση όσο και η κρυπτογράφηση, επειδή είναι σημαντικό και (1) να εξασφαλίζεται πως μη εξουσιοδοτημένοι χρήστες δε διαπερνούν το νοητό ιδιωτικό δίκτυο και (2) να εξασφαλίζεται πως αυτοί που κρυφακούν στο Διαδίκτυο δε μπορούν να διαβάσουν μηνύματα που αποστέλλονται πάνω στο νοητό ιδιωτικό διαδίκτυο. Επειδή και τα δύο χαρακτηριστικά είναι συνήθως επιθυμητά, οι περισσότερες υλοποιήσεις είναι πολύ πιθανό να χρησιμοποιούν το ESP παρά το AH. Η λειτουργία ανταλλαγής κλειδιού επιτρέπει τη χειροκίνητη ανταλλαγή κλειδιών όπως επίσης και ένα αυτοματοποιημένο σχήμα.

Η προδιαγραφή του IPsec είναι ιδιαίτερα πολύπλοκη και καλύπτει πολυάριθμα έγγραφα. Τα περισσότερο σημαντικά από αυτά, που εκδόθηκαν το Νοέμβριο του 1998, είναι οι RFCs 2401, 2402, 2406 και 2408. Σε αυτό το μέρος, παρέχεται μία περίληψη των περισσότερο σημαντικών στοιχείων του IPSec.

4.8.9.4 Αλληλεπιδράσεις IPsec και Tunneling

Το πρωτόκολλο IPsec, δεν περιλαμβάνει το DS πεδίο της επικεφαλίδας IP σε οποιοδήποτε από τους κρυπτογραφικούς υπολογισμούς του
Ως εκ τούτου η τροποποίηση του τομέα DS από έναν κόμβο δικτύων δεν έχει καμία επίδραση στην end-to-end ασφάλεια IPsec's, επειδή δεν μπορεί να προκαλέσει αποτυχία σε οποιονδήποτε IPsec έλεγχο ακεραιότητας.. Κατά συνέπεια, το IPsec δεν παρέχει άμυνα ενάντια στην τροποποίηση ενός αντιπάλου DS τομέα (δηλ., μια man-in-the-middle επίθεση) μιας και η αντίπαλη τροποποίηση δεν θα έχει επίσης καμία επίδραση στη end-to-end ασφάλεια IPsec's.
Σε μερικά περιβάλλοντα, η δυνατότητα να τροποποιηθεί ο τομέας DS χωρίς να επηρεάσει την ακεραιότητα των IPsec ελέγχων μπορεί να αποτελέσει ένα μυστικό κανάλι. Εάν είναι απαραίτητο να αποβληθεί ένα τέτοιο κανάλι ή να μειωθεί το εύρος ζώνης του, οι οργανισμοί DS πρέπει να διαμορφωθούν έτσι ώστε η απαραίτητη επεξεργασία να μπορεί να εκτελεστεί στους κόμβους εξόδου DS όπου η κυκλοφορία βγαίνει από τις περιοχές υψηλής ασφάλειας.
Η μέθοδος tunnel του IPsec παρέχει ασφάλεια για την ενθυλακωμένη επικεφαλίδα IP του πεδίου DS. Ένα πακέτο μεθόδου tunnel IPsec περιέχει δύο επικεφαλίδες IP : μια εξωτερική επικεφαλίδα που παρέχεται από τον κόμβο εισόδου tunnel και μια ενθυλακωμένη εσωτερική επικεφαλίδα που παρέχεται από το αρχικό πακέτο.
Όταν ένα IPsec tunnel φιλοξενείται (γενικά ή εν μέρει) σε ένα διαφοροποιημένο δίκτυο υπηρεσιών, οι ενδιάμεσοι κόμβοι δικτύων λειτουργούν στην εξωτερική επικεφαλίδα του πεδίο DS.
Στον tunnel κόμβο εξόδου, η επεξεργασία IPsec περιλαμβάνει το stripping της εξωτερικής επικεφαλίδας και την αποστολή του πακέτου (αν είναι απαραίτητο) που χρησιμοποιεί την εσωτερική επικεφαλίδα. Εάν η εσωτερική επικεφαλίδα IP δεν έχει υποβληθεί σε επεξεργασία από έναν κόμβο εισόδου DS, ο tunnel κόμβος εξόδου είναι ο DS κόμβος εισόδου για την εξερχόμενη κυκλοφορία, και ως εκ τούτου πρέπει να πραγματοποιήσει τις αντίστοιχες ρυθμίσεις κυκλοφορίας.
Εάν η επεξεργασία IPsec περιλαμβάνει έναν αρκετά ισχυρό κρυπτογραφικό έλεγχο ακεραιότητας του ενθυλακωμένου πακέτου, ο tunnel κόμβος εξόδου μπορεί ακίνδυνα να υποθέσει ότι το DS πεδίο στην εσωτερική επικεφαλίδα έχει την ίδια αξία όπως είχε στον tunnel κόμβο εισόδου. Αυτό το γεγονός επιτρέπει σε ένα tunnel κόμβο εξόδου στον ίδιο οργανισμό DS με τον tunnel κόμβο εισόδου, να μεταχειριστεί ακίνδυνα ένα πακέτο που περνά έναν τέτοιο έλεγχο ακεραιότητας. Μια σημαντική συνέπεια είναι ότι έτσι και αλλιώς εσωτερικές επισφαλείς συνδέσεις σε έναν οργανισμό DS μπορεί να εξασφαλιστούν από ένα αρκετά ισχυρό IPsec tunnel.
Αυτή η ανάλυση και οι επιπτώσεις της ισχύουν για οποιοδήποτε tunneling πρωτόκολλο που εκτελεί ελέγχους ακεραιότητας, αλλά το επίπεδο διαβεβαίωσης του τομέα DS της εσωτερικής επικεφαλίδας εξαρτάται με βάση την ακεραιότητα έλεγχου που εκτελείται από το tunneling πρωτόκολλο. Με την απουσία ικανοποιητικής διαβεβαίωσης για την διέλευση ενός tunnel από τους κόμβους έξω από έναν οργανισμό DS, το ενθυλακωμένο πακέτο πρέπει να αντιμετωπιστεί σαν να είχε φθάσει σε έναν κόμβο εισόδου DS έξω από τον οργανισμό.
Το πρωτόκολλο IPsec απαιτεί από το πεδίο DS της εσωτερικής επικεφαλίδας να μην αλλαχτεί από την επεξεργασία ενθυλάκωσης IPsec σε ένα tunnel κόμβο εξόδου. Αυτό εξασφαλίζει ότι τροποποιήσεις ενός αντιπάλου στο πεδίο DS δεν μπορούν να χρησιμοποιηθούν για να προωθηθεί η κλοπή ή η άρνηση υπηρεσιών πέρα από το σημείο τέλους του IPsec tunnel.

Εάν οι προδιαγραφές IPsec τροποποιηθούν στο μέλλον για να επιτρέψουν σε ένα tunnel κόμβο εξόδου να τροποποιήσει το πεδίο DS σε μια εσωτερική επικεφαλίδα IP, τότε πρέπει να ενσωματωθούν πρόσθετες διορθώσεις. Για ένα tunnel που περιλαμβάνεται εξ ολοκλήρου μέσα σε έναν ενιαίο οργανισμό DS και για το οποίο οι συνδέσεις εξασφαλίζονται επαρκώς ενάντια στις τροποποιήσεις του εξωτερικού DS τομέα, τα μόνα όρια στις εσωτερικές DS τροποποιήσεις τομέων θα ήταν εκείνα που επιβάλλονται από την υπηρεσία του οργανισμού.
Διαφορετικά, ο tunnel κόμβος εξόδου που εκτελεί τέτοιες τροποποιήσεις θα ενεργούσε ως κόμβος εισόδου DS για την κυκλοφορία εξόδου του tunnel και θα πραγματοποιούσε όρους βελτίωσης κυκλοφορίας ενός κόμβου εισόδου, συμπεριλαμβανομένης της άμυνας ενάντια στην κλοπή - άρνηση υπηρεσιών.
Ένα IPsec tunnel μπορεί να αντιμετωπισθεί με τουλάχιστον δύο διαφορετικούς τρόπους από αρχιτεκτονική άποψης. Εάν το tunnel αντιμετωπίζεται ως λογικό ενιαίο "εικονικό καλώδιο", οι ενέργειες των ενδιάμεσων κόμβων στην αποστολή tunneled κυκλοφορίας δεν πρέπει να είναι ορατές πέρα από τις άκρες του tunnel και ως εκ τούτου το πεδίο DS δεν πρέπει να τροποποιηθεί ως μέρος της ενθυλακωμένης επεξεργασίας.
Αντίθετα, εάν το tunnel αντιμετωπίζεται ως multi-hop μέρος στην αποστολή της κυκλοφορίας, τότε η τροποποίηση του πεδίου DS ως τμήμα της tunnel ενθυλακωμένης επεξεργασίας μπορεί να είναι επιθυμητή.

4.8.9.5 Καταγραφή

Η καταγραφή δεν υποστηρίζεται από όλα τα συστήματα που παρέχουν διαφοροποιημένες υπηρεσίες. Εντούτοις, εάν η υποστήριξη των διαφοροποιημένων υπηρεσιών είναι ενσωματωμένη σε ένα σύστημα που υποστηρίζει την καταγραφή, τότε η υλοποίηση των διαφοροποιημένων εφαρμογών υπηρεσιών πρέπει επίσης να υποστηρίζει την καταγραφή. Εάν υπάρχει τέτοια υποστήριξη, η εφαρμογή πρέπει να επιτρέπει στον διαχειριστή του συστήματος να ενεργοποιήσει ή να θέσει εκτός λειτουργίας την καταγραφή για διαφοροποιημένες υπηρεσίες, και μπορεί να επιτρέπει στην καταγραφή να ενεργοποιηθεί ή να είναι εν μέρει εκτός λειτουργίας.
Ως επί το πλείστον, η καταγραφή είναι ένα τοπικό θέμα. Εντούτοις, διάφορα ελέγξιμα γεγονότα προσδιορίζονται στην παρούσα εργασία και για κάθε ένα από αυτά τα γεγονότα ένα ελάχιστο σύνολο πληροφοριών πρέπει να συμπεριλαμβάνεται στα αρχεία καταγραφής. Μπορεί επίσης να περιλαμβάνονται πρόσθετες πληροφορίες (π.χ., τα πακέτα που σχετίζονται με αυτό που προκάλεσε το ελέγξιμο γεγονός) στο αρχείο καταγραφής για κάθε ένα από αυτά τα γεγονότα. Επίσης μπορεί να οδηγήσουν σε καταχωρήσεις αρχείων καταγραφής.

4.8.10 Πρωτόκολλα Ελέγχου (accounting protocols)

Συστήματα ελέγχου έχουν εφαρμοστεί επιτυχώς χρησιμοποιώντας πρωτόκολλα όπως τα RADIUS, TACACS+, και το SNMP. Αυτό το τμήμα περιγράφει χαρακτηριστικά κάθε ένα από αυτά τα πρωτόκολλα.

4.8.10.1 RADIUS

Ο έλεγχος του RADIUS, αναπτύχθηκε ως πρόσθετο τμήμα στο πρωτόκολλο επικύρωσης RADIUS.. Κατά συνέπεια, ο έλεγχος του RADIUS μοιράζεται την προσέγγιση της επικύρωσης RADIUS, χωρίς υποστήριξη για επεξεργασία κατά δέσμες ή polling. Σαν αποτέλεσμα αυτού του γεγονότος, οι κλίμακες ελέγχου RADIUS με τον αριθμό γεγονότων ελέγχου αντί του αριθμού συσκευών και οι μεταφορές ελέγχου είναι ανεπαρκής.
Μιας και ο έλεγχος RADIUS είναι βασισμένος σε UDP και timeout-retry οι παράμετροι δεν διευκρινίζονται, και εφαρμογές ποικίλλουν ευρέως στην προσέγγιση της αξιοπιστίας. Μερικές από τις εφαρμογές επαναλαμβάνουν τις προσπάθειες σύνδεσης μέχρι την επίτευξη της παράδοσης ή την εξάντληση των προσωρινών αποθηκευτών (buffers), ενώ άλλες χάνουν στοιχεία ελέγχου μετά από μερικές επαναπροωθήσεις. Μιας και ο έλεγχος RADIUS δεν προβλέπει την ανάγνωση του στρώματος εφαρμογής ή των μηνυμάτων λάθους, μια απάντηση έλεγχου RADIUS είναι ισοδύναμη με μια αναγνώριση στρώματος μεταφοράς και δεν παρέχει καμία προστασία ενάντια στις δυσλειτουργίες του στρώματος εφαρμογής. Λόγω της έλλειψης αξιοπιστίας, δεν είναι δυνατό να γίνει ταυτόχρονος έλεγχος χρήσης βασισμένος στον έλεγχο RADIUS και μόνο. Τυπικά απαιτείται μια άλλη πηγή στοιχείων συσκευών, όπως το polling μιας συνόδου MIB ή μιας συνόδου Telnet.
Οι εφαρμογές ελέγχου RADIUS είναι τρωτές στην απώλεια πακέτων όπως και σε αποτυχίες του στρώματος εφαρμογής, αποτυχίες δικτύων και επανεκκινήσεις συσκευών. Αυτές οι ανεπάρκειες ενισχύονται στον έλεγχο inter-domain όπως απαιτεί η περιήγηση(roaming). Αφ' ετέρου, η κατά-γεγονός προσέγγιση του ελέγχου RADIUS είναι χρήσιμη όπου απαιτείται καθυστέρηση επεξεργασίας, όπως η διαχείριση πιστωτικού κινδύνου ή η ανίχνευση απάτης.
Ενώ ο έλεγχος RADIUS παρέχει hop-by-hop επικύρωση, προστασία ακεραιότητας, και IPSEC, μπορεί να υιοθετηθεί για να παρέχεί hop-by-hop εμπιστευτικότητα, ενώ η ασφάλεια αντικειμένου στοιχείων δεν υποστηρίζεται, και έτσι τα συστήματα που βασίζονται σε έλεγχο RADIUS δεν είναι σε θέση να αναπτυχθούν με τα μη-έμπιστα proxies, ή σε καταστάσεις που απαιτούν παρακολούθηση
Ενώ το RADIUS δεν υποστηρίζει τη συμπίεση, η συμπίεση IP, μπορεί να υιοθετηθεί. Ενώ σε γενικές γραμμές υπάρχει η δυνατότητα καθορισμού νέων ιδιοτήτων, το RADIUS πάσχει από περιορισμένο χώρο ιδιοτήτων (256 ιδιότητες).

4.8.10.2 TACACS +

Το TACACS + προσφέρει ένα πρότυπο ελέγχου με αρχή, stop και ενδιάμεσα μηνύματα αναπροσαρμογής. Δεδομένου ότι το TACACS + είναι βασισμένο στο TCP, οι εφαρμογές είναι ελαστικές ενάντια στην απώλεια πακέτων και τα βραχυχρόνια χωρίσματα δικτύου. Μιας και το TACACS + τρέχει πάνω στο TCP, προσφέρει υποστήριξη τόσο για το στρώμα μεταφορών όσο και για το στρώμα εφαρμογής, και είναι κατάλληλο για ταυτόχρονο έλεγχο χρήσης και χειρισμό των γεγονότων ελέγχου που απαιτούν μέτρια αλλά όχι και τη χαμηλότερη καθυστέρηση επεξεργασίας.
Το TACACS + επιτρέπει την επικύρωση και την ακεραιότητα hop-by-hop καθώς επίσης και την hop-by-hop εμπιστευτικότητα. Η ασφάλεια των στοιχείων

αντικείμενου δεν υποστηρίζεται, και επομένως συστήματα βασισμένα στον έλεγχο TACACS + δεν μπορούν να αναπτυχθούν με την παρουσία μη-έμπιστων proxies. Ενώ το TACACS+ δεν υποστηρίζει συμπίεση, η συμπίεση IP, μπορεί να υιοθετηθεί

4.8.10.3 SNMP

Το καθιερωμένο πρωτόκολλο που χρησιμοποιείται για τη διαχείριση ενός διαδικτύου ονομάζεται *SNMP (Simple Network management Protocol - απλό πρωτόκολλο διαχείρισης δικτύου).* Το πρωτόκολλο SNMP ορίζει πώς ακριβώς ένας διαχειριστής επικοινωνεί με έναν πράκτορα. Για παράδειγμα, το SNMP ορίζει τη μορφή των αιτήσεων που στέλνει ένας διαχειριστής σε έναν πράκτορα και τη μορφή των απαντήσεων που επιστρέφει ο πράκτορας. Ακόμα, το SNMP ορίζει την ακριβή σημασία κάθε πιθανής αίτησης και απάντησης. Ειδικότερα, το SNMP ορίζει ότι ένα μήνυμα SNMP κωδικοποιείται με ένα πρότυπο που ονομάζεται *ASN.1 (Abstract Syntax Notation.1 - αφηρημένος συντακτικός συμβολισμός* 1)*.

Αν και οι πλήρεις λεπτομέρειες της κωδικοποίησης ASN.1 υπερβαίνουν τα όρια αυτού του βιβλίου, ένα απλό παράδειγμα θα μας βοηθήσει να εξηγήσουμε την κωδικοποίηση: Ας υποθέσουμε ότι στέλνεται ένας ακέραιος αριθμός μεταξύ ενός πράκτορα και ενός διαχειριστή. Για να μπορούν να στέλνονται μεγάλες τιμές χωρίς να γίνεται σπατάλη χώρου σε κάθε μεταφορά, το ASN.1 χρησιμοποιεί ένα συνδυασμό μήκους και τιμής για κάθε αντικείμενο που μεταφέρεται. Για παράδειγμα, ένας ακέραιος από *Ο* μέχρι 255 μπορεί να μεταφέρεται με μία μόνο οκτάδα. Οι ακέραιοι της περιοχής από 256 μέχρι *65535* χρειάζονται δύο οκτάδες, ενώ οι μεγαλύτεροι ακέραιοι χρειάζονται τρεις ή περισσότερες οκτάδες. Για να κωδικοποιήσει έναν ακέραιο, το ASN.1 στέλνει ένα ζεύγος τιμών: ένα μήκος, L, ακολουθούμενο από *L* οκτάδες οι οποίες περιέχουν τον ακέραιο. Για να μπορούν να κωδικοποιούνται οσοδήποτε μεγάλοι ακέραιοι, το ASN.1 επιτρέπει επίσης να καταλαμβάνει το μήκος περισσότερες από μία οκτάδες. Συνήθως, τα εκτεταμένα μεγέθη δε χρειάζονται για τους ακεραίους που χρησιμοποιούνται με το πρωτόκολλο SNMP. Η κωδικοποίηση παρουσιάζεται στον Πίνακα 2.

Αν και θα ακολουθήσουμε τη σύμβαση να χρησιμοποιούμε τους όρους *διαχειριστής* και *πράκτορας, ο* χρήστης θα πρέπει να θυμάται ότι συμπεριφέρονται όπως οποιοσδήποτε πελάτης και διακομιστής.

Αν και πολλές τοποθεσίες χρησιμοποιούν ακόμα την έκδοση 2 του SNMP, η οποία γράφεται *SNMPv2,* το τρέχον πρότυπο είναι το *SNMPv3.* Προφέρεται έι ες *εν τελεία ένα.*

δεκαδικός ακέραιος	δεκαεξαδικός ισοδύναμος	οκτάδα μήκους	οκτάδες τιμής (δεκαεξαδικό)
27	1B	01	1B
792	318	02	03 18
24,567	5FF7	02	5P F7
190,345	2E789	03	02 E7 89

Πίνακας 2 Παράδειγμα κωδικοποίησης ASN.1 για ακεραίους. Μπροστά από κάθε ακέραιο τοποθετείται ένα πεδίο μήκους, το οποίο καθορίζει τον αριθμό των οκτάδων που χρησιμοποιούνται για την κωδικοποίηση της ακέραιας τιμής.

Υπόδειγμα προσκόμισης-αποθήκευσης

Το πρωτόκολλο SNMP δεν ορίζει μεγάλο σύνολο διαταγών. Χρησιμοποιεί το *υπόδειγμα προσκόμισης-αποθήκευσης (fetch-store paradigm),* στο οποίο υπάρχουν δύο βασικές πράξεις: *η fetch{προσκόμιση),* η οποία χρησιμοποιείται για να ληφθεί μια τιμή από μια συσκευή, και η *store (αποθήκευση),* η οποία χρησιμοποιείται για να τοποθετηθεί μια τιμή σε μια συσκευή. Σε κάθε αντικείμενο που μπορεί να προσκομιστεί ή να αποθηκευτεί δίνεται ένα μοναδικό όνομα μια διαταγή που πραγματοποιεί μια πράξη προσκόμισης ή αποθήκευσης πρέπει να καθορίζει το όνομα του αντικειμένου.

Είναι μάλλον προφανές πώς μπορούν να χρησιμοποιούνται πράξεις προσκόμισης για την εποπτεία μιας συσκευής ή για να διαπιστωθεί η κατάσταση της: Πρέπει να οριστεί ένα σύνολο αντικειμένων κατάστασης, και να τους δοθούν ονόματα. Για να αποκτήσει ένας διαχειριστής πληροφορίες κατάστασης, προσκομίζει την τιμή που αντιστοιχεί σε ένα δεδομένο αντικείμενο. Για παράδειγμα, μπορεί να οριστεί ένα αντικείμενο το οποίο καταμετρά τα πλαίσια που απορρίπτει μια συσκευή επειδή το άθροισμα ελέγχου του πλαισίου είναι λανθασμένο. Το λογισμικό πρέπει να προγραμματιστεί έτσι ώστε να αυξάνει κατά ένα το μετρητή όποτε ανιχνεύεται ένα σφάλμα αθροίσματος ελέγχου. Ο διαχειριστής μπορεί να χρησιμοποιήσει το SNMP για να προσκομίσει την τιμή που αντιστοιχεί στο μετρητή, ώστε να προσδιορίσει αν παρουσιάζονται σφάλματα αθροίσματος ελέγχου.

Η χρήση του υποδείγματος προσκόμισης-αποθήκευσης για να ασκείται έλεγχος σε μια συσκευή μπορεί να μη φαίνεται προφανής· οι πράξεις ελέγχου ορίζονται ως παρενέργειες της αποθήκευσης σε ένα αντικείμενο.

Για παράδειγμα, το SNMP δεν περιλαμβάνει ξεχωριστές διαταγές για το *μηδενισμό (reset)* του μετρητή των σφαλμάτων αθροίσματος ελέγχου ή για την *επανεκκίνηση (reboot)* της συσκευής. Στην περίπτωση του μετρητή των σφαλμάτων αθροίσματος ελέγχου, η αποθήκευση μιας μηδενικής τιμής στο αντικείμενο είναι η προφανής λύση, επειδή έτσι ο μετρητής μηδενίζεται. Για πράξεις όπως η επανεκκίνηση, όμως, ένας πράκτορας του SNMP πρέπει να προγραμματιστεί έτσι ώστε να ερμηνεύει τις αιτήσεις αποθήκευσης και να εκτελεί την κατάλληλη ακολουθία πράξεων για να επιτευχθεί το επιθυμητό αποτέλεσμα. Έτσι, το SNMP θα μπορούσε να ορίζει ένα αντικείμενο επανεκκίνησης, και να
καθορίζει ότι η αποθήκευση της τιμής μηδέν στο αντικείμενο θα προκαλεί την επανεκκίνηση του συστήματος. Στην πράξη, όμως, τα περισσότερα συστήματα δεν

έχουν μετρητή επανεκκίνησης - το λογισμικό του πράκτορα πρέπει να ελέγχει άμεσα για μια πράξη αποθήκευσης η οποία καθορίζει το αντικείμενο επανεκκίνησης, και μετά να εκτελεί την ακολουθία των βημάτων που απαιτούνται για να επανεκκινήσει το σύστημα. Ας συνοψίσουμε:
Το SNMP χρησιμοποιεί το υπόδειγμα προσκόμισης-αποθήκευσης (fetch-store) για την αλληλεπίδραση μεταξύ ενός διαχειριστή και ενός πράκτορα. Ο διαχειριστής προσκομίζει τιμές για να προσδιορίσει την κατάσταση της συσκευής οι πράξεις που ελέγχουν τη συσκευή ορίζονται ως παρενέργειες της αποθήκευσης τιμών σε αντικείμενα.

4.9 Εξασφάλιση των Backups

Η διαδικασία δημιουργίας backup είναι ένα κλασικό μέρος στην ασφάλεια ενός συγκροτήματος ηλεκτρονικών υπολογιστών.
Μέσα στο πλαίσιο της παρούσας εργασίας, τα backups εξετάζονται ως τμήμα του γενικού σχεδίου ασφάλειας ενός οργανισμού.
Υπάρχουν διάφορες πτυχές των backups που είναι σημαντικές μέσα σε αυτό το πλαίσιο:

(1) Σιγουρευόμαστε ότι ο οργανισμός δημιουργεί backups.
(2) Σιγουρευόμαστε ότι ο οργανισμός χρησιμοποιεί offsite αποθήκευση. Ο οργανισμός αποθήκευσης πρέπει να επιλεχτεί προσεκτικά και για την ασφάλειά του και για τη διαθεσιμότητά του.
(3) Χρησιμοποιούμε κρυπτογράφηση των backups για να παρασχεθεί η πρόσθετη προστασία των πληροφοριών όταν είναι off-site. Εντούτοις, πρέπει να ξέρουμε ότι θα χρειαστεί ένα καλό διοικητικό σχέδιο έτσι ώστε να είμαστε σε θέση μελλοντικά να ανακτήσουμε τα στοιχεία από οποιοδήποτε σημείο. Επίσης, πρέπει να σιγουρευτούμε ότι θα υπάρχει πρόσβαση στα απαραίτητα προγράμματα αποκρυπτογράφησης σε τόσο χρόνο στο μέλλον όσο χρειάζεται να εκτελεστεί η αποκρυπτογράφηση.
(4) Δεν πρέπει να υποθέτουμε ότι τα backups είναι πάντα καλά.
Έχουν υπάρξει πολλές περιπτώσεις γεγονότων ασφάλειας υπολογιστών που έχουν συνεχιστεί για μακριές χρονικές περιόδους προτού να παρατηρηθεί από τον οργανισμό. Σε τέτοιες περιπτώσεις, τα backups των επηρεασθέντων συστημάτων είναι επίσης μολυσμένα.
(5) Περιοδικά ελέγχουμε την ακρίβεια και την πληρότητα τών backup.

Κεφάλαιο 5. Χειρισμός ασφάλειας

5.1 Εισαγωγή

Αυτό το κεφάλαιο παρέχει την καθοδήγηση που χρειάζεται προτού, κατά τη διάρκεια, και μετά από ένα γεγονός ασφάλειας σε έναν host (ξενιστή), ένα δίκτυο, έναν οργανισμό, ή ένα multi-site περιβάλλον. Η φιλοσοφία σε περίπτωση παραβίασης της ασφάλειας υπολογιστών είναι η αντίδραση σύμφωνα με ένα ήδη διαμορφωμένο σχέδιο.

Αυτό ισχύει εάν η παραβίαση είναι το αποτέλεσμα μιας εξωτερικής επίθεσης εισβολέων, μιας ακούσιας ζημίας, ενός σπουδαστή που χρησιμοποιεί κάποιο νέο πρόγραμμα για να εξετάσει τις αδυναμίες λογισμικού, ή ενός δυσαρεστημένου υπαλλήλου. Κάθε ένας από τους πιθανούς τύπους γεγονότων πρέπει να εξεταστεί εκ των προτέρων από τα σχέδια πιθανοτήτων.

Η παραδοσιακή ασφάλεια υπολογιστών, ενώ είναι αρκετά σημαντική στο γενικό σχέδιο ασφάλειας του οργανισμού, δίνει συνήθως λίγη προσοχή στο πώς πρέπει να χειριστεί πραγματικά μια επίθεση κατά την εμφάνισή της .

Το αποτέλεσμα είναι ότι όταν μια επίθεση είναι υπό εξέλιξη, πολλές αποφάσεις λαμβάνονται βιαστικά και μπορεί να είναι καταστρεπτικές στην προσπάθεια ανακάλυψης της πηγής του γεγονότος, της συλλογή των στοιχείων που χρησιμοποιούνται στις προσπάθειες συνέχισης, στην προετοιμασία για την αποκατάσταση του συστήματος, και την προστασία των πολύτιμων στοιχείων που περιλαμβάνονται στο σύστημα.

Ένα από το σημαντικότερα, αλλά συχνά αγνοημένα, οφέλη για τον αποδοτικό χειρισμό είναι το οικονομικό.

Η ανταπόκριση του τεχνικού και διευθυντικού προσωπικού σε ένα γεγονός απαιτεί σημαντικούς πόρους.

Εάν εκπαιδευτούν στο να χειρίζονται τα γεγονότα αποτελεσματικά, απαιτείται λιγότερος χρόνος όταν εμφανίζεται ένα πρόβλημα.

Λόγω του παγκόσμιου δικτύου τα περισσότερα γεγονότα δεν είναι περιορισμένα σε έναν απλό οργανισμό .

Οι αδυναμίες των λειτουργικών συστημάτων ισχύουν για διάφορα εκατομμύρια συστημάτων, και πολλές από αυτές αξιοποιούνται μέσα στο ίδιο το δίκτυο.

Επομένως, είναι ζωτικής σημασίας όλοι οι οργανισμοί με τα περιληφθέντα συμβαλλόμενα μέρη να ενημερώνονται το συντομότερο δυνατόν.

Ένα άλλο όφελος είναι οι δημόσιες σχέσεις. Η δημοσιότητα γύρω από τα γεγονότα ασφάλειας υπολογιστών μπορεί να είναι καταστρεπτική για τη σχέση μιας οργάνωσης με τους τρέχοντες ή τους πιθανούς πελάτες. Ο αποδοτικός χειρισμός ελαχιστοποιεί τη δυνατότητα αρνητικής έκθεσης.

Ένα τελικό όφελος ενός αποδοτικού χειρισμού ασφαλείας συσχετίζεται με τα νομικά ζητήματα. Είναι πιθανό, στο εγγύς μέλλον, οι οργανώσεις να μπορούν να θεωρηθούν υπεύθυνες επειδή ένας από τους κόμβους τους χρησιμοποιήθηκε για την προώθηση μιας επίθεσης δικτύων. Παρόμοια, οι άνθρωποι που αναπτύσσουν patches ή workarounds μπορούν να μηνυθούν

εάν τα patches ή workarounds είναι ατελέσφορα, με συνέπεια τη παραβίαση των συστημάτων

Γνωρίζοντας τις αδυναμίες του λειτουργικού συστήματος και τα σχέδια επιθέσεων, και λαμβάνοντας έπειτα τα κατάλληλα μέτρα για να αντιμετωπιστούν αυτές οι πιθανές απειλές, είναι λάθος η παράκαμψη των νομικών συμβουλών.
Αυτό το τμήμα παρέχει μια περίληψη και μια αφετηρία για τη δημιουργία της πολιτικής ενός οργανισμού για το χειρισμό των γεγονότων ασφάλειας. Τα τμήματα είναι:

(1) Προετοιμασία και προγραμματισμός (ποιοι είναι οι σκοποί και οι στόχοι στο χειρισμό ενός γεγονότος).
(2) Ανακοίνωση (ποιος πρέπει να ειδοποιηθεί στην περίπτωση ενός γεγονότος).
- Τοπικοί διευθυντές και προσωπικό
- Νομικοί και εξεταστικοί αντιπρόσωποι
- Ομάδες χειρισμού ασφάλειας υπολογιστών
- Επηρεασμένοι και σχετικοί οργανισμοί
- Εσωτερικές επικοινωνίες
- Δημόσιες σχέσεις και δελτία τύπου

(3) Προσδιορισμός ενός γεγονότος (εάν υπάρχει γεγονός και πόσο σοβαρό είναι αυτό).
(4) Χειρισμός (τι πρέπει να γίνει όταν εμφανίζεται ένα γεγονός).
- Ανακοίνωση (ποιος πρέπει να ενημερωθεί για το γεγονός)
- Προστασία της δραστηριότητας στοιχείων (ποια αρχεία πρέπει να διατηρηθούν από πριν, κατά τη διάρκεια, και μετά από το γεγονός)
- Συγκράτηση (πώς μπορεί η ζημία να περιοριστεί)
- Εξόντωση (πώς να αποβληθούν οι λόγοι που προκάλεσαν το γεγονός)
- Αποκατάσταση (πώς πρέπει να επανεγκαθιδρύσει η υπηρεσία και τα συστήματα)
- Συνέχεια (ποιες ενέργειες πρέπει να ληφθούν μετά από το γεγονός)

(5) Συνέπεια (ποιες είναι οι επιπτώσεις των προηγούμενων γεγονότων).
(6) Διοικητική απάντηση στα γεγονότα.

Το υπόλοιπο αυτού του κεφαλαίου θα αναλύσει τα ζητήματα που περιλαμβάνουν κάθε ένα από τα σημαντικά θέματα που απαριθμούνται ανωτέρω, και θα παράσχει κάποιες οδηγίες ως προς αυτό που πρέπει να περιληφθεί σε μια πολιτική οργανισμού για το χειρισμό των γεγονότων.

5.2 Προετοιμασία και προγραμματισμός για το χειρισμό ενός γεγονότος

Μέρος του χειρισμού ενός γεγονότος είναι να υπάρχει ήδη προετοιμασία για την αντιμετώπισή του προτού εμφανιστεί. Αυτό περιλαμβάνει την καθιέρωση ενός κατάλληλου επιπέδου προστασίας όπως περιγράφτηκε στα προηγούμενα κεφάλαια.
Η ενέργεια αυτή θα βοηθήσει τον οργανισμό να αποτρέψει γεγονότα καθώς και να περιορίσει την πιθανή ζημία.. Η προστασία περιλαμβάνει επίσης την προετοιμασία οδηγιών διαχείρισης ως τμήμα ενός σχεδίου αντιμετώπισης για την οργάνωση ή τον οργανισμό. Η δημιουργία των σχεδίων αποβάλλει ένα μεγάλο μέρος της ασάφειας που εμφανίζεται κατά τη διάρκεια ενός γεγονότος και οδηγεί σε ένα πιο κατάλληλο και λεπτομερές σύνολο απαντήσεων.

Είναι ζωτικής σημασίας να εξεταστεί το προτεινόμενο σχέδιο προτού να εμφανιστεί ένα γεγονός μέσω των "δοκιμαστικών λειτουργιών". Μια ομάδα ακόμη πρέπει να προσλάβει μια ειδική ομάδα για να ενεργεί παράλληλα με τη δοκιμαστική λειτουργία. (Σημείωση: μια ειδική ομάδα είναι ομάδα ειδικών που προσπαθούν να διαπεράσουν την ασφάλεια ενός συστήματος.)
Η εκμάθηση της σωστής απάντησης σε ένα γεγονός είναι σημαντική για διάφορους λόγους:

(1) Προστατεύει τους πόρους που θα μπορούσαν να προσβληθούν
(2) Προστατεύει τους πόρους που θα μπορούσαν να χρησιμοποιηθούν περισσότερο επικερδώς εάν ένα γεγονός δεν απαιτούσε τις υπηρεσίες τους
(3)Συμμορφώνει με (κυβέρνησης ή άλλους) κανονισμούς
(4) Αποτρέπει τη χρήση των συστημάτων σε επιθέσεις ενάντια σε άλλα συστήματα.
(5) Ελαχιστοποιεί τη δυνατότητα για αρνητική έκθεση

Όπως σε κάθε σετ προσχεδιασμένων διαδικασιών, προσοχή πρέπει να δοθεί σε ένα σύνολο στόχων που χειρίζονται ένα γεγονός. Αυτοί οι στόχοι θα έχουν διαφορετική προτεραιότητα ανάλογα με τον οργανισμό.
Ένα συγκεκριμένο σύνολο στόχων μπορεί να προσδιοριστεί για την αντιμετώπιση των γεγονότων:

(1)Υπολογισμός του πώς συνέβη.
(2) Ανακάλυψη του πώς θα αποφευχθεί η περαιτέρω εκμετάλλευση της ίδιας αδυναμίας.
(3) Αποφυγή της κλιμάκωσης και περαιτέρω γεγονότων.
(4) Αξιολόγηση του αντίκτυπου και της ζημίας του γεγονότος.
(5) Επαναφορά του συστήματος.
(6) Ενημέρωση των πολιτικών και των διαδικασιών που απαιτείται.
(7) Ανακάλυψη του υπεύθυνου.

Λόγω της φύσης του γεγονότος, μπορεί να υπάρξει μια σύγκρουση μεταξύ της ανάλυσης της αρχικής πηγής ενός προβλήματος και της αποκατάστασης των συστημάτων και των υπηρεσιών. Οι γενικοί στόχοι (όπως η βεβαίωση της ακεραιότητας των κρίσιμων συστημάτων) μπορεί να είναι ένας λόγος για την μη ανάλυση ενός γεγονότος. Φυσικά, αυτό είναι μια σημαντική διοικητική απόφαση αλλά όλα τα συμβαλλόμενα μέρη πρέπει να γνωρίζουν ότι χωρίς ανάλυση, το ίδιο γεγονός μπορεί να συμβεί πάλι.
Είναι επίσης σημαντικό να δοθεί προτεραιότητα σε ενέργειες που λαμβάνονται κατά τη διάρκεια ενός γεγονότος πολύ πριν το χρόνο της εμφάνισης του. Μερικές φορές ένα γεγονός μπορεί να είναι τόσο σύνθετο που είναι αδύνατο να γίνουν όλα μονομιάς. Οι προτεραιότητες είναι ουσιαστικές. Αν και οι προτεραιότητες ποικίλουν από ίδρυμα σε ίδρυμα, οι ακόλουθες προτεινόμενες προτεραιότητες μπορούν να χρησιμεύσουν ως μια αφετηρία για τον καθορισμό της απάντησης της οργάνωσης:

(1) **Προτεραιότητα πρώτη** -- Προστασία της ανθρώπινης ζωής. Η ασφάλεια της ανθρώπινης ζωής έχει πάντα την μεγαλύτερη προτεραιότητα

(2)**Προτεραιότητα δεύτερη** -- Προστασία απόρρητων ή ευαίσθητων στοιχείων. Αποτροπή της εκμετάλλευσης απορρήτων ή ευαίσθητων συστημάτων, δικτύων ή περιοχών. Ενημέρωση των επηρεασθέντων και ευαίσθητων συστημάτων, δικτύων ή περιοχών για τις ήδη εμφανισμένες διεισδύσεις.

(3)**Προτεραιότητα τρίτη** -- Προστασία άλλων στοιχείων, συμπεριλαμβανομένου ιδιόκτητων, επιστημονικών, διευθυντικών και άλλων στοιχείων, επειδή η απώλεια στοιχείων είναι δαπανηρή από άποψη πόρων. Αποτροπή της εκμετάλλευσης άλλων συστημάτων, δικτύων ή περιοχών και ενημέρωση των ήδη επηρεασθέντων συστημάτων, δικτύων ή περιοχών για τις επιτυχείς διεισδύσεις.

(4)**Προτεραιότητα τέταρτη** -- Αποτροπή της ζημίας στα συστήματα (π.χ., απώλεια ή αλλαγή των αρχείων συστημάτων, ζημία σε δίσκους, κ.λπ.). Η ζημία στα συστήματα μπορεί να οδηγήσει σε απώλεια χρόνου και σε κόστος αποκατάστασης.

(5)**Προτεραιότητα πέμπτη** -- Ελαχιστοποίηση της διάσπασης των υπολογιστικών πόρων. Είναι καλύτερα σε πολλές περιπτώσεις να κλείσει ένα σύστημα ή να αποσυνδεθεί από ένα δίκτυο από να διακινδυνευτεί ζημία στα δεδομένα ή τα συστήματα. Οι οργανισμοί θα πρέπει να αξιολογούν τα υπέρ και τα κατά ανάμεσα στη διακοπή και την αποσύνδεση ή την παραμονή σε λειτουργία. Μπορεί να υπάρξουν συμφωνίες που μπορεί να απαιτούν τη συνεχή λειτουργία των συστημάτων ακόμη και λαμβάνοντας υπόψη την περαιτέρω εμφάνιση ζημίας. Εντούτοις, η ζημία και το μέγεθος ενός γεγονότος μπορούν να είναι τόσο εκτενείς που οι συμφωνίες μπορεί να χρειαστεί να αγνοηθούν.

Μια σημαντική επίπτωση στον καθορισμό των προτεραιοτήτων είναι ότι μόλις η ανθρώπινη ζωή και τα θέματα εθνικής ασφάλειας έχουν αντιμετωπιστεί, είναι γενικά σημαντικότερο να σωθούν τα δεδομένα παρά το λογισμικό και το υλικό συστημάτων. Αν και είναι ανεπιθύμητο να υπάρξει οποιαδήποτε ζημία ή απώλεια κατά τη διάρκεια ενός γεγονότος, τα συστήματα μπορούν να αντικατασταθούν. Εντούτοις, η απώλεια ή ο συμβιβασμός των δεδομένων (ειδικά ταξινομημένα ή ιδιόκτητα στοιχεία) δεν είναι συνήθως μια αποδεκτή έκβαση κάτω από οποιεσδήποτε περιστάσεις.
Μια άλλη σημαντική ανησυχία είναι η επίδραση σε άλλους, πέρα από τα συστήματα και τα δίκτυα όπου το γεγονός εμφανίζεται. Μέσα στα όρια που επιβάλλονται από τους κυβερνητικούς κανονισμούς είναι πάντα σημαντικό να ενημερωθούν τα επηρεασθέντα συμβαλλόμενα μέρη το συντομότερο δυνατόν. Λόγω των νομικών επιπτώσεων αυτού του θέματος, πρέπει να περιληφθεί στις προγραμματισμένες διαδικασίες για να αποφευχθούν περαιτέρω καθυστερήσεις και αβεβαιότητες για τους διαχειριστές.
Οποιοδήποτε σχέδιο απάντησης στα γεγονότα ασφάλειας πρέπει να καθοδηγηθεί από τις τοπικές πολιτικές και τους κανονισμούς. Κυβέρνηση και ιδιωτικός τομέας που ασχολούνται με ευαίσθητο υλικό έχουν συγκεκριμένους κανόνες που πρέπει να ακολουθήσουν.
Οι πολιτικές που επιλέγονται από τον οργανισμό, σύμφωνα με τον τρόπο αντίδρασης στα γεγονότα, θα διαμορφώσουν την απάντηση.
Παραδείγματος χάριν, μπορεί να έχει λίγο νόημα να δημιουργηθούνε μηχανισμοί για να ελέγξουν και να επισημάνουν τους εισβολείς εάν ο οργανισμός δεν προγραμματίζει να λάβει μέτρα ενάντια στους εισβολείς όταν πιάνονται. Άλλες οργανώσεις μπορεί να έχουν πολιτικές που έχουν επιπτώσεις στα σχέδιά. Οι

τηλεφωνικές επιχειρήσεις δημοσιεύουν συχνά τις πληροφορίες για τα τηλεφωνικά ίχνη μόνο στις αντιπροσωπείες επιβολής νόμου.
Ο χειρισμός των γεγονότων μπορεί να είναι χρονοβόρος και να απαιτεί την εκτέλεση ενός αριθμού στερεότυπων στόχων που θα μπορούσαν να αντιμετωπιστούν από το προσωπικό υποστήριξης. Για να ελευθερωθεί το τεχνικό προσωπικό μπορεί να είναι χρήσιμο να προσδιοριστεί το προσωπικό υποστήριξης που θα αναλάβει τις καθημερινές εργασίες .

5.3 Ειδοποίηση και σημεία επαφής

Είναι σημαντικό να δημιουργηθούν επαφές με το προσωπικό προτού να εμφανιστεί ένα πραγματικό γεγονός. Πολλές φορές, τα γεγονότα δεν είναι πραγματικές έκτακτες ανάγκες. Πράγματι, συχνά θα είμαστε σε θέση να χειριστούμε τις δραστηριότητες εσωτερικά. Εντούτοις, θα υπάρξουν επίσης πολλές φορές που θα πρέπει άλλοι έξω από το άμεσο τμήμα να περιληφθούν στο χειρισμό του γεγονότος.
Αυτές οι πρόσθετες επαφές περιλαμβάνουν τους τοπικούς manager και τους διαχειριστές συστημάτων, διοικητικές επαφές για άλλους οργανισμούς στο διαδίκτυο, και διάφορες εξεταστικές οργανώσεις. Η γνωριμία με αυτές τις επαφές προτού να εμφανιστούν τα γεγονότα θα βοηθήσει να κατασταθεί η αντιμετώπιση του γεγονότος αποδοτικότερη. Για κάθε τύπο επαφής επικοινωνίας, τα συγκεκριμένα "σημεία επαφής" (POC) πρέπει να καθοριστούν.
Αυτά μπορεί να είναι τεχνικής ή διοικητικής φύσεως και μπορεί να περιλαμβάνουν νομικές ή εξεταστικές αντιπροσωπείες καθώς επίσης και φορείς παροχής υπηρεσιών και προμηθευτές. Μετά την επίτευξη αυτών των επαφών, είναι σημαντικό να αποφασιστεί πόσες πληροφορίες θα μοιραστούν σε κάθε κατηγορία επαφής. Είναι ιδιαίτερα σημαντικό να καθοριστεί ποιες πληροφορίες θα δοθούν στους χρήστες ενός τόπου, στο κοινό (συμπεριλαμβανομένου του Τύπου), καθώς και σε άλλους.
Η αντιμετώπιση αυτών των ζητημάτων είναι ιδιαίτερα σημαντική για ένα τοπικό αρμόδιο για το χειρισμό του γεγονότος, δεδομένου ότι αυτός είναι αρμόδιος για την πραγματική ενημέρωση των υπολοίπων. Ένας κατάλογος επαφών σε κάθε μια από αυτές τις κατηγορίες είναι σημαντικός χρονικός αποταμιευτής για αυτό το πρόσωπο κατά τη διάρκεια ενός γεγονότος. Μπορεί να είναι αρκετά δύσκολο να βρεθεί ένα κατάλληλο πρόσωπο κατά τη διάρκεια ενός γεγονότος όταν πολλά επείγοντα γεγονότα βρίσκονται σε εξέλιξη.
Συνιστάται όλοι οι σχετικοί αριθμοί τηλεφώνου (επίσης διευθύνσεις ηλεκτρονικού ταχυδρομείου και αριθμοί fax) να περιλαμβάνονται στην πολιτική ασφάλειας περιοχών. Τα ονόματα και τα στοιχεία επαφής όλων των ατόμων που θα συμμετάσχουν άμεσα στο χειρισμό ενός γεγονότος πρέπει να τοποθετηθούν στην κορυφή αυτού του καταλόγου.

5.3.1 Τοπικοί διευθυντές και προσωπικό

Όταν ένα γεγονός είναι εν εξελίξει, ένα σημαντικό ζήτημα είναι η απόφαση για το ποιος είναι υπεύθυνος για το συντονισμό της δραστηριότητας του πλήθους των φορέων. Ένα σημαντικό λάθος που μπορεί να γίνει είναι να υπάρξουν διάφοροι άνθρωποι που κάθε ένας τους να λειτουργεί ανεξάρτητα. και όχι από κοινού. Αυτό

θα προσθέσει μόνο σύγχυση στο γεγονός και θα οδηγήσει πιθανώς σε μια ατελέσφορη προσπάθεια.

Ένα POC μπορεί ή όχι να είναι υπεύθυνο για τη δημιουργία του γεγονότος. Υπάρχουν δύο ευδιάκριτοι ρόλοι που πρέπει να αποδοθούν κατά την απόφαση του ποιος θα είναι το POC και ποιος θα είναι το πρόσωπο υπεύθυνο για το γεγονός. Το πρόσωπο υπεύθυνο για το γεγονός θα λάβει τις αποφάσεις ως προς την ερμηνεία της πολιτικής που απευθύνεται στο γεγονός. Αντίθετα, το POC πρέπει να συντονίσει τις προσπάθειες όλων των συμβαλλόμενων μερών που ασχολούνται με το χειρισμό του γεγονότος.

Το POC πρέπει επίσης να είναι ένα πρόσωπο με τεχνική πείρα για να συντονίσει επιτυχώς τις προσπάθειες των διευθυντών και των χρηστών συστημάτων που συμμετέχουν στον έλεγχο και την αντίδραση στην επίθεση. Προσοχή πρέπει να ληφθεί κατά τον προσδιορισμό του πρόσωπου αυτού. Δεν πρέπει να είναι απαραιτήτως το ίδιο πρόσωπο που έχει τη διαχειριστική ευθύνη για τα παραβιασμένα συστήματα δεδομένου ότι συχνά τέτοιοι διαχειριστές έχουν μόνο ικανοποιητική γνώση για την καθημερινή χρήση των υπολογιστών, και έλλειψη σε βάθος τεχνικής πείρας.

Μια άλλη σημαντική λειτουργία του POC είναι να διατηρηθεί η επαφή με την επιβολή νόμου και άλλες εξωτερικές αντιπροσωπείες ώστε να επιβεβαιωθεί η συμμετοχή πολλαπλών αντιπροσωπειών . Το επίπεδο συμμετοχής θα καθοριστεί με τις διοικητικές αποφάσεις καθώς επίσης και με τους νομικούς περιορισμούς.

Ένα POC πρέπει επίσης να είναι το μόνο πρόσωπο υπεύθυνο για τη συλλογή των στοιχείων, αφού εμπειρικά, όσο περισσότεροι είναι οι άνθρωποι που αγγίζουν ένα πιθανό κομμάτι στοιχείων, τόσο μεγαλύτερη είναι η πιθανότητα ότι δεν θα είναι αποδεκτά στο δικαστήριο. Για να εξασφαλιστεί ότι τα στοιχεία θα είναι αποδεκτά από τη νομική κοινότητα, η συλλογή των στοιχείων πρέπει να γίνει σύμφωνα με τις προκαθορισμένες διαδικασίες και σύμφωνα με τους τοπικούς νόμους και νομικούς κανονισμούς.

Ένας από τους κρισιμότερους στόχους για το POC είναι ο συντονισμός όλων των σχετικών διαδικασιών. Οι ευθύνες μπορούν να κατανεμηθούν σε ολόκληρο τον οργανισμό, περιλαμβάνοντας πολλαπλάσια ανεξάρτητα τμήματα ή ομάδες.

Αυτό θα απαιτήσει μια καλά συντονισμένη προσπάθεια προκειμένου να επιτευχθεί γενική επιτυχία. Η κατάσταση γίνεται ακόμα πιο σύνθετη εάν συμμετέχουν πολλαπλοί οργανισμοί. Όταν αυτό συμβαίνει, σπάνια ένα POC θα είναι σε θέση επί τόπου να συντονίσει επαρκώς το χειρισμό ολόκληρου του γεγονότος. Άντ' αυτού, πρέπει να αναμιχθούν οι κατάλληλες συναφείς ομάδες απάντησης.

Η διαχειριζόμενη διαδικασία πρέπει να παρέχει μερικούς μηχανισμούς κλιμάκωσης. Προκειμένου να καθοριστεί ένας τέτοιος μηχανισμός, οι οργανισμοί θα πρέπει να δημιουργήσουν ένα εσωτερικό σχέδιο ταξινόμησης για τα γεγονότα.. Δεδομένου ότι ένα γεγονός κλιμακώνεται, μπορεί να υπάρξει μια αλλαγή στο POC που θα πρέπει να διαβιβαστεί σε όλους τους άλλους που περιλαμβάνονται στο χειρισμό του γεγονότος. Όταν γίνεται μια αλλαγή POC, το παλαιό POC πρέπει να ενημερώσει το νέο POC για όλες τις βασικές πληροφορίες.

Τελικά, οι χρήστες πρέπει να ξέρουν πώς να αναφέρουν τα πιθανά γεγονότα. Οι οργανισμοί πρέπει να συντάξουν διαδικασίες υποβολής εκθέσεων που θα λειτουργούν και κατά τη διάρκεια και εκτός των κανονικών ωρών απασχόλησης. Τα γραφεία βοήθειας χρησιμοποιούνται συχνά για να λάβουν αυτές τις εκθέσεις κατά τη διάρκεια των κανονικών ωρών απασχόλησης, ενώ βομβητές και τηλέφωνα μπορούν να χρησιμοποιηθούν για την υποβολή έκθεσης εκτός ωρών απασχόλησης.

5.3.2 Επιβολή νόμου και εξεταστικές αντιπροσωπείες

Σε περίπτωση γεγονότος που έχει νομικές συνέπειες, είναι σημαντικό να καθιερωθεί επαφή με εξεταστικές αντιπροσωπείες το συντομότερο δυνατόν. Η τοπική επιβολή νόμου, τα τοπικά γραφεία ασφάλειας, και τα τμήματα αστυνομίας πανεπιστημιουπόλεων πρέπει επίσης να ενημερωθούν ανάλογα με την περίπτωση. Αυτό το τμήμα περιγράφει πολλά από τα ζητήματα που θα αντιμετωπισθούν, αλλά αναγνωρίζεται ότι κάθε οργάνωση θα έχει τους τοπικούς και κυβερνητικούς νόμους και τους κανονισμούς της που θα συγκρούονται με την επιβολή νόμου και τις εξεταστικές αντιπροσωπείες. Το σημαντικότερο θέμα είναι ότι κάθε οργανισμός πρέπει να λειτουργήσει διαμέσου αυτών των ζητημάτων.
Ένας σημαντικός λόγος για τον καθορισμό αυτού του σημείου επαφής, πολύ πριν ένα γεγονός, είναι ότι μόλις μια σημαντική επίθεση είναι υπό εξέλιξη, υπάρχει λίγος χρόνος να κληθούν αυτές οι αντιπροσωπείες για να καθοριστεί ακριβώς ποιο είναι το σωστό σημείο της επαφής.
Ένας άλλος λόγος είναι ότι είναι σημαντική η συνεργασία με αυτές τις αντιπροσωπείες με έναν τρόπο που θα ενθαρρύνει μια καλή σχέση συνεργασίας, και που θα είναι σύμφωνη με τις διαδικασίες αυτών των αντιπροσωπειών. Το να υπάρχει γνώση αυτών των διαδικασιών εκ των προτέρων, και των προσδοκιών του σημείου επαφής είναι ένα μεγάλο βήμα προς αυτή την κατεύθυνση.
Παραδείγματος χάριν, είναι σημαντικό να συγκεντρωθούν στοιχεία που θα είναι αποδεκτά σε οποιεσδήποτε νομικές διαδικασίες, και αυτό απαιτεί την προγενέστερη γνώση για το πώς συγκεντρώνονται τέτοια στοιχεία. Ένας τελικός λόγος για την καθιέρωση επαφών το συντομότερο δυνατόν είναι ότι είναι αδύνατο να είναι γνωστή η ιδιαίτερη αντιπροσωπεία που θα έχει την αρμοδιότητα σε οποιοδήποτε δεδομένο γεγονός. Η αρχική παραγωγή των επαφών και η εύρεση των κατάλληλων καναλιών θα οδηγήσουν σε μια αρκετά πιο ομαλή αντίδραση σε ένα γεγονός .
Εάν η οργάνωση ή ο οργανισμός έχει νομικό συμβούλιο, πρέπει να ενημερωθεί αυτό το γραφείο το συντομότερο δυνατό αφότου μαθευτεί ότι ένα γεγονός είναι υπό εξέλιξη. Στην χειρότερη περίπτωση, το νομικό συμβούλιο πρέπει να αναμιχθεί για να προστατεύσει τα νομικά και οικονομικά συμφέροντα του οργανισμού ή της οργάνωσής. Υπάρχουν πολλά νομικά και πρακτικά ζητήματα, μερικά από τα οποία είναι:

(1)**Δημοσιότητα** --Εάν ο οργανισμός είναι πρόθυμος να διακινδυνεύσει την αρνητική δημοσιότητα ή την έκθεση για να συνεργαστεί με τις προσπάθειες νομικές δίωξης .

(2)**Downstream liability** -- Εάν αφήνετε ένα παραβιασμένο σύστημα όπως είναι και ένας άλλος υπολογιστής να υποστεί βλάβη επειδή η επίθεση προέρχεται από το σύστημά μας, ο οργανισμός ή η οργάνωσή μπορεί να είναι υπεύθυνη για τις ζημίες που υφίστανται.

(3) **Διανομή των πληροφοριών** -- Εάν ο οργανισμός μας διανέμει πληροφορίες για μια επίθεση στην οποία ένας άλλος οργανισμός έχει εμπλακεί ή η αδυναμία σε ένα προϊόν που μπορεί να έχει επιπτώσεις στη δυνατότητα προώθησης ενός προϊόντος στην αγορά, ο οργανισμός μας μπορούν πάλι να είναι υπεύθυνος για οποιεσδήποτε ζημίες (συμπεριλαμβανομένης της ζημίας της φήμης).

(4) **Αδυναμίες λόγο παρακολούθησης** -- Ο οργανισμός μας μπορεί να μηνυθεί εάν χρήστες του τόπου μας ή αλλού ανακαλύψουν ότι ο οργανισμός ελέγχει τη δραστηριότητα του λογαριασμού τους χωρίς πληροφόρηση των χρηστών.

Δυστυχώς, δεν υπάρχει κανένα σαφές προηγούμενο στις αδυναμίες ή τις ευθύνες των οργανώσεων που εμπλέκονται σε ένα γεγονός ασφάλειας ή στο ποιος πρέπει να συμμετέχει στην υποστήριξη μιας εξεταστικής προσπάθειας. Οι ανακριτές ενθαρρύνουν συχνά τις οργανώσεις να βοηθήσουν στην επισήμανση και τον έλεγχο των εισβολέων.
Πράγματι, οι περισσότεροι ανακριτές δεν μπορούν να κυνηγήσουν τις παραβιάσεις υπολογιστών χωρίς εκτενή υποστήριξη από τις οργανώσεις που ενεπλάκησαν. Εντούτοις, οι ανακριτές δεν μπορούν να παρέχουν προστασία από τις αξιώσεις ευθύνης, και αυτά τα είδη προσπαθειών μπορούν να κρατήσουν για μήνες και να καταβληθεί πολλή προσπάθεια.
Αφ' ετέρου, το νομικό συμβούλιο μιας οργάνωσης πρέπει να δώσει μεγάλη προσοχή και να προτείνει να σταματήσουν οι δραστηριότητες έρευνας και ο εισβολέας να απομακρυνθεί από το σύστημα. Αυτό μπορεί να μην παρέχει προστασία από την ευθύνη, και μπορεί να αποτρέψει τους ανακριτές από τον προσδιορισμό του δράστη.
Η ισορροπία μεταξύ της υποστήριξης της εξεταστικής δραστηριότητας και του περιορισμού της ευθύνης είναι δυσνόητη. Θα πρέπει να εξεταστούν οι συμβουλές της νομικής υπηρεσίας και της ζημίας που ο εισβολέας προκαλεί (ενδεχομένως) κατά τη λήψη της απόφασής για αυτά που γίνονται κατά τη διάρκεια οποιουδήποτε ιδιαίτερου γεγονότος.
Η νομική υπηρεσία πρέπει επίσης να συμμετέχει σε οποιαδήποτε απόφαση να έρθουμε σε επαφή με εξεταστικές αντιπροσωπείες όταν εμφανίζεται ένα γεγονός στον τόπο μας. Η απόφαση να συντονιστούν οι προσπάθειες με τις εξεταστικές αντιπροσωπείες είναι απόφαση του οργανισμού ή της οργάνωσής μας. Η ανάμειξη της νομικής υπηρεσίας θα ενθαρρύνει επίσης τον πολλαπλό συντονισμό μεταξύ του οργανισμού μας και της ιδιαίτερης εξεταστικής αντιπροσωπείας, ο οποίος οδηγεί στη συνέχεια σε μια αποδοτική συνεργασία. Ένα άλλο αποτέλεσμα είναι ότι είναι πιθανό να λάβουμε καθοδήγηση που θα μας βοηθήσει να αποφύγουμε τα μελλοντικά νομικά λάθη.
Τέλος, η νομική υπηρεσία πρέπει να αξιολογήσει τις γραπτές διαδικασίες οργανισμού για την αναφορά γεγονότων. Είναι ουσιαστικό να ληφθεί μια "καθαρή καταγραφή υγείας" από μια νομική προοπτική προτού να πραγματοποιηθούν πραγματικά αυτές οι διαδικασίες.
Είναι ζωτικής σημασίας, κατά την συνεργασία με τις εξεταστικές αντιπροσωπείες, να ελεγχθεί ότι το πρόσωπο που ζητά τις πληροφορίες είναι νόμιμος αντιπρόσωπος της εν λόγω αντιπροσωπείας. Δυστυχώς, πολλοί άνθρωποι με καλές προθέσεις έχουν διαρρεύσει ανεπαίσθητα ευαίσθητες λεπτομέρειες για γεγονότα, που επέτρεψαν πρόσβαση σε αναρμόδιους ανθρώπους στα συστήματά τους, κ.λπ., επειδή κάποιος μπορεί να έχει μεταμφιεστεί ως αντιπρόσωπος μιας κυβερνητικής αντιπροσωπείας.
Είναι επίσης σημαντικό να χρησιμοποιείτε ένας ασφαλής τρόπος επικοινωνίας. Επειδή πολλοί επιτιθέμενοι δικτύων μπορούν εύκολα να επαναδρομολογήσουν e-mail, πρέπει να αποφεύγετε η χρήση ηλεκτρονικού ταχυδρομείου για την επικοινωνία με άλλες αντιπροσωπείες.

Οι μη-εξασφαλισμένες τηλεφωνικές γραμμές (τα τηλέφωνα που χρησιμοποιούνται κανονικά στον επιχειρησιακό χώρο) είναι επίσης συχνοί στόχοι προσβολής από εισβολείς δικτύων.
Δεν υπάρχει κανένα θεσπισμένο σύνολο κανόνων για την απάντηση σε ένα γεγονός όταν αναμιγνύεται η τοπική κυβέρνηση. Κανονικά, εκτός από μια δικαστική απόφαση, καμία αντιπροσωπεία δεν μπορεί να μας αναγκάσει να αποσυνδεθούμε από το δίκτυο, για να αποφύγουμε την τηλεφωνική επαφή με τους πιθανούς επιτιθεμένους, κ.λπ.
Κάθε οργάνωση έχει ένα σύνολο τοπικών και εθνικών νομοθεσιών και κανονισμών που πρέπει να υιοθετηθούν κατά τον χειρισμό των γεγονότων. Συνιστάται κάθε οργανισμός να εξοικειώνεται με εκείνους τους νόμους και κανονισμούς, και να ξέρει τις αντιπροσωπείες που έχουν την αρμοδιότητα πολύ πριν την αντιμετώπιση ενός γεγονότος.

5.3.3 Ομάδες διαχείρισης γεγονότων ασφάλειας υπολογιστών

Υπάρχει αυτήν την περίοδο ένας αριθμός ομάδων απάντησης ασφάλειας υπολογιστών (CSIRTs) όπως το κέντρο συντονισμού CERT, το γερμανικό DFN-CERT, και άλλες ομάδες σε όλο τον κόσμο. Υπάρχουν τέτοιες ομάδες σε πολλές σημαντικές κυβερνητικές αντιπροσωπείες και μεγάλες εταιρίες. Εάν μια τέτοια ομάδα είναι διαθέσιμη, η ειδοποίηση της πρέπει να είναι πρωταρχική μέριμνα κατά τη διάρκεια των αρχικών σταδίων ενός γεγονότος. Αυτές οι ομάδες είναι αρμόδιες για το συντονισμό των γεγονότων ασφάλειας υπολογιστών για μια σειρά περιοχών και μεγαλύτερων οντοτήτων. Ακόμα κι αν το γεγονός θεωρείται ότι έχει περιοριστεί μέσα σε έναν οργανισμό, είναι δυνατό οι πληροφορίες διαθέσιμες μέσω μιας ομάδας απάντησης να μπορούν να βοηθήσουν να επιλυθεί πλήρως το γεγονός.
Εάν καθοριστεί ότι η παραβίαση εμφανίστηκε λόγω μιας βλάβης στο υλικό ή το λογισμικό του συστήματος, πρέπει να ειδοποιηθούν το συντομότερο δυνατόν ο προμηθευτής (ή προμηθευτές) και μια ομάδα διαχείρισης ασφάλειας υπολογιστών. Αυτό είναι ιδιαίτερα σημαντικό επειδή πολλά άλλα συστήματα είναι τρωτά, και αυτές οι οργανώσεις προμηθευτών και ομάδες απάντησης μπορούν να βοηθήσουν και άλλους οργανισμούς που έχουν επηρεαστεί.
Στην οργάνωση μιας πολιτικής περιοχών, μπορεί να είναι επιθυμητό να δημιουργηθεί μια υπό-ομάδα, σαν εκείνες τις ομάδες που υπάρχουν ήδη, η οποία θα είναι αρμόδια για το χειρισμό των γεγονότων ασφάλειας υπολογιστών γιά τον οργανισμό (ή την οργάνωση). Εάν δημιουργηθεί μια τέτοια ομάδα, είναι ουσιαστικό να υπάρχουν γραμμές επικοινωνίας μεταξύ αυτής της ομάδας και των άλλων ομάδων. Μόλις ένα γεγονός είναι εν εξελίξει, είναι δύσκολο να ανοιχτεί ένας ασφαλής διάλογος μεταξύ άλλων ομάδων.

5.3.4 Επηρεασμένοι και αναμεμιγμένοι οργανισμοί

Εάν ένα γεγονός ασκεί επίδραση σε άλλους οργανισμούς, είναι ορθή πρακτική να ενημερωθούν. Μπορεί να είναι προφανές από την αρχή ότι το γεγονός δεν περιορίζεται στον τοπικό οργανισμό, ή μπορεί να προκύψει μόνο μετά από περαιτέρω ανάλυση.

Κάθε οργανισμός μπορεί να επιλέξει να έρθει σε επαφή με άλλους οργανισμούς άμεσα ή μπορούν να περάσουν τις πληροφορίες σε μια κατάλληλη ομάδα απάντησης. Είναι συχνά πολύ δύσκολο να βρεθεί το αρμόδιο POC επί των απομακρυσμένων τόπων και η συναφής ομάδα απάντησης να είναι σε θέση να διευκολύνει την επαφή με τη χρησιμοποίηση των ήδη καθιερωμένων καναλιών.
Τα νομικά ζητήματα και τα ζητήματα ευθύνης που προκύπτουν από ένα γεγονός ασφάλειας διαφέρουν από οργανισμό σε οργανισμό. Είναι σημαντικό να καθοριστεί μια πολιτική για τη διανομή και την καταγραφή των πληροφοριών για άλλους οργανισμούς προτού να εμφανιστεί ένα γεγονός.
Πληροφορίες για συγκεκριμένους ανθρώπους είναι ιδιαίτερα ευαίσθητες, και μπορούν να υπόκεινται στους νόμους μυστικότητας. Για να αποφευχθούν προβλήματα σε αυτόν τον οργανισμό, οι άσχετες πληροφορίες πρέπει να διαγραφούν και πρέπει να περιληφθεί μια δήλωση για το πώς πρέπει να χειριστούν οι υπόλοιπες πληροφορίες. Είναι ουσιαστικό να υπάρξει μια σαφής δήλωση για το πώς αυτές οι πληροφορίες πρόκειται να χρησιμοποιηθούν. Αυτός που ενημερώνει έναν οργανισμό για ένα γεγονός ασφάλειας δε θέλει να διαρρεύσει αυτό στον Τύπο.
Οι ομάδες απάντησης είναι πολύτιμες από αυτή την άποψη. Όταν περνούν τις πληροφορίες σε αρμόδια POCs, είναι σε θέση να προστατεύσουν την ανωνυμία της αρχικής πηγής. Αλλά, πρέπει να γνωρίζουμε ότι, σε πολλές περιπτώσεις, η ανάλυση των αρχείων και των πληροφοριών άλλων τόπων θα αποκαλύψει διευθύνσεις του οργανισμού μας.
Όλα τα προβλήματα που συζητούνται ανωτέρω πρέπει να ληφθούν ως λόγοι να μην αναμιχθούν άλλοι οργανισμοί. Στην πραγματικότητα, η εμπειρία των υπάρχουσων ομάδων αποκαλύπτει ότι οι περισσότεροι οργανισμοί που ενημερώνονται για τα προβλήματα ασφάλειας δεν γνωρίζουν καν ότι ο οργανισμός τους έχει παραβιασθεί. Χωρίς έγκαιρες πληροφορίες, άλλοι οργανισμοί είναι συχνά ανίκανοι να λάβουν μέτρα ενάντια στους εισβολείς.

5.3.5 Εσωτερικές επικοινωνίες

Είναι κρίσιμο κατά τη διάρκεια ενός σημαντικού γεγονότος να υπάρξει ενημέρωση γιατί ορισμένες ενέργειες λαμβάνονται, και πώς αναμένεται από τους χρήστες (ή τμήματα) να συμπεριφερθούν. Ειδικότερα, πρέπει να καταστεί σαφές στους χρήστες τι επιτρέπετε να πουν (και να μην πουν) στον εξωτερικό κόσμο (συμπεριλαμβανομένων άλλων τμημάτων).
Παραδείγματος χάριν, δεν θα ήταν καλό για μια οργάνωση εάν οι χρήστες απαντούσαν στους πελάτες, " λυπούμαστε που τα συστήματα είναι εκτός, είχαμε έναν εισβολέα και προσπαθούμε να επιδιορθώσουμε το πρόβλημα." Θα ήταν πολύ καλύτερο εάν είχαν καθοδηγηθεί να απαντήσουν με μια έτοιμη δήλωση όπως, " λυπούμαστε που τα συστήματά μας δεν είναι διαθέσιμα, αλλά περνούν από συντήρηση για να παρέχουν καλύτερες υπηρεσίες στο μέλλον."
Οι επικοινωνίες με πελάτες και συνεργάτες συμβάσεων πρέπει να αντιμετωπιστούν με έναν λογικό, αλλά ευαίσθητο τρόπο. Κάποιος μπορεί να προετοιμαστεί για τα κύρια ζητήματα με την προετοιμασία ενός πίνακα ελέγχου(checklist). Όταν εμφανίζεται ένα γεγονός, ο πίνακας ελέγχου μπορεί να χρησιμοποιηθεί με την προσθήκη μιας ή δύο προτάσεων για τις συγκεκριμένες περιστάσεις του γεγονότος.
Τα τμήματα δημόσιων σχέσεων μπορούν να είναι πολύ χρήσιμα κατά τη διάρκεια των γεγονότων. Πρέπει να συμμετέχουν σε όλους τους σχεδιασμούς και μπορούν να

δώσουν σωστά δομημένες απαντήσεις για χρήση όταν είναι απαραίτητη η επαφή με εξωτερικά τμήματα και οργανώσεις.

5.3.6 Δημόσιες σχέσεις - δελτία τύπου

Έχει υπάρξει μια τεράστια αύξηση στο μέγεθος κάλυψης που αφιερώνεται σε γεγονότα ασφάλειας υπολογιστών. Τέτοια κάλυψη Τύπου υπάρχει σε όλες τις χώρες δεδομένου ότι το Διαδίκτυο συνεχίζει να αυξάνεται και να επεκτείνεται διεθνώς. Ένα από τα σημαντικότερα ζητήματα που πρέπει να εξεταστούν είναι το πότε, ποίος, και πόσες πληροφορίες πρέπει να απελευθερωθούν στο ευρύ κοινό μέσω του Τύπου.
Υπάρχουν πολλά ζητήματα που πρέπει να εξεταστούν κατά την λήψη απόφασης αυτού του ιδιαίτερου ζητήματος. Πρώτα απ' όλα, εάν υπάρχει ένα γραφείο δημόσιων σχέσεων στον οργανισμό, είναι σημαντικό να χρησιμοποιηθεί ως σύνδεσμος με τον Τύπο. Το γραφείο δημόσιων σχέσεων είναι εκπαιδευμένο στη διατύπωση πληροφοριών που πρέπει να δημοσιευθούν, και βοηθά να βεβαιωθεί ότι η εικόνα του οργανισμού προστατεύεται κατά τη διάρκεια και μετά από ένα γεγονός.
Ένα γραφείο δημόσιων σχέσεων έχει το πλεονέκτημα στο ότι μπορούμε να επικοινωνήσουμε μαζί του κρυφά και να παρέχουμε έναν «ενδιάμεσο» μεταξύ της συνεχής προσοχής του Τύπου και της ανάγκης του POC να διατηρηθεί ο έλεγχος του γεγονότος.
Εάν δεν υπάρχει γραφείο δημοσίων σχέσεων, οι πληροφορίες που θα δημοσιευθούν πρέπει να εξεταστούν προσεκτικά. Εάν οι πληροφορίες είναι ευαίσθητες, μπορεί να είναι συμφέρον να παρασχεθούν ελάχιστες από αυτές ή απλά μια επισκόπηση στον Τύπο. Είναι δυνατό οι οποιεσδήποτε πληροφορίες που παρέχονται στον Τύπο να περάσουν γρήγορα στο δράστη του γεγονότος. Επίσης η παραπλάνηση του Τύπου μπορεί συχνά να αποτύχει και να προκαλέσει περισσότερη ζημία από τη δημοσίευση ευαίσθητων πληροφοριών.
Ενώ είναι δύσκολο να καθοριστεί εκ των προτέρων το επίπεδο λεπτομέρειας που πρέπει να παρασχεθεί στον Τύπο, μερικές οδηγίες που πρέπει να ληφθούν υπόψη είναι ότι πρέπει να:

(1) **Κρατηθεί χαμηλό το τεχνικό επίπεδο λεπτομέρειας.**
Λεπτομερής πληροφορίες για το γεγονός μπορούν να παρέχουν αρκετές πληροφορίες σε άλλους πιθανούς εισβολείς ώστε να προωθήσουν παρόμοιες επιθέσεις σε άλλους οργανισμούς, ή ακόμα και να βλάψουν τη δυνατότητα του οργανισμού να διώξει ποινικώς το ένοχο συμβαλλόμενο μέρος μόλις τελειώσει το γεγονός.

(2)**Κρατηθούν οι υποθέσεις εκτός των δηλώσεων στον Τύπο.**
Υποθέσεις για το ποιος είναι αυτός που προκαλεί το γεγονός ή τα κίνητρα του είναι πολύ πιθανό να είναι εσφαλμένες και μπορεί να προκαλέσουν μια λανθασμένη άποψη του γεγονότος.

(3)**Υπάρχει συνεργασία με τις υπηρεσίες επιβολής νόμου για να βεβαιωθεί ότι τα στοιχεία προστατεύονται.**
Εάν περιλαμβάνεται δίωξη, πρέπει να βεβαιωθεί ότι τα συλλεχθέντα στοιχεία δεν αποκαλυφθούν στον Τύπο.

(4)**Μην γίνει πρόωρη συνέντευξη Τύπου πριν γίνει η κατάλληλη προετοιμασία.**
Ο Τύπος προσπαθεί να πιάσει απροετοίμαστο τον εκπρόσωπο του οργανισμού για να εκμαιεύσει πληροφορίες .

(5) **Μην επιτραπεί στον Τύπου να αποσπάσει την προσοχή από το χειρισμό του γεγονότος.**
Η επιτυχής περάτωση ενός γεγονότος είναι αρχικής σπουδαιότητας.

5.4 Προσδιορισμός ενός γεγονότος

5.4.1 Είναι πραγματικό;

Αυτό το στάδιο καθορίζει εάν ένα πρόβλημα υπάρχει πραγματικά. Πολλά, εάν όχι τα περισσότερα σημάδια που συχνά συνδέονται με τη μόλυνση ιών, παραβίαση συστημάτων, κακόβουλους χρήστες, κ.λπ., είναι απλά ανωμαλίες όπως οι βλάβες υλικού ή η περίεργη συμπεριφορά του συστήματος ή των χρηστών.
Για να καθοριστεί εάν υπάρχει πραγματικά ένα γεγονός, είναι συνήθως χρήσιμο να ληφθεί και να χρησιμοποιηθεί οποιοδήποτε λογισμικό ανίχνευσης που μπορεί να είναι διαθέσιμο. Οι πληροφορίες καταγραφής ελέγχου είναι επίσης εξαιρετικά χρήσιμες, ειδικά στον καθορισμό της ύπαρξης μιας επίθεσης δικτύων.
Είναι εξαιρετικά σημαντικό να ληφθεί μια εικόνα των συστημάτων μόλις υπάρξει υποψία κάποιου λάθους. Πολλά γεγονότα προκαλούν μια δυναμική αλυσίδα γεγονότων, και μια αρχική εικόνα των συστημάτων μπορεί να είναι το πολυτιμότερο εργαλείο για τον εντοπισμό και την αναγνώριση οποιαδήποτε πηγής επίθεσης. Τέλος, είναι σημαντικό να υπάρχει ένα ημερολόγιο το οποίο να καταγράφει γεγονότα από τα συστήματα, τις τηλεφωνικές συνομιλίες κ.λπ., που μπορούν να οδηγήσουν σε έναν γρηγορότερο και συστηματικό προσδιορισμό του προβλήματος, και είναι η βάση για τα επόμενα στάδια χειρισμού.
Υπάρχουν ορισμένες ενδείξεις ή "συμπτώματα" ενός γεγονότος που αξίζουν ιδιαίτερη προσοχή:

(1)Πτώσεις συστημάτων(Systems crashes).

(2)Νέοι λογαριασμοί χρηστών, ή υψηλή δραστηριότητα σε ένα προηγουμένως χαμηλής δραστηριότητας λογαριασμό.

(3) Νέα αρχεία (συνήθως με νέα ή παράξενα ονόματα αρχείων,
όπως data.xx ή το K ή χχ).

(4) Αποκλίσεις ελέγχου (σε ένα σύστημα Unix μπορεί να παρατηρηθεί η μείωση ενός αρχείου ελέγχου αποκαλούμενου/ usr/admin/lastlog, κάτι που πρέπει να μας κάνει να υποψιαστούμε ότι μπορεί να υπάρχει εισβολέας).

(5)Αλλαγές στα μήκη ή τις ημερομηνίες αρχείων (ένας χρήστης πρέπει να θεωρηθεί ύποπτος εάν τα αρχεία .EXE σε έναν υπολογιστή MS-DOS είναι ανεξήγητα αυξημένα πάνω από 1800 bit).

(6)Προσπάθειες δημιουργίας εγγραφών στο σύστημα (ένας διαχειριστής παρατηρεί ότι ένας προνομιούχος χρήστης σε ένα vms σύστημα προσπαθεί να αλλάξει το RIGHTSLIST. DAT).

(7)Τροποποίηση στοιχείων ή διαγραφή (τα αρχεία αρχίζουν να εξαφανίζονται).

(8) Άρνηση υπηρεσίας (διευθυντής συστημάτων και όλοι οι άλλοι χρήστες κλειδώνονται από ένα σύστημα Unix).

(9) Ανεξήγητη, κακή απόδοση συστημάτων

(10) Ανωμαλίες ("GOTCHA" επιδεικνύεται στην κονσόλα ή με την ύπαρξη συχνά ανεξήγητων "ηχητικών σημάτων").

(11)Ύποπτοι έλεγχοι (υπάρχουν πολυάριθμες ανεπιτυχής προσπάθειες σύνδεσης από έναν άλλο κόμβο).

(12) Ύποπτο browsing (κάποιος γίνεται root χρήστης σε ένα σύστημα Unix και έχει πρόσβαση σε αρχεία πολλών λογαριασμών χρηστών.)

(13) Ανικανότητα ενός χρήστη να εισέλθει στο σύστημα λόγω τροποποιήσεων του λογαριασμού του.

Αυτός ο κατάλογος δεν είναι πλήρης, απλώς απαριθμήσαμε διάφορες κοινές περιπτώσεις. Είναι καλύτερο να υπάρξει συνεργασία με ολόκληρο το προσωπικό ασφάλειας υπολογιστών για να ληφθεί μια απόφαση σαν ομάδα για το εάν ένα γεγονός είναι σε εξέλιξη.

5.4.2 Τύποι και πεδίο γεγονότων

Μαζί με τον προσδιορισμό του γεγονότος είναι και η αξιολόγηση του μεγέθους και του αντίκτυπου του προβλήματος. Είναι σημαντικό να προσδιοριστούν σωστά τα όρια του γεγονότος προκειμένου να εξεταστεί αποτελεσματικά και να δοθούν προτεραιότητες στις απαντήσεις.
Προκειμένου να προσδιοριστεί το πεδίο και να δοθεί ένα σύνολο κριτηρίων που να είναι κατάλληλα για τον οργανισμό και για τον τύπο των διαθέσιμων συνδέσεων. Μερικά από τα ζητήματα περιλαμβάνουν τις εξής ερωτήσεις:

(1) Είναι αυτό ένα γεγονός που αφορά πολλούς οργανισμούς;
(2) Έχουν επηρεαστεί πολλοί υπολογιστές του οργανισμού από αυτό το γεγονός;
(3) Περιλαμβάνονται ευαίσθητες πληροφορίες;
(4) Ποιο είναι το σημείο εισόδου του γεγονότος (δίκτυο, τηλεφωνική γραμμή, τοπικό τερματικό, κ.λπ....);
(5) Έχει αναμιχθεί ο Τύπος ;
(6) Ποια είναι η πιθανή ζημία του γεγονότος;
(7) Ποιος είναι ο κατ' εκτίμηση χρόνος αντιμετώπισης του γεγονότος;
(8) Ποιοι πόροι απαιτούνται για να διαχειριστεί το γεγονός;
(9) Έχει αναμιχθεί ο νόμος ;

5.4.3 Αξιολόγηση της ζημίας και της έκτασης της

Η ανάλυση της ζημίας και της έκτασης του γεγονότος μπορεί να είναι αρκετά χρονοβόρα, αλλά μπορεί να οδηγήσει σε κάποια αποκάλυψη για τη φύση του γεγονότος, και να βοηθήσει την έρευνα και την δίωξη. Μόλις εμφανιστεί η παραβίαση, ολόκληρο το σύστημα και όλα τα συστατικά του πρέπει να θεωρούνται ύποπτα. Το λογισμικό συστημάτων είναι ο πιθανότερος στόχος. Η προετοιμασία είναι ένα βασικό βήμα για να είμαστε σε θέση να ανιχνεύσουμε όλες τις αλλαγές σε ένα πιθανώς μολυσμένο σύστημα. Αυτό περιλαμβάνει τον έλεγχο όλων των μέσων από τον προμηθευτή χρησιμοποιώντας έναν αλγόριθμο που είναι ανθεκτικός σε προσπάθειες παραβίασης.
Υποθέτοντας ότι τα αρχικά μέσα διανομής από τους προμηθευτές είναι διαθέσιμα, πρέπει να αρχίσει μια ανάλυση όλων των αρχείων συστημάτων, και οποιεσδήποτε παρατυπίες εμφανιστούν πρέπει να σημειωθούν και να αναφερθούν σε όλα τα συμβαλλόμενα μέρη που συμμετέχουν στο χειρισμό του γεγονότος. Μπορεί να είναι πολύ δύσκολο, σε μερικές περιπτώσεις, να αποφασιστούν ποια εφεδρικά μέσα(backup) παρουσιάζουν μια σωστή θέση του συστήματος.
Παραδείγματος χάριν, το γεγονός μπορεί να είχε συνεχιστεί για μήνες ή έτη πριν από την ανακάλυψη, και ο ύποπτος μπορεί να είναι υπάλληλος του οργανισμού ή να έχει οικεία γνώση ή πρόσβαση στα συστήματα. Σε όλες τις περιπτώσεις, η προ του γεγονότος προετοιμασία θα καθορίσει τη δυνατότητα αποκατάστασης.
Εάν το σύστημα υποστηρίζει κεντρική είσοδο (logging) (τα πιο πολλά μπορούν), επιστρέφουμε σε παλιότερα ημερολόγια και ψάχνουμε για ανωμαλίες. Εάν η διαδικασία ελέγχου και ο έλεγχος χρόνου σύνδεσης είναι ενεργά, ψάχνουμε για σχέδια χρήσης συστημάτων. Σε μικρότερη έκταση, η χρήση των δίσκων μπορεί να ρίξει κάποιο φως στο γεγονός. Ο έλεγχος μπορεί να παρέχει πολλές χρήσιμες πληροφορίες σε μια ανάλυση ενός γεγονότος. Η δυνατότητά να εξεταστούν όλες οι πτυχές ενός συγκεκριμένου γεγονότος εξαρτάται έντονα από την επιτυχία αυτής της ανάλυσης.

5.5 Χειρισμός ενός γεγονότος

Ορισμένα βήματα είναι απαραίτητα να γίνουν κατά τη διάρκεια του χειρισμού ενός γεγονότος. Σε όλες τις σχετικές με την ασφάλεια δραστηριότητες, το σημαντικότερο θέμα που πρέπει να θιγεί είναι ότι όλοι οι οργανισμοί πρέπει να έχουν σε ισχύ πολιτικές(ασφάλειας).
Χωρίς καθορισμένες πολιτικές και στόχους, οι δραστηριότητες που θα αναληφθούν θα παραμείνουν χωρίς εστίαση. Οι στόχοι πρέπει να καθοριστούν από τη διοίκηση και τη νομική υπηρεσία εκ των προτέρων.
Ένας από τους πιο θεμελιώδεις στόχους είναι να αποκατασταθεί ο έλεγχος των συστημάτων που έχουν επηρεαστεί και να περιοριστεί ο αντίκτυπος και η ζημία. Στην χειρότερη περίπτωση, το κλείσιμο του συστήματος, ή η αποσύνδεση του συστήματος από το δίκτυο, μπορεί να είναι η μόνη πρακτική λύση.
Δεδομένου ότι οι δραστηριότητες που περιλαμβάνονται είναι περίπλοκες, πρέπει να παρθεί βοήθεια ανάλογα με τις ανάγκες. Προσπαθώντας να λύσουμε το πρόβλημα μόνοι μας, μπορεί να εμφανιστεί πραγματική ζημία λόγω των καθυστερήσεων ή ελλιπών πληροφοριών. Οι περισσότεροι διαχειριστές παίρνουν την ανακάλυψη ενός εισβολέα ως προσωπική πρόκληση. Αυτό μπορεί να οδηγήσει στην αμέλεια άλλων

στόχων σύμφωνα με τις τοπικές πολιτικές. Η προσπάθεια να πιαστούν οι εισβολείς μπορεί να είναι χαμηλής προτεραιότητας, έναντι της ακεραιότητας των συστημάτων. Παραδείγματος χάριν, η παρατήρηση της δραστηριότητας ενός χάκερ μπορεί να είναι χρήσιμη, αλλά μπορεί να μην θεωρηθεί αξία του κινδύνου για να επιτραπεί η συνέχιση της πρόσβασης του.

5.5.1 Τύποι ενημερώσεων και ανταλλαγή των πληροφοριών

Όταν επιβεβαιωθεί η εμφάνιση ενός γεγονότος, πρέπει να ειδοποιηθεί το κατάλληλο προσωπικό. Το πώς αυτή η ειδοποίηση επιτυγχάνεται είναι πολύ σημαντικό στη διατήρηση του γεγονότος υπό έλεγχο τόσο από μια τεχνική όσο και από μια συναισθηματική σκοπιά. Οι περιστάσεις πρέπει να περιγραφούν με όσο το δυνατόν περισσότερες λεπτομέρειες, προκειμένου να βοηθηθεί η γρήγορη αναγνώριση και η κατανόηση του προβλήματος. Μεγάλη προσοχή πρέπει να λαμβάνεται κατά τον καθορισμό σε ποιες ομάδες δίδονται τεχνικές πληροφορίες κατά τη διάρκεια της ειδοποίησης.

Παραδείγματος χάριν, είναι χρήσιμο να περαστεί αυτό το είδος πληροφοριών σε μια ομάδα διαχείρισης δεδομένου που μπορεί να βοηθήσει με την παροχή χρήσιμων δεδομένων για την διόρθωση αδυναμιών που σχετίζονται με ένα γεγονός. Αφ' ετέρου, η τοποθέτηση κρίσιμης γνώσης σε δημόσιο χώρο (π.χ., μέσω των ομάδων πληροφόρησης USENET ή των καταλόγων διευθύνσεων) μπορεί ενδεχομένως να βάλει έναν μεγάλο αριθμό συστημάτων σε κίνδυνο παραβίασης. Είναι άστοχο να υποτεθεί ότι όλοι οι διαχειριστές που παρακολουθούν μια ιδιαίτερη ομάδα πληροφόρησης έχουν πρόσβαση στον κώδικα πηγής λειτουργικών συστημάτων, ή μπορεί ακόμη και να καταλάβουν μια συμβουλή αρκετά καλά ώστε να λάβουν επαρκή μέτρα.

Καταρχήν, οποιαδήποτε ειδοποίηση οποιουδήποτε είτε εντός είτε εκτός του οργανισμού προσωπικού πρέπει να είναι ρητή. Αυτό απαιτεί οποιαδήποτε δήλωση (είτε πρόκειται για ένα μήνυμα ηλεκτρονικού ταχυδρομείου, τηλεφώνημα, fax, βομβητής, ή semaphone) που παρέχει πληροφορίες για το γεγονός να είναι σαφής, συνοπτική, και πλήρης. Εάν συσταθεί ένα τμήμα εργασίας, είναι χρήσιμο να παρασχεθούν οι πληροφορίες σε κάθε συμμετέχοντα για το τι επιτυγχάνεται σε άλλες προσπάθειες. Αυτό όχι μόνο θα μειώσει την επανάληψη προσπαθειών, αλλά θα επιτρέψει στους ανθρώπους που εργάζονται στα μέρη του προβλήματος να ξέρουν από πού θα λάβουν πληροφορίες σχετικές με το μέρος του γεγονότος που ασχολούνται.

Ένα ακόμη σημαντικό ζήτημα κατά την επικοινωνία είναι να είμαστε απόλυτα ειλικρινείς. Η προσπάθεια να αποκρυφτούν οι πτυχές του γεγονότος με την παροχή ψεύτικων ή ελλιπών πληροφοριών μπορεί όχι μόνο να αποτρέψει μια επιτυχή επίλυση του γεγονός, αλλά μπορεί ακόμη και να επιδεινώσει την κατάσταση.

Η επιλογή της γλώσσας που χρησιμοποιείτε κατά την ειδοποίηση ανθρώπων για το γεγονός μπορεί να έχει βαθιά επίδραση στον τρόπο που παραλαμβάνονται οι πληροφορίες. Όταν χρησιμοποιούνται συναισθηματικοί ή εμπρηστικοί όροι, αυξάνετε η δυνατότητα ύπαρξης ζημιών και αρνητικών εκβάσεων του γεγονότος. Είναι σημαντικό να υπάρξει ηρεμία και στις γραπτές και στις προφορικές επικοινωνίες.

Ένα άλλο ζήτημα είναι ότι δεν μιλούν όλοι οι άνθρωποι την ίδια γλώσσα. Τεχνικό και μη τεχνικό προσωπικό χρησιμοποιούν διαφορετική ορολογία Εξαιτίας αυτού του γεγονότος, μπορούν να προκύψουν παρανοήσεις και καθυστέρηση, ειδικά εάν πρόκειται για ένα πολυεθνικό γεγονός.

Άλλα διεθνή ζητήματα περιλαμβάνουν διάφορες νομικές επιπτώσεις γεγονότων ασφάλειας καθώς και πολιτιστικές διάφορες. Εντούτοις, οι πολιτιστικές διαφορές δεν υπάρχουν μόνο μεταξύ των χωρών. Υπάρχουν ακόμη και μέσα στις χώρες, μεταξύ διαφορετικών κοινωνικών ομάδων ή ομάδων χρηστών.
Παραδείγματος χάριν, ένας διαχειριστής ενός πανεπιστημιακού συστήματος μπορεί να είναι ελαστικός στο ενδεχόμενο προσπάθειας σύνδεσης με το σύστημα μέσω Telnet, αλλά ο διαχειριστής ενός στρατιωτικού συστήματος είναι πιθανό να εξετάσει την ίδια δράση ως μια πιθανή επίθεση.
Ένα άλλο ζήτημα που συνδέεται με την επιλογή γλώσσας είναι η ειδοποίηση του μη τεχνικού ή του εκτός οργανισμού προσωπικού. Είναι σημαντικό να περιγραφεί ακριβώς το γεγονός χωρίς την ύπαρξη αδικαιολόγητου εκνευρισμού ή σύγχυσης. Ενώ είναι δυσκολότερο να περιγραφεί το γεγονός σε ένα μη τεχνικό ακροατήριο, είναι συχνά σημαντικότερο. Μπορεί να απαιτηθεί μια μη τεχνική περιγραφή για την υψηλή διοίκηση, τον Τύπο, ή τις υπηρεσίες επιβολής νόμου.
Η σημασία αυτών των επικοινωνιών δεν πρέπει να υποτιμηθεί και μπορεί να κάνει τη διαφορά μεταξύ της κατάλληλης επίλυσης του γεγονότος και της κλιμάκωσης σε κάποιο πιο υψηλό επίπεδο ζημίας.
Εάν αναμιχθεί μια ομάδα απάντησης, ίσως είναι απαραίτητο να συμπληρωθεί ένα πρότυπο για την ανταλλαγή πληροφοριών. Αν και αυτό μπορεί να φανεί ως ένα πρόσθετο φορτίο και προσθέτει μια ορισμένη καθυστέρηση, βοηθά την ομάδα να ενεργήσει με αυτό το ελάχιστο σύνολο πληροφοριών.
Η ομάδα απάντησης μπορεί να είναι σε θέση να αντιδράσει σε πτυχές του γεγονότος του οποίου ο τοπικός διαχειριστής είναι απληροφόρητος. Εάν οι πληροφορίες δίνονται και σε κάποιο άλλο, οι ακόλουθες ελάχιστες πληροφορίες πρέπει να παρασχεθούν:

(1) Χρονικές ζώνες εισόδου... παγκόσμια ή τοπική ώρα
(2) Πληροφορίες για το απομακρυσμένο σύστημα, συμπεριλαμβανομένων των ονομάτων host (ξενιστών), των διευθύνσεων IP και (ίσως) των Ids των χρηστών
(3) Όλες οι σχετικές καταχωρήσεις εισόδου με τον απομακρυσμένο οργανισμό
(4) Τύπος γεγονότος (τι συνέβη, γιατί πρέπει να ενδιαφερθούμε)

Εάν συμπεριλαμβάνονται τοπικές πληροφορίες (δηλ., τοπικός χρήστης IDs) στις καταχωρήσεις εισόδου, θα είναι απαραίτητο να ελεγχθούν οι καταχωρήσεις για να αποφευχθούν εκ των προτέρων ζητήματα μυστικότητας. Γενικά, πρέπει να δοθούν όλες οι πληροφορίες που μπορούν να βοηθήσουν έναν απομακρυσμένο οργανισμό στην επίλυση ενός γεγονότος, εκτός αν οι τοπικές πολιτικές το απαγορεύουν.

5.5.2 Προστασία στοιχείων και ημερολογίων δραστηριότητας

Κατά την απάντηση σε ένα γεγονός, καταγράφονται όλες οι σχετικές λεπτομέρειες με το γεγονός. Αυτό θα παράσχει πολύτιμες πληροφορίες σε μας και σε άλλους κατά την προσπάθεια να διευκρινιστεί η πορεία των γεγονότων. Η καταγραφή όλων των λεπτομερειών εξοικονομεί τελικά χρόνο. Εάν δεν καταγράφετε κάθε σχετικό τηλεφώνημα, παραδείγματος χάριν, είναι πιθανό να ξεχαστεί μια σημαντική μερίδα των πληροφοριών που λαμβάνετε, οδηγώντας πάλι σε επαφή με την πηγή

πληροφοριών. Συγχρόνως, οι λεπτομέρειες καταγραφής θα παράσχουν στοιχεία για τις προσπάθειες δίωξης..
Η καταγραφή ενός γεγονότος θα βοηθήσει επίσης να εκτελεστεί μια τελική αξιολόγηση της ζημίας (κάτι που η διοίκηση, καθώς επίσης και οι ανώτεροι υπάλληλοι επιβολής νόμου, θα θέλουν να ξέρουν), και θα παράσχει τη βάση για τις επόμενες φάσεις της διαδικασίας διαχείρισης: εξόντωση, αποκατάσταση κ.α
Κατά τη διάρκεια των αρχικών σταδίων ενός γεγονότος, είναι συχνά απραγματοποίητο να καθοριστεί εάν η δίωξη είναι δυνατή, έτσι πρέπει να καταγράφονται στοιχεία όπως στην περίπτωση συγκέντρωσης στοιχείων για μια δικαστική υπόθεση. Πρέπει τουλάχιστον, να καταγραφούν:

(1) Όλα τα γεγονότα συστημάτων (αρχεία ελέγχου)
(2) Όλες οι ενέργειες.
(3) Όλες οι εξωτερικές συνομιλίες (συμπεριλαμβανομένου του προσώπου με το οποίο μιλήσαμε, της ημερομηνίας και του χρόνου, καθώς και το περιεχόμενο της συνομιλίας)

Ο απλούστερος τρόπος για τη διατήρηση τεκμηρίων είναι το κράτημα ημερολόγιου. Αυτό επιτρέπει την πρόσβαση σε μια συγκεντρωμένη, χρονολογική πηγή πληροφοριών όταν χρειάζεται, αντί της απαίτησης έρευνας κάθε σελίδας μεμονωμένων φύλλων εγγράφων. Πολλές από αυτές τις πληροφορίες μπορεί να αποτελέσουν πιθανές αποδείξεις σε ένα δικαστήριο Κατά συνέπεια, όταν υπάρχει δυνατότητα νομικής συνέχισης, πρέπει να ακολουθηθούν έτοιμες διαδικασίες και να αποφευχθεί ο οποιαδήποτε ανάρμοστος χειρισμός των πιθανών στοιχείων ο οποίος θα θέσει την νομική δίωξη σε κίνδυνο. Εάν κριθεί απαραίτητο, μπορούν να ληφθούν τα ακόλουθα μέτρα :

(1) Τακτικά (π.χ., κάθε ημέρα) πρέπει να παραδίδονται φωτοτυπημένα, υπογεγραμμένα αντίγραφα του ημερολογίου (καθώς επίσης και τα μέσα που χρησιμοποιήθηκαν για την καταγραφή των γεγονότων συστημάτων) σε έναν επιστάτη εγγράφων.
(2) Ο επιστάτης πρέπει να αποθηκεύσει αυτά τα αντίγραφα σε μια ασφαλή θέση (π.χ., ένα χρηματοκιβώτιο).
(3) Όταν υποβάλλονται πληροφορίες για αποθήκευση, πρέπει να λαμβάνετε μια υπογεγραμμένη, χρονολογημένη απόδειξη από τον επιστάτη εγγράφων.

Η αποτυχία εφαρμογής αυτών των διαδικασιών μπορεί να οδηγήσει στην ακύρωση οποιωνδήποτε στοιχείων που παρουσιάστηκαν σε ένα δικαστήριο.

5.5.3 Περιορισμός

Ο κύριος στόχος σε αυτή την περίπτωση είναι να περιοριστεί η έκταση μιας επίθεσης. Ένα ουσιαστικό μέρος του περιορισμού είναι η λήψη αποφάσεων (π.χ., ο καθορισμός εάν πρέπει να κλεισθεί ένα σύστημα, να γίνει αποσύνδεση από ένα δίκτυο, να γίνει έλεγχος της δραστηριότητα συστημάτων ή δικτύων, η υιοθέτηση παγίδων, το κλείσιμο λειτουργιών όπως η μακρινή μεταφορά αρχείων, κ.λπ.).

Μερικές φορές αυτή η απόφαση είναι τετριμμένη. Κλείνουμε το σύστημα εάν οι πληροφορίες είναι απόρρητες, ευαίσθητες, ή προσωπικές. Λαμβάνουμε υπόψη ότι η απαγόρευση κάθε πρόσβασης, ενώ ένα γεγονός είναι υπό εξέλιξη, προφανώς ειδοποιεί όλους τους χρήστες, συμπεριλαμβανομένων των υποτιθέμενων χρηστών που δημιουργούν το πρόβλημα, ότι οι διαχειριστές γνωρίζουν ότι υπάρχει πρόβλημα. Αυτό μπορεί να έχει αρνητική επίδραση σε μια έρευνα.
Σε μερικές περιπτώσεις, είναι συνετό να απαγορευθεί κάθε πρόσβαση ή η λειτουργία το συντομότερο δυνατόν, και κατόπιν να αποκαθίσταται η κανονική λειτουργία σε καθορισμένα στάδια. Σε άλλες περιπτώσεις, αξίζει να διακυβευτεί κάποια ζημία στο σύστημα εάν η διατήρηση της λειτουργίας του συστήματος επιτρέψει να προσδιοριστεί ο εισβολέας. Αυτό το στάδιο πρέπει να περιλαμβάνει την πραγματοποίηση των προκαθορισμένων διαδικασιών.
Η οργάνωση ή ο οργανισμός πρέπει, παραδείγματος χάριν, να καθορίσει τους αποδεκτούς κινδύνους όσον αφορά ένα γεγονός, και πρέπει να ορίσει συγκεκριμένες ενέργειες και στρατηγικές. Αυτό είναι ιδιαίτερα σημαντικό όταν είναι απαραίτητη μια γρήγορη απόφαση και δεν είναι δυνατή η προηγούμενη επικοινωνία με όλα τα συμβαλλόμενα μέρη ώστε να συζητηθεί η απόφαση.
Ελλείψει προκαθορισμένων διαδικασιών, το υπεύθυνο πρόσωπο για το γεγονός δεν θα έχει συχνά τη δύναμη να λάβει δύσκολες διοικητικές αποφάσεις (όπως να χαθούν τα αποτελέσματα ενός δαπανηρού πειράματος με τη διακοπή ενός συστήματος). Μια τελική δραστηριότητα κατά τη διάρκεια αυτού του σταδίου διαχείρισης του γεγονότος είναι η ενημέρωση των αρμόδιων αρχών.

5.5.4 Χτυπώντας την αιτία

Μόλις περιορισθεί το γεγονός, είναι καιρός να χτυπηθεί η αιτία. Αλλά πριν γίνει αυτό, πρέπει να ληφθεί μεγάλη προσοχή κατά τη συλλογή όλων των απαραίτητων πληροφοριών για το παραβιασμένο σύστημα και την αιτία του γεγονότος δεδομένου ότι πιθανώς θα χαθούν κατά τον καθαρισμό του συστήματος.
Μπορεί να υπάρχει διαθέσιμο λογισμικό που θα βοηθήσει στη διαδικασία καθαρισμού όπως το λογισμικό antivirus. Εάν έχουν δημιουργηθεί οποιαδήποτε ψευδή αρχεία, πρέπει να αρχειοθετηθούν πριν διαγράφουν. Στην περίπτωση μόλυνσης από ιούς, είναι σημαντικό να καθαριστούν και να επαναμορφοποιηθούν οποιαδήποτε μέσα περιέχουν μολυσμένα αρχεία. Τέλος, πρέπει να εξασφαλιστεί ότι όλα τα αντίγραφα ασφάλειας είναι καθαρά. Πολλά συστήματα που μολύνονται με ιούς περιοδικά επαναμολύνονται απλά επειδή οι άνθρωποι δεν απομακρύνουν συστηματικά τον ιό από τα αντίγραφα ασφάλειας. Μετά από κάθε καθαρισμό του συστήματος, πρέπει να ληφθεί ένα νέο αντίγραφο ασφαλείας.
Η διόρθωση όλων των αδυναμιών μόλις εμφανιστεί ένα γεγονός είναι δύσκολη. Το κλειδί για την διόρθωση των αδυναμιών είναι η γνώση και η κατανόηση της παραβίασης.
Μπορεί να είναι απαραίτητο να επιστραφούν οι αρχικές ρυθμίσεις και να διαμορφωθεί ξανά το σύστημα. Για την αντιμετώπιση της χειρότερης περίπτωσης, πρέπει να διατηρηθεί ένα αρχείο της αρχικής οργάνωσης συστημάτων καθώς και κάθε αλλαγή προσαρμογής. Στην περίπτωση μιας βασισμένης σε δίκτυο επίθεσης, είναι σημαντικό να εγκατασταθούν οι απαραίτητες διορθώσεις για κάθε αδυναμία λειτουργικών συστημάτων που αξιοποιήθηκε.

Όπως αναφέρεται στην παράγραφο 5.4.2, ένα ημερολόγιο ασφάλειας μπορεί να είναι πολυτιμότερο κατά τη διάρκεια της φάσης διόρθωσης των αδυναμιών. Τα ημερολόγια που επιδεικνύουν πώς ανακαλύφθηκε και περιορίστηκε το γεγονός μπορούν να χρησιμοποιηθούν αργότερα για να βοηθήσουν να καθοριστεί πόσο εκτενής ήταν η ζημία από ένα δεδομένο γεγονός.
Τα μέτρα που λαμβάνονται μπορούν να χρησιμοποιηθούν στο μέλλον για να εξασφαλιστεί ότι δεν θα εμφανιστεί πάλι το ίδιο πρόβλημα Ιδανικά, κάποιος θα έπρεπε να αυτοματοποιήσει και να εφαρμόσει τακτικά την ίδια δοκιμή όπως χρησιμοποιήθηκε για να ανιχνευθεί το γεγονός ασφάλειας.

5.5.5 Αποκατάσταση

Μόλις αντιμετωπισθεί η αιτία ενός γεγονότος, η φάση αποκατάστασης καθορίζει το επόμενο στάδιο δράσης. Ο στόχος της αποκατάστασης είναι να επιστρέψει το σύστημα στην κανονική λειτουργία του. Γενικά, η καλύτερη πρακτική είναι να επαναενεργοποιηθούν οι διάφορες υπηρεσίες ανάλογα με τις απαιτήσεις ώστε να ελαχιστοποιηθεί όσο είναι δυνατό η δυσαρέσκεια των χρηστών. Πρέπει να είναι κατανοητό ότι οι κατάλληλες διαδικασίες αποκατάστασης για το σύστημα είναι εξαιρετικά σημαντικές και πρέπει να είναι συγκεκριμένες.

5.5.6 Τελικό στάδιο

Μόλις θεωρηθεί ότι ένα σύστημα είναι πια ασφαλές, είναι δυνατό να υπάρχουν ακόμη τρύπες, και παγίδες, που θα μπορούσαν να βλάψουν το σύστημα. Ένα από τα σημαντικότερα στάδια της απάντησης στα γεγονότα που παραλείπετε πιο συχνά, είναι το «τελικό στάδιο». Στο «τελικό στάδιο», το σύστημα πρέπει να ελεγχθεί για στοιχεία που μπορεί να χάθηκαν κατά τη διάρκεια του σταδίου καθαρισμού. Για αρχή, θα ήταν συνετό να χρησιμοποιηθούν μερικά από τα εργαλεία που αναφέρονται στο κεφάλαιο 7 . Αυτά τα εργαλεία δεν πρέπει να αντικαταστήσουν το συνεχή έλεγχο συστημάτων και τις ορθές πρακτικές διοίκησης συστημάτων.
Το σημαντικότερο στοιχείο του «τελικού σταδίου» εκτελεί μια «μετά το γεγονός» ανάλυση. Ακριβώς τι συνέβη, και σε ποιους χρόνους; Πόσο καλά έδρασε το προσωπικό που ασχολείται με το γεγονός; Ποιο είδος πληροφοριών χρειάστηκε γρήγορα το προσωπικό, και πώς θα μπορούσαν να έχουν πάρει εκείνες τις πληροφορίες το συντομότερο δυνατόν; Τι διαφορετικό θα έκανε το προσωπικό την επόμενη φορά;
Μετά από ένα γεγονός, είναι συνετό να γραφτεί μια έκθεση περιγράφοντας την ακριβή ακολουθία γεγονότων: η μέθοδος ανακάλυψης, η διαδικασία διορθώσεων, η διαδικασίας ελέγχου, και μιας περίληψης εμπειριών που αποκομίσαμε. Αυτό θα βοηθήσει στη σαφή κατανόηση του προβλήματος. Είναι επίσης σημαντική, η δημιουργία ενός επίσημου χρονοδιαγράμματος γεγονότων για νομικούς λόγους.
Μια τελική έκθεση είναι πολύτιμη για πολλούς λόγους. Παρέχει μια αναφορά που χρησιμοποιείται σε περίπτωση άλλων παρόμοιων γεγονότων. Είναι επίσης σημαντικό, να λαμβάνετε όσο το δυνατόν γρηγορότερα μια εκτίμηση του μεγέθους ζημίας που προκάλεσε το γεγονός. Αυτή η εκτίμηση πρέπει να περιλαμβάνει τις δαπάνες που συνδέονται με οποιαδήποτε απώλεια λογισμικού και αρχείων, ζημίας υλικού, και

δαπανών εργατικού δυναμικού για να αποκατασταθούν τα επηρεασμένα αρχεία, να μετατραπούν τα επηρεασθέντα συστήματα, και ούτω καθ' εξής.
Αυτή η εκτίμηση μπορεί να γίνει η βάση για την επίτευξη νομικής δίωξης. Η έκθεση μπορεί επίσης να βοηθήσει να δικαιολογηθεί η προσπάθεια της ασφάλειας υπολογιστών μιας οργάνωσης στη διοίκηση.

5.6 Συνέπειες ενός γεγονότος

Μετά το πέρας του γεγονότος πρέπει να πραγματοποιηθούν, διάφορες ενέργειες. Αυτές οι ενέργειες μπορούν να συνοψιστούν ως εξής:

(1) Πρέπει να ληφθεί ένας κατάλογος των στοιχείων των συστημάτων, (δηλ., μια προσεκτική εξέταση που θα καθορίσει πώς το σύστημα επηρεάστηκε από το γεγονός).

(2) Οι εμπειρίες που αποκομίσθηκαν ως αποτέλεσμα του γεγονότος πρέπει να περιληφθούν στο αναθεωρημένο σχέδιο ασφάλειας ώστε να αποτραπεί επανεμφάνιση του γεγονότος

(3) Μια νέα ανάλυση κινδύνου πρέπει να αναπτυχθεί λαμβάνοντας υπόψη το γεγονός.

(4) Πρέπει να αρχίσει μια έρευνα και μια δίωξη των ατόμων που προκάλεσαν το γεγονός, εάν αυτό κριθεί επιθυμητό.

Μόλις συνέλθει ένας οργανισμός από ένα γεγονός, η πολιτική και οι διαδικασίες πρέπει να αναθεωρηθούν για να καλύψουν τις αλλαγές ώστε να αποτραπούν παρόμοια γεγονότα. Ακόμη και χωρίς την ύπαρξη ενός γεγονότος, θα ήταν συνετό να αναθεωρούνται οι πολιτικές και οι διαδικασίες σε συχνή βάση. Οι αναθεωρήσεις επιβάλλονται επιτακτικά λόγο των σημερινών μεταβαλλόμενων υπολογιστικών περιβαλλόντων.
Ολόκληρος ο σκοπός αυτής της διαδικασίας είναι να βελτιωθούν όλα τα μέτρα ασφάλειας για να προστατευθεί ο οργανισμός από μελλοντικές επιθέσεις.
Ένας οργανισμός ή μια οργάνωση πρέπει να αποκτήσει πρακτική γνώση από αυτή την εμπειρία. Ένας συγκεκριμένος στόχος του απολογισμού είναι να αναπτυχθούν νέες δυναμικές μέθοδοι. Μια άλλη σημαντική απόφαση μπορεί να είναι η εκπαίδευση τελικών χρηστών και διαχειριστών για να αποτραπεί επανεμφάνιση του προβλήματος ασφάλειας.

5.7 Ευθύνες

5.7.1 Καλή συμπεριφορά στο Διαδίκτυο

Κατά τη διάρκεια ενός γεγονότος ασφάλειας υπάρχουν δύο επιλογές. Κατ' αρχάς, ένας οργανισμός μπορεί να επιλέξει να παρατηρεί τον εισβολέα με την ελπίδα της σύλληψης του ή μπορεί να απομακρύνει τον εισβολέα από τα συστήματα το συντομότερο δυνατό . Αυτό είναι μια απόφαση που πρέπει να ληφθεί με πολύ σκέψη, αφού μπορεί να υπάρξουν νομικά μειονεκτήματα αν επιλεχθεί η διατήρηση του

οργανισμού σε λειτουργία, γνωρίζοντας ότι ένας εισβολέας χρησιμοποιεί τον οργανισμό ως βάση προώθησης για να φτάσει σε άλλους οργανισμούς. Η καλή συμπεριφορά στο Διαδίκτυο σημαίνει ότι πρέπει να γίνεται προσπάθεια να προειδοποιηθούν άλλοι οργανισμοί που μπορεί να έχουν χτυπηθεί από κάποιο εισβολέα.

5.7.2 Απάντηση του διαχειριστή στα γεγονότα

Όταν ένα γεγονός ασφάλειας περιλαμβάνει έναν χρήστη, η πολιτική ασφάλειας του οργανισμού πρέπει να περιγράψει ποια μέτρα πρόκειται να ληφθούν. Η καταπάτηση πρέπει να αντιμετωπιστεί σοβαρά, αλλά είναι πολύ σημαντικό να υπάρχει βεβαιότητα για το ρόλο που έπαιξε ο χρήστης. Θα μπορούσε να υπάρξει ένα λάθος στην απόδοση της παραβίασης ασφάλειας σε ένα χρήστη; Η εφαρμογή δράσης από το διαχειριστή υποθέτοντας ότι ο χρήστης προκάλεσε σκόπιμα το γεγονός μπορεί να μην είναι κατάλληλη για έναν χρήστη που μπορεί απλά να έκανε ένα λάθος.
Μπορεί να χρειαστεί να περιληφθούν καταλληλότερες κυρώσεις για μια τέτοια κατάσταση στις πολιτικές μας (π.χ., εκπαίδευση ή επίπληξη ενός χρήστη) ενώ ταυτόχρονα να υπάρχουν πιο αυστηρά μέτρα για τις σκόπιμες πράξεις της κακής χρήσης και παραβίασης των συστημάτων.

Κεφάλαιο 6. Τρέχουσες δραστηριότητες

Σε αυτό το σημείο, ο οργανισμός έχει ενδεχομένως αναπτύξει μια πλήρη πολιτική ασφάλειας και έχει αναπτύξει τις διαδικασίες που θα βοηθήσουν στη διαμόρφωση και τη διαχείριση αυτής της τεχνολογίας. Τα συστήματα και τα δίκτυα δεν είναι ένα στατικό περιβάλλον, έτσι θα πρέπει να αναθεωρούνται οι πολιτικές και οι διαδικασίες σε συχνή βάση. Υπάρχουν διάφορα μέτρα που μπορούν να ληφθούν τα οποία θα βοηθήσουν στην διατήρηση επαφής με τις αλλαγές γύρω μας έτσι ώστε να μπορούν να αρχίσουν οι προβλεπόμενες ενέργειες για την αντιμετώπιση αυτών των αλλαγών.
Το ακόλουθο σύνολο κανόνων είναι γενικό και μπορούμε να προσθέσουμε και άλλους ανάλογα με την περίπτωση για κάθε οργανισμό.

(1) Εγγραφή σε συμβουλευτικά έντυπα που εκδίδονται από διάφορες ομάδες ασφάλειας, όπως εκείνα του κέντρου συντονισμού CERT, και ενημέρωση των συστημάτων ενάντια στις απειλές που υπάρχουν για τα συστήματα του οργανισμού.

(2) Παρακολούθηση των συμπληρωμάτων ασφάλειας(patches) που παράγονται από τους προμηθευτές του εξοπλισμού, και εγκατάσταση τους.

(3) Ενεργή προσοχή στις διαμορφώσεις των συστημάτων για να προσδιοριστούν οποιεσδήποτε αλλαγές που μπορεί να έχουν εμφανιστεί, και έρευνα όλων των ανωμαλιών.

(4) Αναθεώρηση όλων των πολιτικών ασφάλειας και των διαδικασιών ετησίως (τουλάχιστον).

(5) Μελέτη των σχετικών καταλόγων διευθύνσεων και των ομάδων πληροφόρησης USENET για την ενημέρωση των πιο πρόσφατων πληροφοριών που μοιράζονται μεταξύ φιλικών διαχειριστών.

(6) Διεξαγωγή τακτικών έλεγχων ώστε να υπάρχει συμμόρφωση με τις πολιτικές και τις διαδικασίες.

Κεφάλαιο 7. Εργαλεία και τοποθεσίες

Αυτό το κεφάλαιο παρέχει έναν συνοπτικό κατάλογο δημόσια διαθέσιμης τεχνολογίας ασφάλειας που μπορεί να μεταφορτωθεί από το Διαδίκτυο.
Μερικά από τα εργαλεία που απαριθμούνται είναι εφαρμογές όπως προγράμματα τελικών χρηστών (πελάτες) και ενισχυτική υποδομή συστημάτων τους (κεντρικοί υπολογιστές). Άλλα είναι εργαλεία που ένας γενικός χρήστης δεν θα δει ποτέ ή θα πρέπει να χρησιμοποιήσει, αλλά μπορεί να χρησιμοποιηθούν από εφαρμογές, ή από διαχειριστές για να ανιχνευθούν λάθη και προβλήματα ασφάλειας ή για να υπάρξει προστασία ενάντια σε εισβολείς.
Είναι θλιβερό το γεγονός ότι σήμερα υπάρχουν πολύ λίγες ενσυνείδητες εφαρμογές ασφάλειας. Πρώτιστα, αυτό προκαλείται από την ανάγκη για μια υποδομή ασφάλειας που πρέπει πρώτα να ληφθεί, ώστε οι περισσότερες εφαρμογές να λειτουργήσουν ασφαλώς .Ιδιαίτερη προσπάθεια πραγματοποιείται αυτήν την περίοδο για να δημιουργηθεί αυτή η υποδομή έτσι ώστε οι εφαρμογές να μπορούν να εκμεταλλευθούν τις ασφαλείς επικοινωνίες.
Τα περισσότερα από τα εργαλεία και εφαρμογές που περιγράφονται κατωτέρω μπορούν να βρεθούν σε έναν από τους ακόλουθους οργανισμούς αρχείων:

(1)Κέντρο συντονισμού CERT
ftp://info.cert.org:/pub/tools
(2)DFN-CERT
ftp://ftp.cert.dfn.de/pub/tools/
(3) Διαδικασίες υπολογιστών, έλεγχος, και εργαλεία ασφάλειας (COAST)
coast.cs.purdue.edu:/pub/tools

Είναι σημαντικό ότι υπάρχουν πολλοί τέτοιοι οργανισμοί, συμπεριλαμβανομένου του CERT και του COAST, σε όλο το Διαδίκτυο. Πρέπει να υπάρχει προσοχή στη χρήση ενός "καλά γνωστού" οργανισμού για την ανάκτηση λογισμικού, και πρέπει να χρησιμοποιούνται εργαλεία επαλήθευσης (md5 checksums, κ.λπ....) για να επικυρώνετε αυτό το λογισμικό. Ένας έξυπνος cracker μπορεί να διαφημίσει λογισμικό ασφάλειας που έχει σχεδιαστεί σκόπιμα για να παρέχει πρόσβαση στα στοιχεία ή τα συστήματα μας.

Εργαλεία

COPS
DES
Drawbridge
identd (not really a security tool)
ISS
Kerberos
logdaemon
lsof
MD5

PEM
PGP
rpcbind/portmapper replacement
SATAN
sfingerd
S/KEY
smrsh
ssh
swatch
TCP-Wrapper
tiger
Tripwire
TROJAN.PL

Κεφάλαιο 8. Κατάλογοι διευθύνσεων και άλλοι πόροι

Θα ήταν αδύνατο να απαριθμηθούν όλοι οι κατάλογοι και οι πόροι που ασχολούνται με την ασφάλεια οργανισμών. Εντούτοις, υπάρχουν κάποια "σημεία" από τα οποία ο αναγνώστης μπορεί να αρχίσει. Όλες αυτές οι αναφορές ισχύουν για όλο το "ΔΙΑΔΙΚΤΥΟ". Πιο συγκεκριμένοι πόροι μπορούν να βρεθούν μέσα από αυτές τις αναφορές.

8.1 Κατάλογοι διευθύνσεων

(1) CERT(TM) Advisory

Send mail to: cert-advisory-request@cert.org
Message Body: subscribe cert <FIRST NAME> <LAST NAME>
Ένα συμβουλευτικό CERT παρέχει πληροφορίες για το πώς να ληφθεί ένα patch ή ένα σύνολο από λεπτομέρειες για την επίλυση ενός γνωστού προβλήματος ασφάλειας υπολογιστών.
Το Κέντρο Συντονισμού CERT συνεργάζεται με τους προμηθευτές για να παραγάγει λύσεις ή κάποιο patch για ένα πρόβλημα, και δεν δημοσιεύει τις πληροφορίες αδυναμίας μέχρι να βρεθεί κάποια λύση ή όταν ένα patch είναι διαθέσιμο. Ένα συμβουλευτικό CERT μπορεί επίσης να μας προειδοποιήσει για τρέχουσες επιθέσεις (π.χ.,"CA-91:18.Active.Internet.tftp.Attacks).
Συμβουλευτικά CERT δημοσιεύονται επίσης στην ομάδα πληροφόρησης USENET: comp.security.announce. Τα συμβουλευτικά αρχεία CERT είναι διαθέσιμα μέσω του ανώνυμου FTP από info.cert.org in the /pub/cert_advisories directory.

(2) Λίστα VIRUS-L

Send mail to: listserv%lehiibm1.bitnet@mitvma.mit.edu Message Body: subscribe virus-L FIRSTNAME LASTNAME
Το VIRUS-L είναι ένας συγκροτημένος κατάλογος διευθύνσεων με μια εστίαση στα ζητήματα ιών υπολογιστών. Περισσότερες πληροφορίες, συμπεριλαμβανομένου ενός αντιγράφου των οδηγιών επικοινωνίας, βρίσκονται στο αρχείο "VIRUS-L. README", διαθέσιμο από το ανώνυμο FTP cs.ucr.edu.

(3) Firewall Διαδικτύου

Send mail to : majordomo@greatcircle.com
Message Body: subscribe firewalls user@host (ξενιστής)
Ο κατάλογος διευθύνσεων Firewall είναι φόρουμ συζήτησης για τους διαχειριστές και τους εφαρμοστές firewall.

8.2 Ομάδες πληροφόρησης USENET

(1) comp.security.announce
Η ομάδα πληροφόρησης comp.security.announce συγκροτείται
και χρησιμοποιείται απλώς για τη διανομή συμβουλευτικών CERT .

(2) comp.security.misc
Το comp.security.misc είναι φόρουμ για συζήτηση της ασφάλειας υπολογιστών,
ειδικά όπως αυτό αφορά το λειτουργικό σύστημα Unix .

(3) alt.security
Η ομάδα πληροφόρησης alt.security είναι επίσης φόρουμ για
συζήτηση της ασφάλειας υπολογιστών, καθώς επίσης και άλλων
ζητημάτων όπως οι κλειδαριές αυτοκινήτων και τα συστήματα συναγερμών.

(4) comp.virus
Η ομάδα πληροφόρησης comp.virus είναι μια συγκροτημένη ομάδα πληροφόρησης
με μια εστίαση στα ζητήματα ιών υπολογιστών. Για περισσότερες πληροφορίες,
συμπεριλαμβανομένου ενός αντιγράφου
με οδηγίες, δείτε το αρχείο "VIRUS-L. README", διαθέσιμο μέσω του ανώνυμου
FTP στο info.cert.org in the /pub/virus-l directory.

(5) comp.risks
Η ομάδα πληροφόρησης comp.risks είναι ένα ανοικτό φόρουμ
που ασχολείται με κίνδυνους που αφορούν το κοινό σχετικά με υπολογιστικά
συστήματα.

8.3 Σελίδες στο World Wide Web

(1) http://www.first.org/
Σελίδα πόρων ασφάλειας υπολογιστών. Η κύρια εστίαση είναι στις κρίσιμες πληροφορίες απάντησης, πληροφορίες για απειλές, για αδυναμίες, και λύσεις υπολογιστών σχετικές με την ασφάλεια. Συγχρόνως, προσπαθεί να είναι ένας γενικός δείκτης στις πληροφορίες ασφάλειας υπολογιστών για ένα ευρύ φάσμα θεμάτων, συμπεριλαμβανομένων των γενικών κινδύνων, της μυστικότητας, των νομικών ζητημάτων, των ιών, της διαβεβαίωσης, της πολιτικής, και της κατάρτισης.

(2) http://www.telstra.com.au/info/security.html
Αυτή η σελίδα περιέχει έναν κατάλογο συνδέσεων με πηγές πληροφοριών στο δίκτυο και την ασφάλεια υπολογιστών. Δεν υπάρχει καμία υπονοούμενη καταλληλότητα στα εργαλεία, τις τεχνικές και τα έγγραφα που περιλαμβάνονται μέσα σε αυτό το αρχείο. Πολλά εάν όχι όλα αυτά τα στοιχεία λειτουργούν σωστά, αλλά δεν εγγυόμαστε ότι

αυτό ισχύει με απόλυτη βεβαιότητα. Αυτές οι πληροφορίες παρέχονται μόνο για την εκπαίδευση και τη νόμιμη χρήση των τεχνικών ασφάλειας υπολογιστών.

(3) http://www.alw.nih.gov/Security/security.html
Αυτή η σελίδα περιέχει γενικές πληροφορίες για την ασφάλεια υπολογιστών. Οι πληροφορίες οργανώνονται κατά την πηγή και κάθε τμήμα οργανώνεται από το θέμα. Οι πρόσφατες τροποποιήσεις σημειώνονται στη σελίδα των «Νέων».

(4) http://csrc.ncsl.nist.gov/
Αυτό το αρχείο στη σελίδα του Εθνικού Ιδρύματος Προτύπων και Γραφείων Συμψηφισμού των Πόρων Ασφάλειας Υπολογιστών Τεχνολογίας περιέχει διάφορες ανακοινώσεις, προγράμματα, και έγγραφα σχετικά με την ασφάλεια υπολογιστών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

RFCs

- **RFC 2196** - Network Working Group, "Site Security Handbook", B. Fraser, September 1997.
- **RFC 2475** - Network Working Group, "An Architecture for Differentiated Services", S. Blake, D. Blake, M. Carlson, E. Davies, Z. Wang, W. Weiss December 1998.
- **RFC 1704** - Network Working Group, "On Internet Authentication", N. Haller, R. Atkinson, October 1994.
- **RFC 2975** - Network Working Group, "Introduction to Accounting Management", B. Aboba, J. Arkko, D. Harrington, October 2000.
- **RFC 2989** - Network Working Group, "Criteria for Evaluating AAA Protocols for Network Access", B. Aboba, P. Calhoun, S. Glass, T. Hiller, P. McCann, H. Shiino, P .Walsh, G. Zorn, G. Dommety, C. Perkins, B. Patil, D. Mitton, S. Manning, M. Beadles, X. Chen, S. Sivalingham, A. Hameed, M. Munson, S. Jacobs, B. Lim, B. Hirschman, R. Hsu, H. Koo, M. Lipford, E. Campbell, Y. Xu, S. Baba, E. Jaques, November 2000.

BOOKS

- Douglas E. Comer, Δίκτυα και Διαδίκτυα Υπολογιστών, 2001.
- William Stallings, Επικοινωνίες Υπολογιστών και Δεδομένων, 2003.

INTERNET SITES

- Πανεπιστήμιο Μακεδονίας (www.uom.gr)