ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΑΠΟΤΡΟΠΗ ΔΙΑΡΡΟΗΣ ΔΕΔΟΜΕΝΩΝ

Διπλωματική εργασία

του

Θεοφάνη Β. Δημητρίου

Θεσσαλονίκη Ιούνιος 2017

ΑΠΟΤΡΟΠΗ ΔΙΑΡΡΟΗΣ ΔΕΔΟΜΕΝΩΝ

Θεοφάνης Β. Δημητρίου

Απόφοιτος Στρατιωτικής Σχολής Ευελπίδων τάξεως 2001

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ιωάννης Μαυρίδης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 27 Ιουνίου 2017

Ιωάννης Μαυρίδης	Αθανάσιος Μανίτσαρης	Εμμανουήλ Στειακάκης
Καθηγητής	Καθηγητής	Αν. Καθηγητής
.....	.....	.....

Θεοφάνης Β. Δημητρίου

.....

Περίληψη

Η διαρροή ή απώλεια δεδομένων (data leak/loss prevention - DLP) αποτελεί σήμερα ένα σημαντικό πρόβλημα για την ασφάλεια των πληροφοριακών συστημάτων (ΠΣ) των οργανισμών / επιχειρήσεων, αλλά ακόμα και σε ατομικό επίπεδο. Η αποθήκευση τεράστιων όγκων δεδομένων σε διακομιστές (servers) και σε προσωπικούς υπολογιστές ανά τον κόσμο, παρέχει στους διαχειριστές ΠΣ, σημαντικές δυνατότητες για την προστασία της εμπιστευτικότητας όλων των ειδών των δεδομένων είτε είναι προσωπικά, οικονομικά, πολιτικά κ.ά., καθώς πέρα από τις άμεσες επιπτώσεις, μπορούν να προκαλέσουν οικονομικές απώλειες και νομικές κυρώσεις. Ανάλογα με την πληροφορία που υπάρχει μέσα σε αυτά. Για αυτό θεωρείται αναγκαίος ο καθορισμός των βασικών αρχών σχεδίασης και υλοποίησης ΠΣ για την ανίχνευση και την αποτροπή διαρροής ή απώλειας δεδομένων, καθώς επίσης και η αξιοποίηση κατάλληλων τύπων λύσεων DLP.

Στο πλαίσιο αυτής της διπλωματικής εργασίας, θα μελετηθούν με βάση τη διεθνή βιβλιογραφία τα ζητήματα και οι προκλήσεις που σχετίζονται με τη διαρροή / απώλεια δεδομένων, θα εντοπιστούν και θα αξιολογηθούν οι διάφορες τεχνικές και τα εργαλεία ανίχνευσης και αποτροπής διαρροών δεδομένων, στο πλαίσιο διαφορετικών τύπων λύσεων (π.χ. ολοκληρωμένες λύσεις DLP, λύσεις DLP συγκεκριμένων χαρακτηριστικών, λύσεις DLP βάσει καναλιών επικοινωνίας κ.ά.). Ως αποτέλεσμα της αξιολόγησης, θα καταγραφούν τα μειονεκτήματα και τα πλεονεκτήματα που παρουσιάζει κάθε τεχνική κι εργαλείο, με σκοπό την κατάδειξη των χαρακτηριστικών που είναι κρίσιμα για την κατάλληλη λύση ανάλογα με την περίπτωση. Επιπλέον, στο πλαίσιο μιας συγκεκριμένης μελέτης περίπτωσης θα πραγματοποιηθεί η εφαρμογή τεχνικών και εργαλείων, όπως τα OpenDLP και το myDLP, για την προστασίας κειμένων που παράγονται από περιβάλλοντα όπως το LibreOffice.

Λέξεις Κλειδιά

Διαρροή Δεδομένων, Απώλεια Δεδομένων, Ασφάλεια Πληροφοριών, Πληροφοριακά Συστήματα, OpenDLP, myDLP, δεδομένα σε αποθήκευση, δεδομένα σε χρήση, δεδομένα σε κίνηση.

Abstract

Data leak / loss prevention (DLP) constitutes today a major problem for the security of information systems (IT) of organizations or companies, as well as individual. Storing huge volumes of data on servers and personal computers around the world provides IT managers with important capabilities to protect the confidentiality of all kinds of data, whether personal, financial, political or else. That is because they can cause financial losses and legal penalties. Depending on the information within them. Therefore, it is necessary to define the basic principles of design and implementation of the CP for the detection and prevention of leakage or loss of data, as well as the use of suitable types of DLP solutions.

In the context of this thesis, the issues and challenges related to leakage / loss of data will be studied on the basis of the international literature, the various leakage detection and prevention techniques and tools will be identified and evaluated in different types of solutions (DLP integrated solutions, DLP specific features solutions, DLP based communication channels, etc.). As a result of the evaluation, the drawbacks and advantages of each technique and tool will be documented to illustrate the characteristics that are critical to the appropriate solution as the case may be. In addition, in the context of a specific case study, techniques and tools such as OpenDLP and myDLP will be used to protect texts produced by environments such as LibreOffice.

Keywords
Data leakage, data loss, information security, information systems, OpenDLP, myDLP, date in rest, data in use, data in motion.

Πρόλογος – Ευχαριστίες

Ένα ακόμα δύσκολο και απαιτητικό ταξίδι έφτασε στο τέλος του. Σημασία δεν έχει η γραμμή τερματισμού, ούτε το λιμάνι που έφτασες. Σημασία έχει το ταξίδι, πόση πρόοδος και γνώση αποκτήθηκε σε όλα τα επίπεδα. Αισθάνομαι λοιπόν επιτακτική την ανάγκη, όλους όσους συνέβαλαν στο να πραγματοποιηθεί αυτό το εγχείρημα, που πριν λίγα χρόνια έμοιαζε όνειρο απατηλό, να τους ευχαριστήσω από τα βάθη της καρδίας μου.

Πρωτίστως θα ήθελα να ευχαριστήσω τους μικρούς μου μπόμπιρες που έκαναν υπομονή όταν με καλούσαν να παίξουμε και έπρεπε να τους εξηγήσω ότι θα πρέπει να περιμένουν λίγο.

Όλους εκείνους, οι οποίοι με χρειάζονταν και θα έπρεπε να περιμένουν μέχρι να τελειώσω το διάβασμα, τους οφείλω ένα μεγάλο ευχαριστώ. Επίσης να ευχαριστήσω όλους εκείνους όσους με κοιτούσαν περίεργα, σαν να μην το χωράει ο νους τους, στο άκουσμα της λέξης : «...έχω διάβασμα».

Οφείλω να ευχαριστήσω ακόμα όλους τους καθηγητές του τμήματος για την προσπάθεια που καταβάλουν και την υπομονή τους στο να μας μεταδώσουν τις πολύτιμες γνώσεις τους, ώστε να πραγματοποιήσουμε το επόμενο σκαλί της προόδου.

Τέλος, αν και δεν μπορεί να χωρέσει σε μια παράγραφο η εκτίμηση και ο σεβασμός προς το πρόσωπό του, θα ήθελα να ευχαριστήσω θερμά από τα βάθη της καρδιάς μου, τον σημαντικότερο ίσως άνθρωπο που πίστεψε ότι μπορώ να καταφέρω μια τέτοια προσπάθεια, τον καθηγητή μου κύριο Ιωάννη Μαυρίδη, ο οποίος από την πρώτη κιόλας στιγμή, είτε βοηθώντας με, παίρνοντάς με στην κυριολεξία από το χέρι και δείχνοντάς μου πώς πρέπει να διαβάζω, είτε δείχνοντάς μου το σωστό δρόμο της γνώσης, με εμπιστεύθηκε τόσο κατά την ανάθεση, όσο και κατά την εκπόνηση της διπλωματικής εργασίας. Η ανθρωπιά του, οι πολύτιμες γνώσεις του και η καθοδήγησή του με έφεραν στο σημείο αυτό.

Εν κατακλείδι και πάνω από όλα θα μου επιτρέψετε να ευχαριστήσω το Θεό, ο οποίος με προστάτευε, μου έδινε δύναμη και με αξίωσε να φτάσω μέχρι εδώ.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1 : Εισαγωγή

1.1 Γενικά

Καθημερινά γινόμαστε μάρτυρες στον έντυπο ή γραπτό τύπο, καθώς και σε αντίστοιχες ιστοθέσεις στο διαδίκτυο, ζητημάτων που αφορούν την ασφάλεια και την σημασία των πληροφοριών, οι οποίες διαχειρίζονται από αυτοματοποιημένα πληροφοριακά συστήματα. Είναι μεγάλο το πλήθος των περιστατικών που οδήγησαν σε διαρροή δεδομένων προσωπικού χαρακτήρα, σε παραβίαση στοιχείων της ηλεκτρονικής ταυτότητας προσώπων (ακόμα και στοιχείων πιστωτικών καρτών) σε οικονομική απώλεια, σε απώλεια φήμης επιχειρήσεων, σε διαρροή ευαίσθητων πληροφοριών επιχειρηματικής, κυβερνητικής ή ακόμα και στρατιωτικής φύσης, σε δυσλειτουργία τηλεπικοινωνιακών υποδομών, δικτύων παραγωγής και διανομής ενέργειας. Στις περιπτώσεις που τα περιστατικά αυτά έχουν πραγματοποιηθεί με δόλο ή άλλο, μη νόμιμο σκοπό, αναφερόμαστε σε μια κατηγορία εγκλημάτων γνωστή ως «κυβερνοέγκλημα». Σε οικονομικούς όρους, η οικονομική απώλεια λόγω κυβερνοεγκλήματος εκτιμάται σε 100 δις USD το χρόνο για την οικονομία των ΗΠΑ και σε 500 δις USD για την παγκόσμια οικονομία.[1]

1.1.1 Πρόβλημα Ασφαλείας

Γίνεται επομένως εύκολα κατανοητό ότι υπάρχει ένα πρόβλημα σε ότι αφορά την ασφάλεια των πληροφοριών και την προστασία από μια ενδεχόμενη διαρροή καθώς επίσης και από μια ενδεχόμενη εκμετάλλευση αυτή της πληροφορίας για άνομες και παράνομες πράξεις. Επομένως, χρειάζεται να καθορίσουμε και να εντοπίσουμε το πρόβλημα. Το πόσο απαραίτητο και σημαντικό είναι η προστασία της πληροφορίας που αποθηκεύουμε, επεξεργαζόμαστε και μεταδίδουμε.

Η ασφάλεια πληροφοριών νοείται και υπάρχει στο πλαίσιο ενός πληροφοριακού συστήματος. Κατ' επέκταση και η προστασία από μια διαρροή δεδομένων αναφέρεται στο πλαίσιο ενός πληροφοριακού συστήματος. Σύστημα είναι ένα πλήθος αλληλεπιδρώντων στοιχείων, που έχουν οργανικά ταξινομηθεί σε ένα ενιαίο σύνολο έτσι ώστε να εκτελούν μια ορισμένη εργασία και λειτουργία. Πληροφοριακό σύστημα είναι ένα οργανωμένο σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες, δεδομένα), τα οποία αλληλοεπιδρούν μεταξύ τους, καθώς και με το περιβάλλον, και σκοπό έχουν την παραγωγή και διαχείριση πληροφορίας για την υποστήριξη των ανθρωπίνων δραστηριοτήτων στο πλαίσιο ενός οργανισμού, επιχείρησης ή ακόμα και ιδιωτικής ζωής. Επίσης μια άλλη προσέγγιση μπορούμε να αναφέρουμε ότι μια τεχνολογική υποδομή μαζί με ένα οργανωτικό πλαίσιο συγκροτούν ένα πληροφοριακό σύστημα.

Είναι χρήσιμο να τονισθεί ότι τα προβλήματα που προκύπτουν πάνω στην ασφάλεια των πληροφοριών εμφανίζονται όταν προσπαθούμε να πετύχουμε 6 λειτουργικούς στόχους:

[1] Σωκράτης Κ. Κάτσικας: Διαχείριση της Ασφάλειας Πληροφοριών

α. Τα πληροφοριακά συστήματα πρέπει να κάνουν ακριβώς αυτό το οποίο σχεδιάστηκαν.

β. Τα πληροφορικά συστήματα δεν πρέπει ποτέ να κάνουν κάτι για το οποίο δεν έχουν σχεδιαστεί.

γ. Τα πληροφοριακά συστήματα πρέπει να λειτουργούν στον χρόνο που επιβάλλει ο σχεδιασμός τους.

δ. Τα πληροφοριακά συστήματα δεν πρέπει ποτέ να λειτουργούν εκτός του χρόνου για το οποίο σχεδιάστηκαν να λειτουργούν.

ε. Τα πληροφοριακά συστήματα πρέπει να χρησιμοποιούνται μόνο από εξουσιοδοτημένο προσωπικό.

στ. Τα πληροφορικά συστήματα δεν πρέπει ποτέ να χρησιμοποιούνται από μη εξουσιοδοτημένο προσωπικό.

Από όλα τα παραπάνω γίνεται κατανοητό ότι το πρόβλημα ασφαλείας, το οποίο θα μας οδηγήσει σε μια ενδεχόμενη διαρροή δεδομένων, δεν είναι απλώς η προστασία του δικτύου ή του διαδικτύου.

Συνεπώς γίνεται αντιληπτό, τα συστήματα ανίχνευσης παρεισφρήσεων (Intrusion Detection Systems – IDS) ή τα αναχώματα ασφαλείας (firewalls), που θεωρούνται λύσεις ασφαλείας, δεν επαρκούν γιατί εστιάζουν μόνο στο δίκτυο και αγνοούν τα υπόλοιπα (άνθρωπος, υλικό, διαδικασίες). Ο καθένας που μπορεί να ακολουθήσει κάποιες οδηγίες ασφαλείας ή έχει πιστοποιηθεί από πλευράς ασφαλείας δίνοντας του την δυνατότητα να έχει πρόσβαση στα πληροφοριακά του συστήματα, επίσης δεν είναι ενδεδειγμένη λύση, ούτε παρέχει την απαιτούμενη ασφάλεια. Είναι αξιοπρόσεκτο ότι ορισμένες εταιρίες ή οργανισμοί προκειμένου να πραγματοποιήσουν εξοικονόμηση χρημάτων ή ακόμα και λόγο έλλειψης προσωπικού, αναθέτουν την ασφάλεια ενός πληροφοριακού συστήματος σε κάποιο πρόσωπο που δεν έχει άμεση σύνδεση ή εξασφαλισμένη εκπαίδευση και εξειδίκευση. Αυτό σημαίνει ότι το συγκεκριμένο πρόσωπο πέραν των εργασιών που έχει προσληφθεί να εκτελέσει, έχει και επιπλέον εργασία και καθήκοντα.

Επίσης θεωρείται επιβεβλημένο στο σημείο αυτό να τονισθεί ότι το πραγματικό πρόβλημα επικεντρώνεται στο γεγονός της κακής σχεδίασης λογισμικού, της ατελής υλοποίησης και στην μαζική ανάπτυξη κρίσιμων εφαρμογών σε εγγενώς ανασφαλείς πλατφόρμες. Συμπεραίνουμε ότι όλα τα προηγούμενα δεν έχουν συσχέτιση με τα εργαλεία λογισμικού ή τους σχεδιασμούς των δικτύων, αλλά με το πώς σχεδιάζουμε το λογισμικό, ποιοι το σχεδιάζουν και πώς επιλέγουμε να γίνει η εγκατάσταση του λογισμικού σε οργανισμούς, επιχειρήσεις ή και σε ιδιώτες.

1.1.2 Ιστορική Αναδρομή

Στη δεκαετία του ’50 οι υπολογιστικές μηχανές περιείχαν υλικό το οποίο ήταν σχεδιασμένο με αρχιτεκτονικές συνόλου εντολών (Instruction Set Architectures – ISA), δηλαδή το λειτουργικό λογισμικό ξανασχεδιαζόταν για κάθε νέα μηχανή. Συνεπώς δεν υπήρχε η ανάγκη για ασφάλεια στο λειτουργικό λογισμικό, επειδή δεν ήταν εφικτή η απομακρυσμένη πρόσβαση. Η φυσική ασφάλεια του κτηρίου και των υλικών ασφάλιζε και το πληροφοριακό σύστημα.

Στις δεκαετίες ’60 και ’70 αρχίζουν και αναπτύσσονται οι λεγόμενοι “mini – computers” (π.χ. PDP-8, PDP-12 και PDP-11). Η τεχνολογία λειτουργικών συστημάτων αναπτύχθηκε και προχώρησε ένα βήμα παραπέρα και από single-user/batch σε multi-user και time-sharing λειτουργία. Αυτό το γεγονός είχε ως συνέπεια ότι έπρεπε να εφευρεθούν μηχανισμοί οι οποίοι θα εμπόδιζαν τα προγράμματα του ενός χρήστη να παρεμβαίνουν στη λειτουργία των προγραμμάτων άλλων χρηστών. Κατ’ αυτόν τον τρόπο εισήχθη και η έννοια της ασφάλειας, με τη μορφή της προστασίας μνήμης τόσο στο επίπεδο του υλικού όσο και στο επίπεδο λογισμικού. Με αφετηρία το γεγονός αυτό οδηγούμαστε στη γέννηση της ειδικότητας των προγραμματιστών και της επιστήμης των υπολογιστών. Παρατηρείται αύξηση με εντυπωσιακούς ρυθμούς του πλήθους των εγκατεστημένων μηχανών, δημιουργώντας εξάρτηση από την υπολογιστική τεχνολογία στις επιχειρήσεις. Παράλληλα με την εκρηκτική αύξηση των δυνατοτήτων του υλικού, επεκτάθηκαν και οι έννοιες της ασφαλείας. Την εποχή εκείνη το αποτέλεσμα των ερευνητικών προσπαθειών ήταν ο εντοπισμός και η επιδιόρθωση ατελειών ασφαλείας. Δεν είναι υπερβολή να αναφέρουμε ότι αυτή η προσέγγιση δεν χαρακτηρίζεται ως σωστή. Ακόμα και αν διορθωθούν όλες οι εντοπισμένες ατέλειες, κανείς δεν μπορεί να είναι βέβαιος ότι δεν υπάρχουν και άλλες μη εντοπισμένες. Μια ενδεδειγμένη προσέγγιση θα ήταν η ασφάλεια να είναι από την αρχή ένα από τα στοιχεία σχεδιασμού του λειτουργικού συστήματος.

Τη δεκαετία του ’80 το τεχνολογικό άλμα μας έφερε την επανάσταση των προσωπικών υπολογιστών (Personal Computers –PC). Η λιανική αγορά γεμίζει λόγο χαμηλού κόστους. Μπορούμε εύκολα να αντιληφθούμε, ότι λόγο του χαμηλού κόστους οι δυνατότητες είναι περιορισμένες και σχεδόν όλες οι τεχνολογικές εξελίξεις όπως οι τεχνικές διαχείρισης μνήμης, παραλείπονται. Η ασφάλεια του λειτουργικού συστήματος συνειδητά παραλείφθηκε στα PC, όχι μόνο γιατί δεν ήταν απαραίτητη για την χρήση για την οποία σχεδιάστηκε και προοριζόταν να λειτουργήσει αλλά και γιατί θα απαιτούσε την κατανάλωση πολύτιμων πόρων (μνήμη CPU και χώρου στον σκληρό δίσκο).

1.1.3 Δίκτυα Υπολογιστών

Επιπροσθέτως εκείνη την εποχή δίκτυα δεν υπήρχαν, ούτε τα λειτουργικά συστήματα των DOS 2.3 μπορούσαν να δικτυώσουν. Παράλληλα άρχιζε να αναπτύσσεται και το Internet. Ο κεντρικός και ο κυρίως στόχος εκείνη την περίοδο ήταν απλώς όλο το δίκτυο να λειτουργήσει σωστά, μόνο αυτό. Έτσι τα πρώτα πρωτόκολλα ήταν απλά, και στη συνέχεια αυξήθηκε η πολυπλοκότητά τους προκειμένου να μην παρουσιάζονται σφάλματα άρνησης υπηρεσίας. Συνεπώς στα πρώιμα στάδια δινόταν έμφαση σε θέματα όπως η ευκολία της διασύνδεσης, η μέγιστη αξιοποίηση της χωρητικότητας (bandwidth) και η αξιοπιστία της σύνδεσης. Δεν είχε απασχολήσει η ασφάλεια σαν πρόβλημα και κατά συνέπεια αγνοήθηκε. Τα δύο πρωτόκολλα που δημιουργήθηκαν ήταν το TCP (Transmission Control Protocol) και το IP (Internet Protocol). Η πρόσβαση ελεγχόταν σε φυσικό επίπεδο, οπότε παρείχε και την απαιτούμενη ασφάλεια. Το δίκτυο παρουσίαζε την αίτηση πρόσβασης στην κεντρική μηχανή, και η μηχανή ήταν αρμόδια να επιτρέψει ή όχι την πρόσβαση.

Παρόλα αυτά και ενώ η τεχνολογία της δικτύωσης προχωρούσε, τα λειτουργικά συστήματα των PC δεν υλοποιούσαν μηχανισμούς που θα βοηθούσε την δικτύωση, γιατί η σωστή υλοποίηση των μηχανισμών αυτών απαιτούσε την ύπαρξη συγκεκριμένων χαρακτηριστικών στο υλικό της CPU, που δεν διέθεταν τότε οι μικροεπεξεργαστές. Δεν ενσωματώθηκαν στην τότε αρχιτεκτονική των προσωπικών υπολογιστών γιατί ανέβαζαν υπερβολικά το κόστος και δεν ήταν απαραίτητοι για την λειτουργία του υπολογιστή σε οικιακό περιβάλλον.

Κάποια στιγμή η δικτύωση εξαπλώθηκε. Δημιουργήθηκαν και δίκτυα τα οποία συμπεριλάμβαναν τοπικούς υπολογιστές. Αμέσως έγινε αισθητή η ανάγκη για έλεγχο πρόσβασης σε αυτούς τους υπολογιστές. Πλέον έχει σημασία ποιος μπορεί να έχει πρόσβαση σε έναν υπολογιστή και πότε. Ποιος θα μπορούσε να χρησιμοποιήσει έναν συγκεκριμένο πόρο μιας μηχανής και πότε. Τα προνόμια και οι περιορισμοί, τι επιτρέπεται δηλαδή να κάνει κάποιος και πόσο μπορεί να χρησιμοποιήσει έναν πόρο αντίστοιχα απέκτησαν σημασία.

Γίνεται φανερό πλέον ότι το PC χρειαζόταν ασφάλεια την οποία όμως δεν διέθετε. Την συγκεκριμένη χρονική περίοδο το μοναδικό που φάνηκε σαν λύση ήταν να χρησιμοποιηθούν απλοί μηχανισμοί ελέγχου πρόσβασης. Αυτά ήταν τα αναγνωριστικά χρήστη (username) και τα συνθηματικά (password), καθώς και ένα περιορισμένο από πλευράς δυνατοτήτων σύστημα διαχείρισης εξουσιοδοτήσεων. Παρόλες τις προσπάθειες το σύστημα αυτό ήταν ατελείς και κατά συνέπεια ήταν εύκολο να παραβιαστεί. Δεν υπήρχε μηχανισμός ασφαλείας στο λειτουργικό, ούτε ήταν εφικτό να πραγματοποιηθεί κάτι τέτοιο λόγω των χαρακτηριστικών της αγοράς και του πλήθους των εγκατεστημένων μηχανών.

1.1.4 Προσωπικός Υπολογιστής και Υπολογιστής για την Επιχείρηση.

Όπως αναφέρθηκε παραπάνω οι προσωπικού υπολογιστές εμφάνιζαν πολλές αδυναμίες. Παρά το γεγονός αυτό πολλοί υπεύθυνοι πληροφορικής πολλών επιχειρήσεων βρήκαν την τεχνολογία αυτή πολύ ελκυστική, βολική, πιο κατανοητή και κυρίως φθηνότερη. Για να αποκτήσει και να συντηρήσει κάποια επιχείρηση υπολογιστές mainfraime και mini ήταν αρκετά δύσκολο λόγω της συνεχής φροντίδας που χρειαζόταν. Η λογική που επικράτησε τότε, ήταν ότι αν κάτι δούλευε καλά στο σπίτι θα δούλευε καλά και στην επιχείρηση. Κατά αυτό τον τρόπο γίναμε μάρτυρες της μεταφοράς των PC από το σπίτι στην επιχείρηση, συνεπώς και όλων των κρίσιμων πληροφοριακών λειτουργιών, όπως το λογιστήριο ή η μισθοδοσία ή το σχεδιαστήριο κλπ. Εκείνο που έχει ιδιαίτερη σημασία είναι να καταλάβουμε ότι σε έναν προσωπικό υπολογιστή μπορεί να υπήρχαν αρχεία που είχαν μειωμένη αξία για έναν επίδοξο εισβολέα, αλλά όταν στον συγκεκριμένο υπολογιστή, ίδιων δυνατοτήτων δηλαδή, αποθηκευθούν ευαίσθητα δεδομένα μιας επιχείρησης, όπως μια οικονομική προσφορά ή τα σχέδια ενός καινούργιου έργου (project), αμέσως γίνεται ελκυστικό και εύκολος στόχος για όποιον το επιθυμήσει.

Ακόμα και ο πιο αδαής εύκολα μπορεί να συμπεράνει ότι η εξέλιξη αυτή θα παρουσίαζε το εξής πρόβλημα. Οι απαιτήσεις μιας επιχείρησης είναι διαφορετικές

από εκείνες ενός μεμονωμένου χρήστη. Με την αύξηση των αναγκών των επιχειρήσεων αύξαναν και οι υπολογιστικές απαιτήσεις. Δυστυχώς το PC δεν είχε σχεδιαστεί για τέτοιο σκοπό. Οι πωλήσεις των PC στη σημερινή αγορά των οικιακών καταναλωτών ξεπερνούν τις αντίστοιχες πωλήσεις στις επιχειρήσεις κατά ένα μεγάλο βαθμό. Κατά συνέπεια όλα καθορίζονται από τις προτεραιότητες και τις απαιτήσεις του οικιακού υπολογιστή. Ενώ οι επιχειρήσεις ζητούν και απαιτούν συστήματα ασφαλέστερα, η αγορά και οι κατασκευαστές δεν τα παρέχουν γιατί ακούνε την αγορά των οικιακών καταναλωτών. Είναι γεγονός ότι για να δημιουργηθεί αποτελεσματική ασφάλεια θα πρέπει να αλλάξει εκ βάθρων η σχεδίαση του PC. Κάτι τέτοιο γίνεται αντιληπτό ότι δεν πρόκειται να πραγματοποιηθεί λόγω του πλήθους των μηχανών που υπάρχουν και των χαρακτηριστικών της αγοράς.

Συμπερασματικά είμαστε σε θέση να κατανοήσουμε πλέον ότι η κατάσταση με την οποία ερχόμαστε αντιμέτωποι πολλές φορές στην σημερινή εποχή, οφείλεται στο ότι αναπτύσσουμε κρίσιμες εφαρμογές σε εγγενώς ανασφαλή περιβάλλοντα.

1.2 Η Σημαντικότητα του προβλήματος

Με την ανάπτυξη των πληροφοριακών συστημάτων και την εδραίωση της ψηφιακής εποχής κατά τις τελευταίες δεκαετίες, ο ατομικός, ο επιχειρηματικός και ο εθνικός πλούτος εξαρτώνται όλο και περισσότερο ως συνάρτηση των ψηφιακών πληροφοριών. Η ανάπτυξη και η παραγωγή των δύο τρίτων περίπου της οικονομίας βασίζονται σε τομείς της βιομηχανίας ή των υπηρεσιών οι οποίοι εξαρτώνται σε πολύ μεγάλο βαθμό από τις τεχνολογίες πληροφοριών και επικοινωνιών. Το σημαντικότερο όλων είναι η χρησιμοποίηση της πληροφορίας για σωστή αξιολόγηση των μελλοντικών αποφάσεων ώστε να επιτευχθούν οι προσωπικοί, οι επιχειρηματικοί ή οι εθνικοί στόχοι.

Η ανάπτυξη συνεπώς της οικονομίας της οικονομίας βασίζεται σε μεγάλο βαθμό στις αυξημένες δυνατότητες συλλογής, επεξεργασίας, αποθήκευσης και μετάδοσης πληροφοριών που παρέχουν οι σύγχρονες τεχνολογίες πληροφοριών και επικοινωνιών.

Στο σημείο αυτό θα πρέπει να αναφέρουμε το πώς συμπεριφερόμαστε στην πληροφορία. Δηλαδή αν την θεωρούμε αγαθό ή όχι.

Ένα αγαθό το οποίο έχει και υλική υπόσταση το διαθέτει στην αγορά ένας καταστηματάρχης. Σύμφωνα με το μοντέλο αυτό ο εκάστοτε καταστηματάρχης αγοράζει τα υλικά αυτά πληρώνοντας κάποιο κόστος. Στη συνέχεια τα πουλάει, μειώνεται το απόθεμά του, βγάζει την αξία του υλικού και ενδεχομένως και ένα κέρδος. Ο πελάτης φεύγει με το υλικό που έχει πληρώσει την αξία του και το οποίο του δίνεται η δυνατότητα να μεταπωλήσει.

Στο μοντέλο του παρόχου υπηρεσιών δηλαδή ενός ιατρού, μηχανικού κλπ, το αγαθό που πουλιέται και έχει αξία είναι ο χρόνος και οι ειδικές γνώσεις που διαθέτει ο πάροχος. Εύκολα λοιπόν οδηγούμαστε στο συμπέρασμα ότι η σημαντική διαφορά με το παραπάνω μοντέλο είναι ότι ο χρόνος μπορεί να πουληθεί μόνο μια φορά και δεν μπορεί να μεταπωληθεί.

Φτάνοντας τώρα στο σημείο να διερευνήσουμε εάν η πληροφορία είναι αγαθό, θα πρέπει να αναζητήσουμε αν είναι δυνατόν να αποτελέσει αντικείμενο οικονομικής συναλλαγής, αν έχει δηλαδή αξία. Εύκολα γίνεται κατανοητό ότι οι επενδυτές θα πλήρωναν για να αποκτήσουν πληροφορίες σχετικά με το ύψος της τιμής που θα διαμορφώσει μια μετοχή ή οι επιχειρηματίες για να μάθουν τα σχέδια των ανταγωνιστών τους. Επομένως η πληροφορία από την στιγμή που μπορεί να αποτελέσει αντικείμενο οικονομικής συναλλαγής, είναι λογικό να δεχθούμε ότι αποτελεί αγαθό και έχει οικονομική αξία. Συνεπώς θα πρέπει να αναλογιστούμε αν η αξία είναι μετρήσιμη και πώς μπορεί να μετρηθεί. Στο σημείο αυτό χρήσιμο είναι να επισημάνουμε ένα χαρακτηριστικό της πληροφορίας το οποίο είναι σε θέση να διαμορφώσει πολλές φορές την αξία της. Το γεγονός ότι η πληροφορία δεν καταναλώνεται, μας οδηγεί στο συμπέρασμα ότι μπορεί να πουληθεί δηλαδή περισσότερες από μία φορές από τον ιδιοκτήτη της.

1.2.1 Αξία της Πληροφορίας

Επεκτείνοντας το συλλογισμό μας για το αν η αξία της πληροφορίας είναι μετρήσιμη, οδηγούμαστε στο συμπέρασμα ότι η αξία της είναι μετρήσιμη:

1. Η συλλογή, δημιουργία ή συντήρηση της πληροφορίας συνεπάγεται κόστος. Δηλαδή κάποιος ο οποίος θα αποκτήσει, είτε από αγορά είτε θα είναι προϊόν ανάλυσης, είτε θα κατασκευάσει από την αρχή μια πληροφορία, συνδέοντας δεδομένα μεταξύ τους θα χρειαστεί να παρέχει κάποιο τίμημα. Οδηγούμαστε κατά αυτόν τον τρόπο στο συμπέρασμα ότι έχει αξία για τον κάτοχό της.
2. Η πληροφορία έχει αξία για αυτούς στους οποίους ανήκει, αυτούς που την φυλάσουν, αυτούς που την χρησιμοποιούν και αυτούς που την χρησιμοποιούν. Γίνεται φανερό ότι ένας υπάλληλος του τμήματος προσωπικού ο οποίος χρησιμοποιεί τα δεδομένα της πληροφορίας που αφορά τα προσωπικά στοιχεία ενός υπαλλήλου μιας εταιρίας ή οργανισμού έχει κόστος και κατά συνέπεια αξία λόγο της φύσης των δεδομένων.
3. Το κόστος και η αξία της πληροφορίας υπάρχουν ήδη στον πραγματικό κόσμο.

Από τα παραπάνω οδηγούμαστε στο συμπέρασμα ότι η πληροφορία έχει και κόστος ή αξία ή μπορεί και τα δύο. Η αξία μιας πληροφορίας μπορεί να διαμορφωθεί από μια σειρά από παράγοντες:

1. Η αποκλειστική κατοχή.
2. Η χρησιμότητα.
3. Το κόστος δημιουργίας ή απόκτησης.
4. Η αστική ή άλλη νομική ευθύνη.
5. Η μετατρεψιμότητα ή διαπραγματευσιμότητα.
6. Η επιχειρηματική σημασία.

Επομένως πληροφορία που είναι χρήσιμη έχει αξία τουλάχιστον ίση με τη χρήση που θα της γίνει.

Επιπροσθέτως η πληροφορία επίσης μπορεί να περιέχει σχέση εμπιστοσύνης, λόγω προσωπικής, επιχειρηματικής ή της εθνικής φύσης. Κατά συνέπεια ο κάτοχός της μπορεί να υπέχει και νομική ευθύνη στην περίπτωση που αποτύχει να την προστατέψει.

1.2.2 Κοινωνική Σημασία

Αξίζει στο σημείο αυτό να αναφερθεί ότι η πληροφορία μπορεί να αποτελέσει και ισχυρό όργανο κοινωνικού ελέγχου. Η κατοχή πληροφορίας αποτελούσε συγκριτικό πλεονέκτημα για το άτομο ή την κοινωνική ομάδα που κατείχε την πληροφορία. Όσοι κατείχαν καλύτερη πληροφόρηση ήταν σε πλεονεκτικότερη θέση έναντι των υπολοίπων. Οι σημερινές δυνατότητες των τεχνολογιών πληροφοριών και επικοινωνιών μέσα στις δεδομένες κοινωνικές συνθήκες επιτρέπουν τη συγκέντρωση, επεξεργασία, αποθήκευση και μετάδοση μεγάλου όγκου πληροφοριών. Αυτό το γεγονός μας οδηγεί στην ενοποίηση και ολοκληρωμένη παράθεσή τους, στη συνδυασμένη χρήση πληροφοριών που συλλέχθηκαν ενδεχομένως για διαφορετικούς σκοπούς, ή στη λήψη αποφάσεων αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας πληροφοριών επιτρέποντας έτσι την άσκηση ελέγχου ή παρακολούθησης των δραστηριοτήτων ατόμων ή ακόμη και ολόκληρων κοινωνικών ομάδων. Με την βοήθεια εξιδεικευμένων λογισμικών και εφαρμογών μπορεί να δημιουργηθεί για παράδειγμα το καταναλωτικό προφίλ ενός ατόμου, από τις αναρτήσεις του ή τις επισκέψεις οι οποίες κοινοποιούνται μέσω κοινωνικών δικτύων. Επίσης πληροφορίες που αφορούν την οικονομική κατάσταση, το ποινικό μητρώο, κατάσταση της υγείας κλπ., μπορούν να γίνουν πολύ συχνά αντικείμενο καταχρηστικής αξιοποίησης. Αυτό θα είχε αποφευχθεί στην περίπτωση που αυτές οι πληροφορίες δεν συλλέγονταν. Η αποχή όμως από τη συλλογή πληροφοριών δεν αποτελεί στην πραγματικότητα λύση στο πρόβλημα της κατάχρησης της πληροφορίας για καμιά σύγχρονη κοινωνία.

Η επιβολή κανόνων και πρακτικών που θα εξασφαλίζουν όσο είναι αυτό δυνατό την κοινωνικά αποδεκτή χρήση των πληροφοριών, είναι μία λύση.

Έχει επικρατήσει να αναφερόμαστε και να γράφουμε για την ασφάλεια των πληροφοριών. Για να διασφαλιστεί όμως μία πληροφορία αυτό μπορεί να είναι δύσκολο ή ακόμη και αδύνατο. Ο συγκεκριμένος στόχος μπορεί να επιτευχθεί της διασφάλισης των πληροφοριών με έναν πιο άμεσο και ευκολότερο να επιτευχθεί στόχο. Η προστασία και η διασφάλιση των δεδομένων. Θα πρέπει να διευκρινίσουμε την διαφορά μεταξύ πληροφοριών και δεδομένων η οποία είναι πολύ λεπτή[2].

Τα δεδομένα είναι ένα σύνολο καταγεγραμμένων συμβόλων. Πληροφορία είναι τα δεδομένα μαζί με την υποκειμενική ερμηνεία τους. Η την ερμηνεία που ενδεχομένως να κληθούμε να δώσουμε και στην συνέχεια να την αποθηκεύσουμε με την μορφή δεδομένων. Οπότε μπορούμε να πούμε ότι τα δεδομένα περιέχουν τις πληροφορίες σε ψηφιακή συνήθως μορφή.

[2] Θα αναφερόμαστε στην πληροφορία και στα δεδομένα σαν έννοιες ταυτόσημες, από την στιγμή που η ασφάλεια των δεδομένων συνεπάγεται και την ασφάλεια της πληροφορίας που αυτά περιέχουν.

1.3 Σκοπός και Στόχοι.

Από όλα τα παραπάνω που έχουμε ήδη αναφέρει περιληπτικά γίνεται φανερό ότι χρειάζεται η αλλαγή προσέγγισης που ενδεχομένως να απαιτείται να υιοθετηθεί από τους οργανισμούς, τις επιχειρήσεις ή ακόμα και από ένα άτομο προσωπικά. Οι ανησυχίες των επιχειρήσεων, των οργανισμών και των ιδιωτών σχετικά με την ανάγκη για καλύτερο έλεγχο και την προστασία των ευαίσθητων πληροφοριών έχουν οδηγήσει σε μια νέα σειρά λύσεων που στοχεύουν στην αύξηση της ικανότητας μιας επιχείρησης για την προστασία των περιουσιακών στοιχείων πληροφόρησης.

Σκοπός της παρούσας διπλωματικής είναι:

1. Η επισήμανση και η αναφορά σε ότι αφορά την προστασία των πληροφοριών και των δεδομένων.
2. Η εφαρμογή και η παρουσίαση της τεχνολογίας DLP καθώς και ο τρόπος με τον οποίο αποτρέπει τη διαρροή των εμπιστευτικών αρχείων μιας επιχείρησης με οποιονδήποτε τρόπο (όπως USB sticks, e-mail, bluetooth, print, FTP, copy, P2P, file share, κλπ) εκτός του εταιρικού δικτύου, ενώ παράλληλα παρέχεται η δυνατότητα ελέγχου χρήσης τους από εξουσιοδοτημένο προσωπικό.
   Πραγματοποίηση μιας αναφοράς του γενικότερου πλαισίου που έχει ως κύριο στόχο την προστασία των πληροφοριών και ειδικότερα κατ' επέκταση την πρόληψη διαρροής των δεδομένων (θεσμικές, οργανωτικές, κοινωνικές).
3. Πως μπορεί να πραγματοποιηθεί μια στρατηγική και κατ' επέκταση η εφαρμογή της (πχ δημιουργία Σχεδίων, αντιμετώπιση περιστατικών κλπ)
4. Παρουσίαση λογισμικών ανοικτού κώδικα καθώς και μια εφαρμογή παραδειγμάτων, πώς μπορεί να διαχειριστεί παρόμοιες καταστάσεις και με ποιον τρόπο.
5. Καταγραφή από την χρησιμοποίηση των λογισμικών κατά την εφαρμογή τους.

Στόχος είναι ο καθορισμός των ευαίσθητων πληροφοριών καθώς και ο τρόπος αντιμετώπισής τους. Αρχικός στόχος είναι η ευαισθητοποίηση της διοίκησης των επιχειρήσεων και του αντίστοιχου προσωπικού που χειρίζεται παρόμοιες πληροφορίες και δεδομένα ενώ στη συνέχεια οι τεχνικές, οι στρατηγικές και γενικότερα οι πολιτικές ασφαλείας που θα εφαρμοστούν σε έναν οργανισμό ή μια επιχείρηση, ανάλογα φυσικά με το επίπεδο και τον τομέα ενασχόλησης τους.

Καταγραφή με ποιον τρόπο μπορεί να διαχειριστεί μια παρόμοια κατάσταση ανάλογα με την κάθε περίπτωση, ποια λογισμικά υπάρχουν, εφαρμόζοντας παραδείγματα και για τα δύο που χρησιμοποιήθηκαν.

1.4 Αναγκαιότητα και Σπουδαιότητα της Προστασίας Απώλειας Δεδομένων.

Κάθε οργανισμός, ανεξαρτήτως είδους και μεγέθους, συλλέγει, επεξεργάζεται, αποθηκεύει και μεταδίδει μεγάλους όγκους δεδομένων. Σε μια καθημερινή ημέρα, σημαντικός όγκος δεδομένων πληροφοριών διακινείται ανάμεσα στα μέλη μιας επιχείρηση ή ακόμα και σε τρίτους, τόσο στο εσωτερικό της δίκτυο, όσο και εξωτερικά από αυτό. Επιπλέον, αναγνωρίζει ότι η πληροφορία και οι σχετικές με αυτήν διεργασίες, τα σχετικά συστήματα, δίκτυα και οι άνθρωποι συνιστούν σημαντικούς πόρους για την ικανοποίηση των στόχων του. Παράλληλα όμως γίνεται φανερό ότι οι πόροι αυτοί είναι εκτεθειμένοι σε κινδύνους που απειλούν την καλή λειτουργία τους. Ένας από αυτούς τους κινδύνους είναι και η διαρροή των δεδομένων. Οι γνωστοί δίαυλοι επικοινωνίας στους οποίους αναφερόμαστε είναι το ηλεκτρονικό ταχυδρομείο, (e-mail), έγγραφα κειμενογράφου (word), υπολογιστικά φύλλα (excel), αρχεία βάσης δεδομένων καθώς και άμεσα μηνύματα. Μπορούμε να παρατηρήσουμε ότι ο κυριότερος και μεγαλύτερος όγκος είναι αβλαβή τόσο για μια επιχείρηση όσο και για έναν ιδιώτη. Παρόλα αυτά ορισμένα δεδομένα μπορούν να χαρακτηριστούν ως «ευαίσθητα», «προσωπικά» ή «ιδιόκτητα» (πνευματική ιδιοκτησία), κάνοντάς μας κατανοητό ότι οι εν λόγω πληροφορίες είναι επιβεβλημένο να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, έκθεση ή διακίνηση. Η επιβολή (ή η ανάγκη) της προστασίας των δεδομένων μπορεί να οδηγείται από εξωτερικούς παράγοντες όπως είναι η προστασία της ιδιωτικής ζωής ή νομοθετικών ρυθμίσεων ή εσωτερικά λαμβάνοντας ως γνώμονα τους επιχειρηματικούς στόχους για την προστασία οικονομικών, στρατηγικών ή άλλους τύπους πληροφοριών από τους ανταγωνιστές.

Η παραβίαση και η γνωστοποίηση των δεδομένων αυτών σε αναρμόδια ή μη εξουσιοδοτημένα πρόσωπα ή και στην χειρότερη περίπτωση ακόμα και στους ανταγωνιστές μας, υπήρξε ένας από τους μεγαλύτερους φόβους που αντιμετωπίζουν οι οργανισμοί, επιχειρήσεις και ιδιώτες στις μέρες μας.

Στο σημείο αυτό θα πρέπει να γίνει κατανοητό, ότι δεν έχει σημασία πόσο ισχυρή είναι η τεχνολογία που χρησιμοποιούμε ή πόσο έντονη είναι η παρακολούθηση από τα συστήματα παρακολούθησης (ή συστήματα ανίχνευσης εισβολών), τα δεδομένα, στα οποία συμπεριλαμβάνεται και τα στοιχεία πνευματικής ιδιοκτησίας μπορούν να βρουν έναν τρόπο να διαρρεύσουν εκτός σε λιγότερο ασφαλή συστήματα και συσκευές στις οποίες δεν προοριζόταν να αποθηκευτεί αρχικά. Τέτοιες διαρροές δημιουργούν σημαντικό κίνδυνο στις επιχειρήσεις, οργανισμούς, ιδιώτες αλλά και στους πελάτες ή στους επιχειρηματικούς εταίρους επηρεάζοντας αρνητικά τη φήμη της επιχείρησης, τη συμμόρφωση, το ανταγωνιστικό πλεονέκτημα, τα οικονομικά καθώς και την εμπιστοσύνη των πελατών και των επιχειρηματικών συνεργασιών.

Οι προκλήσεις αυτές δημιούργησαν την ανάγκη για καλύτερο έλεγχο και προστασία των ευαίσθητων δεδομένων, έχουν οδηγήσει σε μια σειρά λύσεων που στοχεύουν στην αύξηση της ικανότητας μιας επιχείρησης για την προστασία των περιουσιακών στοιχείων πληροφόρησης.

Εύκολα οδηγούμαστε στο συμπέρασμα για την ιδιαίτερη προσοχή που πρέπει να δείξουμε ώστε η πρόληψη όλων των δυσμενών συνθηκών που ενδεχομένως να μας οδηγήσει μια παράβλεψη στο πληροφοριακό μας σύστημα να έχει προβλεφθεί και να αντιμετωπιστεί πριν ακόμα είναι πολύ αργά.

Κεφάλαιο 2 : Ασφάλεια Πληροφοριών

2.1 Εισαγωγή

Η ασφάλεια πληροφοριακών συστημάτων σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Άμεση σχέση έχει επίσης και η δυνατότητα να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι αποθηκευμένες στο σωστό σημείο, διακινούνται με τον τρόπο που έχει καθοριστεί από τις πολιτικές ασφαλείας και είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Είναι εύλογο ότι για να πραγματοποιηθεί αυτό απαιτείται η ικανότητα εφαρμογής μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, την σωστή και συνεχή λειτουργία του υπολογιστικού συστήματος, την σωστή αποθήκευση των δεδομένων ανάλογα με την φύση των πληροφοριών που διαθέτουν και την σωστή μεταβίβασή τους.

Με αυτό τον τρόπο και επεκτείνοντας τη σκέψη μας σε ότι αφορά την ασφάλεια των πληροφοριακών συστημάτων μπορούμε να θεωρήσουμε ότι αυτή έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών, οι οποίες μπορεί πολλές φορές να γίνονται είτε από άγνοια, είτε από λαθεμένη εκπαίδευση και γνώση, είτε από βιασύνη, είτε και σκόπιμα, από τους χρήστες ενός υπολογιστικού συστήματος καθώς και την λήψη μέτρων ώστε να πραγματοποιηθεί η ακεραιότητα του συστήματος.

Ο οργανισμός είναι σε θέση να ελαττώσει τον βαθμό κινδύνου, εφαρμόζοντας ορισμένα μέτρα ασφαλείας. Η πληροφορία αποτελεί περιουσιακό στοιχείο του οργανισμού. Συνεπώς είναι η προστασία του αποτελεί ευθύνη της διοίκησης. Οπότε το πρόγραμμα προστασίας των πληροφοριών είναι μια επιχειρησιακή διεργασία σχεδιασμένη ώστε να παρέχει στην διοίκηση τα μέσα για να μπορέσει να ασκήσει τα καθήκοντα της. Καταλήγουμε συνεπώς στο συμπέρασμα ότι η ασφάλεια πληροφοριών δεν είναι αμιγώς τεχνικό θέμα, αλλά κυρίως θέμα ανθρώπων και θέμα διαχείρισης.

Τόσο οι κίνδυνοι όσο και η αποτελεσματικότητα των μέτρων ασφαλείας αλλάζουν με τον χρόνο, ανάλογα με τις συνθήκες που επικρατούν στον οργανισμό. Συνεπώς οφείλουμε να παρακολουθούμε και να αξιολογούμε συνεχώς την αποτελεσματικότητα των εγκατεστημένων μέτρων ασφαλείας, να εξετάζουμε εάν υπάρχουν νέοι κίνδυνοι και να τους αναλύουμε, να επιλέγουμε και να υλοποιούμε κατάλληλα μέτρα ασφαλείας ή να βελτιώνουμε ήδη υπάρχοντα όταν χρειάζεται.

Συγκεκριμένα η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με :

1. Πρόληψη (prevention): Την λήψη δηλαδή μέτρων για να προβλεφθούν προβλήματα και ενδεχόμενες απειλές που μπορεί να δεχθεί ένα πληροφοριακό σύστημα.
2. Ανίχνευση (detection): Την λήψη μέτρων για την ανίχνευση του χρόνου, του πώς, και από ποιον συγκεκριμένα προκλήθηκε το πρόβλημα σε ένα συστατικό του πληροφοριακού συστήματος.

3. Αντίδραση (reaction): Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός πληροφοριακού συστήματος.

Ειδικότερα η ασφάλεια μπορεί να θεωρηθεί ότι αποτελείται από δύο κύριες κατευθύνσεις, την προστασία και τον έλεγχο. Η προστασία στη συνέχεια αναλύεται στην πρόληψη και στην θεραπεία.

Εξάγεται το συμπέρασμα λοιπόν ότι απαιτείται η υιοθέτηση ενός πλαισίου προστασίας πληροφοριών σύμφωνα με το οποίο οποιαδήποτε πολιτισμένη και σοβαρή κοινωνία θα πορεύεται μέσα σε αυτό σεβόμενη τους νόμους και τους πολίτες που χρησιμοποιούν την χρήση ή συλλογή πληροφοριών.

2.2 Πλαίσιο Προστασίας Πληροφοριών

Αναλυτικότερα ένα πλαίσιο προστασίας των πληροφοριών πρέπει να έχει τα εξής χαρακτηριστικά:

α. Να είναι ολοκληρωμένο, η ανάπτυξη του να έχει βασιστεί στις απόψεις του κοινωνικού συνόλου.

β. Να είναι πολυδύναμο, η ανάπτυξη να έχει βασιστεί σε ανάλογη διεθνή εμπειρία και πρακτική.

γ. Να είναι πολυδιάστατο, να συνδυάζει θεσμικές ρυθμίσεις, οργανωσιακές ρυθμίσεις και κοινωνικές δράσεις.

Το πλαίσιο έχει δύο άξονες. Τα πληροφοριακά συστήματα και τις δράσεις που πρέπει να αναληφθούν ώστε να αναγνωριστούν και να ικανοποιηθούν οι ανάγκες και οι απαιτήσεις προστασίας των σχετικών πληροφοριών. Αναφερόμαστε στις θεσμικές ρυθμίσεις, οργανωσιακές ρυθμίσεις και κοινωνικές δράσεις.

Στη συνέχεια οι θεσμικές ρυθμίσεις διακρίνονται σε κανονιστικές και νομικές. Τα πρότυπα (standards) είναι κανονιστικές ρυθμίσεις που ισχύον σε διεθνές, περιφερειακό ή τοπικό επίπεδο.

Συγχρόνως οι οργανωσιακές ρυθμίσεις αφορούν τα μέτρα εκείνα της οργάνωσης που απαιτείται κάθε επιχείρηση ή οργανισμός να πάρει προκειμένου να διασφαλίσει την προστασία των πληροφοριών που διαχειρίζεται. Για να γίνει πιο σαφές τα μέτρα αυτά είναι:

α. Η αναγνώριση των γενικών αρχών που διέπουν την προστασία των πληροφοριών στα πληροφοριακά συστήματα.

β. Η διαμόρφωση πολιτικών ασφαλείας, σύμφωνα με τις οποίες ο οργανισμός θα λειτουργεί προκειμένου να προστατεύσει τις πληροφορίες του

γ. Η διαμόρφωση των τεχνικών και διαδικαστικών μέτρων που απαιτούνται προκειμένου να επιτευχθεί συμμόρφωση με την πολιτική ασφαλείας. Το σύνολο των μέτρων αυτών μπορεί να το συναντήσουμε και ως σχέδιο ασφαλείας (security plan).

Κατόπιν οι κοινωνικές δράσεις και συγκεκριμένα η εκπαίδευση και η ενημέρωση οι οποίες θα στοχεύουν στην ενίσχυση της γνώσης και στην διαμόρφωση κοινωνικής επίγνωσης για την αναγκαιότητα προστασίας των πληροφοριών, ώστε οι πολίτες να ενημερώνονται και να συμμετέχουν στις διαδικασίες που αφορούν τη χρήση των πληροφοριών.

2.3. Θεμελιώδες έννοιες

Είναι χρήσιμο να αντιληφθεί κανείς ότι υπάρχει μια δυσκολία από την έλλειψη γενικότερης αποδεκτής ορολογίας από την στιγμή που υπάρχουν πολλές λέξεις των οποίων η απόδοσή τους στα ελληνικά έχει πολλές έννοιες, όπως είναι για παράδειγμα η λέξη «ασφάλεια» η οποία μπορεί να αποδοθεί ως security, safety ή insurance. Το ίδιο ισχύει και για τη λέξη «κίνδυνος» που αποδίδεται ως risk, danger ή hazard. Γίνεται επομένως κατανοητό ότι απαιτείται να ορίζουμε ένα κοινό λεξιλόγιο σε ότι αφορά τα ζητήματα Ασφαλείας Πληροφοριακών και Επικοινωνιακών Συστημάτων.

Στο σημείο αυτό μπορούμε να αναφέρουμε ότι η ασφάλεια πληροφοριών σχετίζεται με την ασφάλεια των πόρων που αξίζει να προστατευτούν. Οτιδήποτε έχει αξία για έναν οργανισμό, για μια επιχείρηση ακόμα και για έναν ιδιώτη[3], ή αφορά τις επιχειρησιακές του λειτουργίες, οι οποίες συμπεριλαμβάνουν μέσα και τους πληροφοριακούς πόρους που υποστηρίζουν την εργασία και αποστολή του οργανισμού, ονομάζεται αγαθό (asset). Στη συνέχεια τα αγαθά τα διαχωρίζουμε στα φυσικά αγαθά, πληροφορίες/δεδομένα, λογισμικό, ανθρώπους και άυλα αγαθά. Τα αγαθά τα προστατεύομε γιατί όπως αναφέρθηκε και παραπάνω έχουν αξία (value). Είναι δηλαδή σημαντικά και έχουν κόστος για τον οργανισμό ή τον ιδιώτη. Γίνεται εύκολα κατανοητό ότι εάν πραγματοποιηθεί κάποιου είδους ζημιά (harm) αυτή η αξία θα μειωνόταν.

Απειλή (threat) είναι μια δυνητική κατάσταση πρόκλησης περιστατικού παραβίασης ασφαλείας, το οποίο μπορεί να προκαλέσει ζημιά στον οργανισμό ή στον ιδιώτη. Μια απειλή μπορεί να πραγματοποιηθεί εφόσον το αγαθό έχει ευπάθεια σε αυτήν. Μια επιγραμματική περιγραφή των απειλών μπορούμε να αναφέρουμε τις εξής:

α. Ανθρώπινες επιθέσεις.
β. Φυσικές καταστροφές.
γ. Ακούσια ανθρώπινα λάθη.
δ. Εσωτερικές ατέλειες του εξοπλισμού ή του λογισμικού.

Οι απειλές σε σχέση με την προέλευσή τους μπορούν να ενταχθούν σε 3 κατηγορίες:

α. Φυσικές Απειλές.
β. Ακούσιες Απειλές.
γ. Εκούσιες Απειλές.

Στον συγκεκριμένο χώρο της ασφάλειας, έκθεση σε κίνδυνο (exposure) ονομάζουμε μια μορφή πιθανής απώλειας (loss) ή ζημιάς (harm) σε ένα υπολογιστικό σύστημα. Ενδεικτικά παραδείγματα είναι:

[3] Από το σημείο αυτό θα αναφερόμαστε στην έννοια του οργανισμού, της επιχείρησης καθώς και του ιδιώτη σαν «οργανισμό» και θα εννοούμε ότι ένα πληροφοριακό σύστημα μπορεί να βρίσκεται σε κάποια από τις αντίστοιχες θέσεις.

α. μη εξουσιοδοτημένη αποκάλυψη δεδομένων.
β. μη εξουσιοδοτημένη τροποποίηση δεδομένων.
γ. άρνηση αθέμιτης προσπέλασης υπολογιστικών πόρων.

Ευπάθεια (vulnerability) είναι μια αδυναμία ενός αγαθού ή ομάδας αγαθών που μπορεί να εκμεταλλεύονται μία ή και περισσότερες απειλές. Οι πολιτικές και τα προϊόντα ασφαλείας μπορούν να μειώσουν την πιθανότητα να καταστεί δυνατή μια επίθεση, να διαπεράσει τις άμυνες του συστήματος ή να απαιτείται από τον επίδοξο εισβολέα να καταναλώσει χρόνο και πόρους ώστε να μην αξίζει η προσπάθεια. Α-ναντίρρητα έχει διαπιστωθεί και θεωρούμε ότι στην πράξη πλήρες ασφαλές σύστημα ή πλήρης ασφάλεια δεν υπάρχει. Επίσης μπορούμε να κατηγοριοποιήσουμε τα τυπικά σημεία ευπάθειας σε ένα υπολογιστικό σύστημα ως εξής:

α. Φυσικές Ευπάθειες (Physical)
β. Εκ Φύσεως Ευπάθειες (Natural)
γ. Ευπάθειες Υλικού και Λογισμικού (Hardware and Software)
δ. Ευπάθειες Μέσων (Media)
ε. Ευπάθειες Εκπομπών (Emanation)
στ. Ευπάθειες Επικοινωνιών (Communications)
ζ. Ανθρώπινες Ευπάθειες (Human)

Μέτρα Προστασίας (controls) ή αντίμετρα (countermeasures) είναι όλες εκεί-νες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός Πληροφοριακού Συστήματος.

Είμαστε σε θέση να διαχωρίσουμε τους διαφορετικούς τύπους αντιμέτρων ως ανάλυση του προβλήματος ασφαλείας ενός πληροφοριακού συστήματος στις ακό-λουθες συνηστώσες:

α. Φυσική Ασφάλεια συστήματος (physical security).
β. Ασφάλεια υπολογιστικού συστήματος (computer security).
γ. Ασφάλεια Βάσεων Δεδομένων (database security).
δ. Ασφάλεια Δικτύων Επικοινωνιών (network security).

Στις κατηγορίες μέτρων ασφαλείας μπορούμε να εντάξουμε τέσσερις βασι-κούς τρόπους άμυνας οι οποίοι μπορούν να βοηθήσουν ώστε να υπάρξει αρκετή ασφάλεια σε ένα πληροφοριακό σύστημα. Επομένως μπορούμε να διαχωρίσουμε:

α. Μέτρα Προσπέλασης Συστήματος.
β. Μέτρα Προσπέλασης Δεδομένων.
γ. Διαχείριση Συστήματος και Ασφαλείας
δ. Σχεδιασμός Συστήματος

Επιπροσθέτως οι κύριοι τύποι των μέτρων για την πρόληψη και εκμετάλλευση των ευπαθειών ενός πληροφοριακού συστήματος είναι:

α. Κρυπτογράφηση
β. Μέτρα Λογισμικού
γ. Μέτρα Υλικού
δ. Φυσικά Μέτρα Υλικού
ε. Πολιτικές Ασφαλείας

2.4 Σύστημα Διαχείρισης

Σύστημα διαχείρισης (Management system) είναι ένα πλαίσιο πολιτικών, διαδικασιών, οδηγιών και πόρων οι οποίοι απαιτούνται προκειμένου να επιτευχθούν οι στόχοι του οργανισμού.

Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) Information Security Management System – ISMS) είναι εκείνο το τμήμα του συνολικού συστήματος διαχείρισης του οργανισμού το οποίο αφορά την ασφάλεια πληροφοριών.

Μπορούμε εύκολα να συμπεράνουμε ότι ένας οργανισμός με την καθιέρωση, τη συντήρηση, και την διαρκή επικαιροποίηση του Συστήματος Διαχείρισης Ασφαλείας Πληροφοριών αποδεικνύει και είναι σε θέση να επιβεβαιώσει ότι μπορεί να ικανοποιήσει τις απαιτήσεις ασφαλείας που του έχει θέση. Φυσικό επακόλουθο αποτελεί η ικανότητά του οργανισμού να διασφαλίζει την επιχειρησιακή του συνέχεια, να ελαχιστοποιήσει τις ζημιές και τις απώλειες, στην περίπτωση που συμβεί κάποιο περιστατικό ασφαλείας (διαρροή δεδομένων), να αποκτήσει σοβαρό πλεονέκτημα έναντι ανταγωνιστών του, να αυξήσει την κερδοφορία του, να συμμορφωθεί με τις απαιτήσεις του νόμου και τελικά να αποκτήσει καλή φήμη.

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι για να είναι ένα ΣΔΑΠ αποτελεσματικό οι στόχοι και οι δραστηριότητες να μην ξεφεύγουν από τους γενικότερους στόχους που έχει θέσει ο οργανισμός. Οι απαιτήσεις ασφαλείας είναι αναγκαίο να έχουν καθοριστεί με βάση μελέτη ανάλυσης και διαχείρισης κινδύνων. Το ΣΔΑΠ χρειάζεται συνεχή στήριξη από την διοίκηση ενός οργανισμού και η στήριξη αυτή να είναι ορατή σε όλα τα στελέχη.

Είναι επιβεβλημένο το ΣΔΑΠ να περιλαμβάνει:

α. Ένα αποτελεσματικό πρόγραμμα ενημέρωσης.
β. Κατάρτιση και εκπαίδευση στον οργανισμό.
γ. Κατάρτιση και εκπαίδευση των εξωτερικών συνεργατών.

Γίνεται εύκολα κατανοητό ότι το περιεχόμενο, η έκταση και η διάρκεια του προγράμματος πρέπει να είναι ανάλογα με την σχέση που έχει κάθε εργαζόμενος με την ασφάλεια πληροφοριών. Για παράδειγμα μπορούμε να αναφέρουμε ότι ένας υπάλληλος του τμήματος προσωπικού θα χρειαστεί να εκπαιδευτεί στα αντικείμενα που άπτονται σε ότι αφορά τα προσωπικά στοιχεία και τα δεδομένα των εργαζομένων, τα οποία είναι στην εποπτεία και την επιμέλειά του. Για να πραγματοποιηθεί αυτό θα χρειαστούν κάποιες μέρες εκπαίδευσης. Παράλληλα για να εκπαιδευτεί ένας υπάλληλος, ο οποίος θα είναι βοηθός του διαχειριστή και ο οποίος θα είναι ο υπεύθυνος σε ότι αφορά την ασφάλεια και την αποτροπή των διαρροών, θα χρειαστεί μπορεί και μερικούς μήνες. Τέλος το ΣΔΑΠ πρέπει να περιλαμβάνει διαδικασίες δια-

χείρισης ενδεχομένων περιστατικών παραβίασης ασφαλείας και διαρροής δεδομένων, σχέδιο επιχειρησιακής συνέχειας και ένα σύστημα μέτρησης της απόδοσης του για το εάν είναι σε θέση να εκτελέσει την αποστολή του και να εντοπιστούν τα σημεία που επιδέχονται βελτίωση.

2.5. Πρότυπα Ασφαλείας

Ιδιαίτερα σημαντική θεωρείται η προσπάθεια που έχει σημειωθεί ώστε να δημιουργηθεί ένας κατάλογος με εκείνα τα αποτελεσματικά μέτρα ασφάλειας που κάθε οργανισμός θα πρέπει να εφαρμόσει απαραίτητα, ανεξάρτητα από οποιαδήποτε άλλη λειτουργική παράμετρο.

Η σειρά ISO27k παρέχει συστάσεις καλών πρακτικών για την διαχείριση της ασφαλείας πληροφοριών, τη διαχείριση κινδύνων και τα μέτρα ασφαλείας μέσα στο γενικότερο περιβάλλον ενός ΣΔΑΠ. Αυτό σημαίνει ότι σκοπός του προτύπου είναι να θέσει προδιαγραφές για τον σχεδιασμό, την υλοποίηση, τη λειτουργία, την παρακολούθηση, τον έλεγχο και την συντήρηση ενός τεκμηριωμένου ΣΔΑΠ στο πλαίσιο ενός οργανισμού. Επίσης περιλαμβάνει προδιαγραφές για την εκτίμηση και διαχείριση των κινδύνων, προσαρμοσμένες στις ανάγκες του οργανισμού. Το πρότυπο βρίσκει εφαρμογή σε όλους τους τύπους των οργανισμών, σε οποιοδήποτε κλάδο κι αν δραστηριοποιούνται, ανεξάρτητα από το μέγεθος και τις δραστηριότητες του οργανισμού. Συνεπώς μπορεί να αφορά μικρές επιχειρήσεις, μη κερδοσκοπικούς οργανισμούς, κυβερνητικές υποδομές, υποδομές εθνικής άμυνας κλπ. Οι απαιτήσεις του προτύπου δομούνται σε 7 ενότητες. Οι ενότητες αυτές φαίνονται στον πίνακα :

Ενότητες	Υποενότητες
Το περιβάλλον του οργανισμού	Κατανόηση του οργανισμού και του Περιβάλλοντός του.
	Κατανόηση των αναγκών και των προσδοκιών των ιδιοκτητών
	Καθορισμός της έκτασης του ΣΔΑΠ
	ΣΔΑΠ
Η ηγεσία	Ηγεσία και δέσμευση
	Πολιτική
	Οργανωσιακοί ρόλοι, αρμοδιότητες και καθήκοντα.
Ο σχεδιασμός	Ενέργειες για την αντιμετώπιση κινδύνων και την αξιοποίηση ευκαιριών
	Στόχοι ασφαλείας πληροφοριών και σχεδιασμός για την επίτευξή τους
Υποστήριξη	Πόροι
	Ικανότητες
	Επίγνωση
	Επικοινωνία
	Τεκμηρίωση
Λειτουργία	Λειτουργικός σχεδιασμός και έλεγχος
	Εκτίμηση κινδύνων

	Διαχείριση κινδύνων
Αξιολόγηση επιδότησης	Παρακολούθηση, μέτρηση, ανάλυση και αξιολόγηση
	Εσωτερικός έλεγχος
	Επανεξέταση από τη διοίκηση
Βελτίωση	Ασυμμορφία και διορθωτικές ενέργειες
	Συνεχής βελτίωση

Πίνακας 1: Απαιτήσεις Προτύπου ISO 27k

2.6 Οργανωσιακό Πλαίσιο Ασφαλείας Πληροφοριών και Πολιτικές Ασφαλείας.

Ένα πλαίσιο ασφαλείας πληροφοριών περιλαμβάνει πολιτικές, κανόνες, διαδικασίες και οδηγίες. Ένα εγχειρίδιο ασφαλείας (security manual) αποτελείται από ένα σύνολο εγγραφών που περιγράφουν πολιτικές, κανόνες, διαδικασίες και οδηγίες για την ασφάλεια. Αποτελεί ένα βασικό στοιχείο τεκμηρίωσης του ΣΔΑΠ. Εντάσσεται στο πλαίσιο προστασίας των δεδομένων του οργανισμού και απορρέει από την οργανωσιακή πολιτική ασφαλείας και την υποστηρίζει. Το λεπτό σημείο που θα πρέπει να τονισθεί ιδιαίτερα είναι να μην απαξιωθεί στη συνέχεια σαν μια απλή γραφειοκρατική διαδικασία από την στιγμή που θεωρηθεί ότι πραγματοποίησε τις απαιτήσεις του ΣΔΑΠ.

Ανάλογα την φύση του οργανισμού και την ενασχόλησή του απαιτείται η υλοποίηση του πλαισίου ασφαλείας με συγκεκριμένα χαρακτηριστικά που μπορεί να αποτελεί νομική ή κανονιστική υποχρέωσή του. Στη συνέχεια όταν πραγματοποιείται μια αγορά προϊόντων ασφαλείας που μπορεί να αφορά και υλικό και λογισμικό είναι φυσικό εάν δεν υπάρχει κάποιο πλαίσιο ασφαλείας στο οποίο θα ενταχθούν τα προϊόντα αυτά ώστε να λειτουργήσουν ομαλά και με συνεργασία στην ήδη υπάρχουσα τεχνική και οργανωτική υποδομή ασφαλείας αυτά θα καταλήξουν να μην εξυπηρετούν το σκοπό τους και να είναι αναποτελεσματικά.

Όπως ήδη έχουμε αναφέρει επειδή η διαχείριση της ασφάλειας πληροφοριών είναι μια διαδικασία δαπανηρή σε πόρους και ανθρώπους, προσπαθούμε να την πραγματοποιήσουμε με τη δυνατότερη οικονομική επιλογή. Για το λόγο αυτό θεωρείται επιβεβλημένο να αντιμετωπίζεται ως αυτοτελές έργο.

Όταν πραγματοποιηθεί η υλοποίηση του πλαισίου ασφαλείας πληροφοριών βρισκόμαστε ένα στάδιο πιο κοντά στη διαδικασία διαμόρφωσης κουλτούρας ασφαλείας στον οργανισμό. Με τον όρο «κουλτούρα ασφαλείας» εννοούμε ότι οι χρήστες των πληροφοριακών συστημάτων διαμορφώνουν την ίδια αντίληψη και πορεύονται μαζί με την ανάγκη, τους στόχους και τα μέτρα ασφαλείας.

2.6.1 Πολιτικές Ασφαλείας

Είναι γενικά αποδεκτό ότι οι πολιτικές ασφαλείας έχουν καθοριστική σημασία για την προστασία των πληροφοριών σε έναν οργανισμό. Μέσω αυτών προσδιορίζονται οι απαιτήσεις του πληροφοριακού συστήματος σε θέματα ασφαλείας. Αυτό που όμως μπορούμε να διακρίνουμε είναι ότι δεν υπάρχει μια κοινή αποδοχή

για το περιεχόμενο στον όρο «πολιτική ασφαλείας». Πολιτική μπορούμε να αναφέρουμε ότι είναι μια τυπική, σύντομή και υψηλού επιπέδου δήλωση ή σχέδιο, που εκφράζει τις γενικές πεποιθήσεις, τους σκοπούς, τους στόχους και τις αποδεκτές διαδικασίες ενός οργανισμού σε μια συγκεκριμένη θεματική περιοχή. Ένα σύνολο από αρχές (principles) και οδηγίες υψηλού επιπέδου (high level guidelines) που αφορούν τη σχεδίαση και διαχείριση συστημάτων ασφαλείας. Αυτό μας οδηγεί στο γεγονός ότι οι πολιτικές εστιάζουν στο αποτέλεσμα και όχι στον τρόπο και για αυτό το λόγο συμπληρώνονται με οδηγίες και κανόνες. Συνεπώς η πολιτική ασφαλείας θα εκφραστεί με τους κανόνες που θα ρυθμίσουν πως ελέγχονται τα συμμετέχοντα μέρη και πώς λαμβάνονται οι αποφάσεις για προσπέλαση, για χρησιμοποίηση και αποθήκευση των δεδομένων αναλόγως της σπουδαιότητάς τους. Η μη συμμόρφωση με τις πολιτικές του οργανισμού αποτελεί πειθαρχικό παράπτωμα και επιφέρει κυρώσεις. Μια τέτοια διεργασία μπορούμε να την αναλύσουμε σε μια δομή τριών επιπέδων:

α. Υψηλότερο επίπεδο. Στο οποίο ο οργανισμός καθορίζει την πολιτική ασφαλείας πληροφοριών (information security policy), η οποία πρέπει να εγκριθεί από την διοίκηση και καθορίζει την προσέγγιση του οργανισμού στη διαχείριση των στόχων που έχει σχετικά με την ασφάλεια πληροφοριών. Μπορούμε να την αναφέρουμε και ως πολιτική ασφαλείας πληροφοριών υψηλού επιπέδου. (High level information security policy). Το επίπεδο αυτό θα πρέπει το ελάχιστο να περιέχει:

- τους στόχους και τα σχέδια του οργανισμού τα οποία αφορούν την ασφάλεια πληροφοριών.
- Ρόλους και καθήκοντα σχετικά με την ασφάλεια πληροφοριών.
- Επισήμανση της σημασίας που δίνει η διοίκηση στη συμμόρφωση του προσωπικού με την πολιτική.
- Δέσμευση σχετικά με τους πόρους που διατίθενται προκειμένου να αναπτυχθεί, να υλοποιηθεί, να λειτουργήσει και να συντηρηθεί το ΣΔΑΠ.
- Δέσμευση της διοίκησης για επανεξέταση του ΣΔΑΠ σε τακτά χρονικά διαστήματα.
- Διασφάλιση της παροχής κατάλληλης κατάρτισης στο προσωπικό που επηρεάζεται από το ΣΔΑΠ, ώστε να έχουν τις γνώσεις και δεξιότητες που απαιτούνται προκειμένου να μπορούν να ανταποκριθούν στα καθήκοντά τους.

β. Μεσαίο Επίπεδο. Το αμέσως επόμενο επίπεδο η πολιτική ασφαλείας πληροφοριών υποστηρίζεται από θεματικές πολιτικές, οι οποίες στοχεύουν είτε σε συγκεκριμένες ομάδες ατόμων μέσα στον οργανισμό ή καλύπτουν συγκεκριμένα θέματα. Αυτά μπορεί να αφορά πολιτική:

- ελέγχου πρόσβασης
- κατηγοριοποίησης και χειρισμού πληροφοριών
- φυσικής και περιβαλλοντικής ασφάλειας
- για θέματα τελικού χρήστη, όπως:
  - αποδεκτής χρήσης αγαθών
  - καθαρού γραφείου και καθαρής οθόνης
  - μετάδοσης πληροφοριών

- κινητών συσκευών και τηλεργασίας
- περιορισμών στην εγκατάσταση και χρήση λογισμικού

➢ αντιγράφων ασφαλείας
➢ μετάδοσης πληροφοριών
➢ προστασίας από κακόβουλο λογισμικό
➢ διαχείρισης τεχνικών ευπαθειών
➢ κρυπτογραφικών μέτρων ασφαλείας
➢ ασφαλείας επικοινωνιών
➢ ιδιωτικότητας και προστασίας πληροφοριών προσωπικού χαρακτήρα.
➢ σχέσεων με τους προμηθευτές

Επίσης χρειάζεται να περιέχει:

➢ Το θέμα το οποίο αφορά.
➢ Τους στόχους, τους όρους και τις προϋποθέσεις που θέτει.
➢ Τις κατευθύνσεις της διοίκησης για το θέμα.
➢ Αυτούς στους οποίους απευθύνεται η πολιτική.
➢ Το πεδίο εφαρμογής της πολιτικής
➢ Τους ρόλους και τα καθήκοντα του προσωπικού σχετικά με την πολιτική.
➢ Τις κυρώσεις σε περίπτωση μη συμμόρφωσης του προσωπικού με την ποιοτική.
➢ Αυτοί που είναι υπεύθυνοι για να επικοινωνήσει κάποιος για θέματα σχετικά με την πολιτική.

γ. Κατώτερο Επίπεδο. Οι πολιτικές εστιάζουν σε μια συγκεκριμένη εφαρμογή ή σε ένα σύστημα. Για παράδειγμα μια τέτοια πολιτική καλύπτει θέματα όπως ποιος έχει εξουσιοδότηση να διαβάζει ή να τροποποιεί δεδομένα, κάτω από ποιες προϋποθέσεις ισχύουν οι εξουσιοδοτήσεις αυτές, πως ελέγχονται απομακρυσμένα σε ένα συγκεκριμένο σύστημα ή εφαρμογή.

Κανόνες (standards) είναι υποχρεωτικές απαιτήσεις που υποστηρίζουν τις πολιτικές. Καλύπτουν θέματα όπως για παράδειγμα τι υλικό και τι λογισμικό πρέπει να χρησιμοποιείται, πιο πρωτόκολλο απομακρυσμένης πρόσβασης πρέπει να υλοποιηθεί ή ποιος είναι αρμόδιος για να εγκρίνει κάτι.

Διαδικασία (procedure) είναι μια ακολουθία που πραγματοποιείται υποχρεωτικά προκειμένου να πετύχουμε έναν τελικό σκοπό. Οι πολιτικές συχνά καθορίζουν τι πρέπει να προστατευθεί ενώ οι διαδικασίες καθορίζουν τον τρόπο με τον οποίο θα προστατευθούν οι πόροι και αποτελούν τους μηχανισμούς επιβολής των πολιτικών.

Οδηγίες (guidelines) είναι γενικές δηλώσεις, συστάσεις ή διοικητικές εντολές που στοχεύουν στην επίτευξη των στόχων μιας πολιτικής, διαμορφώνοντας ένα πλαίσιο για την υλοποίηση των διαδικασιών. Δεν είναι υποχρεωτικές, είναι μάλλον υποδείξεις προς τους χρήστες. Λόγο της φύσης τους οι οδηγίες αλλάζουν συχνά, καθώς αλλάζει το περιβάλλον και πρέπει να επανεξετάζονται συχνότερα από τις πολιτικές.

Οι μηχανισμοί οι οποίοι θα επιβάλλουν μια πολιτική ασφαλείας μπορούν να καταταγούν στις παρακάτω κατηγορίες:

- Αναγνώριση (identification)
- Αυθεντικοποίηση (authentication)

- Εξουσιοδότηση (authorization)
- Έλεγχο προσπέλασης
- Ακεραιότητα (integrity)
- Συνέπεια (consistency)
- Επίβλεψη (auditing)

2.6.2. Χαρακτηριστικά μιας Πολιτικής Ασφαλείας

Τα επιθυμητά χαρακτηριστικά μιας πολιτικής ασφαλείας μπορούμε να τα ταξινομήσουμε όπως παρακάτω:

α. Είναι εύκολα κατανοητή.

Εξαιτίας του γεγονότος ότι οι πολιτικές γράφονται από ειδικούς της ασφάλειας καθιστά το γεγονός επίφοβο τα κείμενά τους να μην γίνονται αντιληπτά από κάποιον ο οποίος δεν γνωρίζει και δεν έχει ειδικές γνώσεις.

β. Είναι εφαρμόσιμη.

Το να πραγματοποιηθεί μια ήδη και έτοιμη πολιτική ενός οργανισμού δεν σημαίνει ότι η συγκεκριμένη θα είναι εφαρμόσιμη σε κάθε οργανισμό.

γ. Είναι εφικτή.

Θα πρέπει η πολιτική που θα εφαρμοστεί να είναι τέτοια ώστε να μην εμποδίζει την ομαλή και σωστή λειτουργία του οργανισμού.

δ. Είναι εκτελεστή.

Να μπορεί να είναι μέσα στα πλαίσια του λογικού του κάθε ανθρώπου και να μην θεωρείται παράνομη.

ε. Εφαρμόζεται σταδιακά.

Ορισμένες πολιτικές οι οποίες έχουν θεωρηθεί σημαντικές ενδείκνυται να εφαρμόζονται από την αρχή. Ταυτόχρονα χρειάζεται να δίνεται κάποιος χρόνος για την μελέτη και την αφομοίωσή τους. Μια καλή μέθοδος θα ήταν η εφαρμογή μιας πολιτικής σε έναν οργανισμό και να ζητείται από τις επιχειρηματικές μονάδες να υποβάλουν μέσα σε ένα συγκεκριμένο χρονικό διάστημα ένα σχέδιο συμμόρφωσης με την πολιτική. Αυτό το γεγονός δίνει την δυνατότητα στους επικεφαλής των επιχειρησιακών μονάδων που επηρεάζονται να μελετήσουν την πολιτική και την εφαρμογή της και να υποβάλλουν αναφορές με τα αποτελέσματα τους.

στ. Έχει προληπτικό χαρακτήρα.

Η μορφή μιας καλής και σωστής πολιτικής είναι τι πρέπει να γίνει και όχι να απαγορεύσει κάτι.

ζ. Δεν είναι απόλυτη.

Ο τρόπος ο οποίος θα ειπωθεί κάτι χρειάζεται να είναι διπλωματικός και όχι απόλυτος ή ενοχλητικός.

2.6.3 Κύκλος ζωής μιας πολιτικής ασφαλείας.

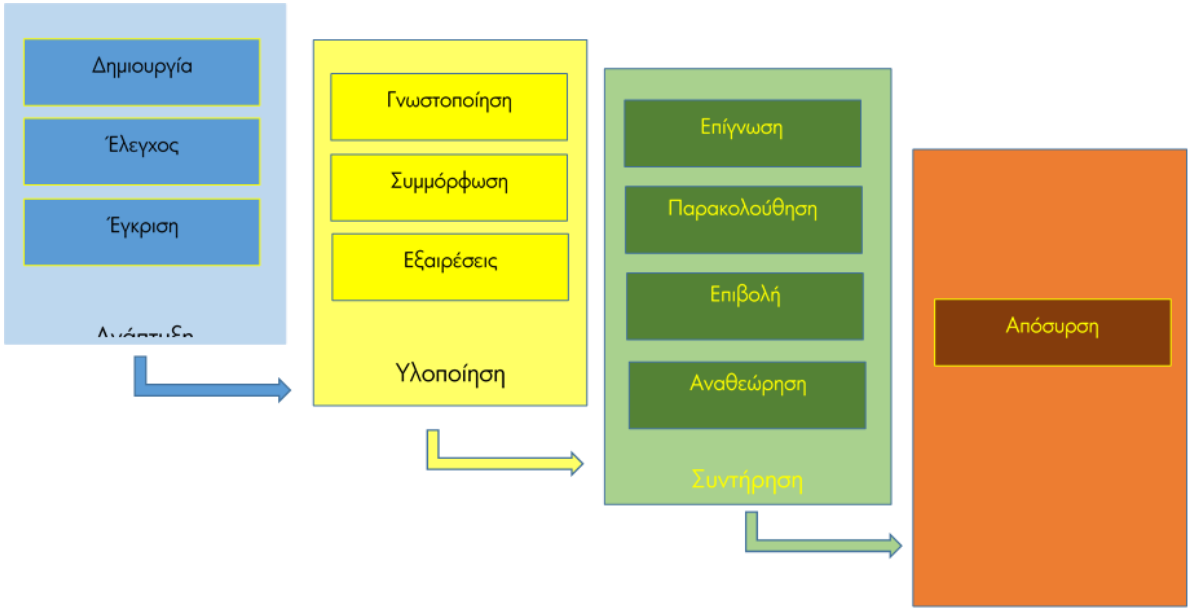
Αναλογιζόμενοι τις διαδικασίες που πραγματοποιούνται κατά την εφαρμογή μιας πολιτικής ασφαλείας καταλήγουμε στο εύλογο συμπέρασμα ότι αυτές δεν είναι δυνατόν να υπάρχουν και να εφαρμόζονται για πάντα ή χρειάζεται να αναπροσαρμόζονται ανάλογα σε τι στάδιο βρίσκεται. Δηλαδή πραγματοποιούν έναν κύκλο ζωής. Υπάρχουν 11 στάδια στην διάρκεια του κύκλου ζωής μιας πολιτικής ασφαλείας:

α. στη φάση της ανάπτυξης, κατά την οποία η πολιτική δημιουργείται, ελέγχεται και εγκρίνεται.

β. στη φάση της υλοποίησης, κατά την οποία η πολιτική γνωστοποιείται και εφαρμόζεται ή παρέχεται εξαίρεση από την εφαρμογή της.

γ. στη φάση της συντήρησης, κατά την οποία αναπτύσσεται επίγνωση του προσωπικού για την πολιτική, παρακολουθείται και επιβάλλεται η εφαρμογή της πολιτικής και επικαιροποιείται συνεχώς

δ. στη φάση της απόσυρσης της πολιτικής, όταν αυτή πλέον δεν έχει λόγο ύπαρξης.



Εικόνα 1: Κύκλος Ζωής μιας Πολιτικής Ασφαλείας

2.7. Μοντέλα Ασφαλείας

Γίνεται κατανοητό ότι για να εφαρμοστούν οι πολιτικές και να επιβληθούν μέσω των μηχανισμών ασφαλείας απαιτείται να ακολουθήσουν κάποια μοντέλα ασφαλείας. Ένα μοντέλο ασφαλείας θα εκφράζει με ακρίβεια και χωρίς συγχύσεις τις απαιτήσεις ασφάλειας ενός συστήματος. Μπορούμε ενδεικτικά να αναφέρουμε:

α. Το Δικτυωτό Μοντέλο
β. Το Μοντέλο Εμπιστευτικότητας Bell – La Padula
γ. Το Μοντέλο Ακεραιότητας Biba
δ. Το Μοντέλο “Graham – Denning”
ε. Το Μοντέλο “Harrison – Ruzzo – Ullman”
στ. Μοντέλα Ροής – Πληροφοριών
ζ. Μοντέλα «Αποτροπής – Παρεμβολών»

Κεφάλαιο 3 : Θεωρητική Θεμελίωση

3.1 Εισαγωγή

Έχοντας παρατηρήσει την αξία που μπορεί να έχουν τα δεδομένα και η πληροφορία που υπάρχει μέσα σε αυτά, γίνεται κατανοητό ότι αυτά θα πρέπει να προστατευθούν. Για να πραγματοποιηθεί αυτό ο συνδυασμός θεσμικών ρυθμίσεων, οργανωσιακών ρυθμίσεων και κοινωνικών δράσεων θεωρείται απαραίτητη. Οι θεσμικές ρυθμίσεις και οι κοινωνικές δράσεις αποτελούν τμήμα και ευθύνη της πολιτείας ενώ οι οργανωσιακές ρυθμίσεις αποτελούν ευθύνη του οργανισμού, που χρησιμοποιεί μια πληροφορία.

Σε ότι αφορά την διαχείριση και κατοχή πληροφοριών από έναν ιδιώτη γίνεται κατανοητό ότι την ευθύνη την έχει αποκλειστικά ο ίδιος. Στην περίπτωση όμως ενός οργανισμού ή μιας επιχείρησης θα πρέπει να έχει προσδιοριστεί και να έχει καθοριστεί ποιος θα έχει την ευθύνη για την ασφάλεια των πληροφοριών και των δεδομένων αν θα είναι τεχνικό θέμα δηλαδή ή θέμα της διοίκησης.

Οι υπεύθυνοι ασφαλείας σε έναν οργανισμό ή μια επιχείρηση καταναλώνονται πρωτίστως στην ανάπτυξη πολιτικών και διαδικασιών, στην εκπόνηση μελετών ανάλυσης κινδύνων, στην διαμόρφωση σχεδίων επιχειρησιακής συνέχειας και στην ανάληψη δράσεων ενημέρωσης και εκπαίδευσης που έχει το προσωπικό σχετικά με την ασφάλεια.

Στο σημείο αυτό να επισημάνουμε την εξής παρατήρηση. Η ασφάλεια είναι σαν μία αλυσίδα. Είναι τόσο ισχυρή όσο είναι ο αδύναμος κρίκος. Αναφερόμαστε στους ανθρώπους και όχι στην τεχνολογία. Είναι γενικά αποδεκτό ότι οι εργαζόμενοι σε έναν οργανισμό ή μια επιχείρηση αποτελούν την σημαντικότερη απειλή είτε ηθελημένα είτε άθελα τους για την ασφάλεια πληροφοριών από ότι τα άτομα που βρίσκονται εκτός του οργανισμού.

Το επίπεδο ασφαλείας πληροφοριών σε έναν οργανισμό εξαρτάται από 3 παράγοντες:

α. τα αποδεκτά επίπεδα κινδύνου που έχει καθορίσει ο οργανισμός
β. τη λειτουργικότητα του πληροφοριακού συστήματος
γ. το κόστος που προτίθεται ο οργανισμός να πληρώσει για την ασφάλεια.

Κάθε οργανισμός πραγματοποιεί και διαχειρίζεται πολλαπλές δραστηριότητες προκειμένου να λειτουργήσει αποδοτικά και αποτελεσματικά σύμφωνα με την εκάστοτε επιχειρηματική σχεδίαση. Οι δραστηριότητες τους είναι ένα αλληλοσχετιζόμενο ή αλληλοεπιδρώντα σύνολο που χρησιμοποιεί πόρους προκειμένου να μετασχηματίσει εισόδους σε εξόδους παράγοντας κάποιο αποτέλεσμα αναφέρεται ως διεργασία (process). Καταλήγουμε με αυτόν τον τρόπο ότι η ασφάλεια πληροφοριών δεν είναι μια στατική κατάσταση πραγμάτων. Είναι μια διεργασία.

Έχοντας την δυνατότητα να παρατηρήσουμε ότι ένας οργανισμός, ακόμα και ένας ιδιώτης ανεξάρτητα του είδους και μεγέθους, συλλέγει, επεξεργάζεται, αποθηκεύει και μεταδίδει μεγάλους όγκους πληροφοριών.

Ο όρος σύστημα σύμφωνα με την γενική θεωρία συστημάτων, δηλώνει έναν αριθμό αλληλοεπιδρώντων στοιχείων τα οποία έχουν οργανικά συναρμολογηθεί σε μια ολότητα, με τρόπο ώστε να εκτελούν μια ορισμένη λειτουργία. Επομένως ένας οργανισμός, μια επιχείρηση ή ένας ιδιώτης μπορούμε να θεωρήσουμε ότι αποτελείται από τα παρακάτω 3 διαφορετικά υποσυστήματα:

1. Το φυσικό σύστημα παραγωγής
2. Το σύστημα Διοίκησης/λήψης αποφάσεων
3. Το πληροφοριακό σύστημα

3.2 Το Πρόβλημα της Διαρροής Δεδομένων.

Η έννοια διαρροής δεδομένων (data loss) είναι απλή. Η μεταβίβαση δεδομένων σε αναρμόδια πρόσωπα (ή χειριστές) όπως επίσης η αποθήκευσή τους σε τόπο που δεν προοριζόταν αρχικά και χωρίς την παροχή της απαραίτητης ασφάλειας. Ο βασικός σκοπός συνεπώς της ασφάλειας των πληροφοριακών συστημάτων σε ότι αφορά την διαρροή δεδομένων πρέπει να είναι η προστασία του υπολογιστικού συστήματος και οποιοδήποτε άλλου στοιχείου σχετίζεται με αυτό με πρώτη και κύρια τις πληροφορίες και κατά αντιστοίχιση τα δεδομένα που βρίσκονται μέσα σε αυτό. Είναι αξιοπρόσεκτο ότι κάποια μη εξουσιοδοτημένη ενέργεια ή διαρροή δεδομένων δεν περιορίζεται μόνο σε μη εξουσιοδοτημένα πρόσωπα. Μπορεί να παρουσιαστεί σε χρήστες του οργανισμού, εξουσιοδοτημένους χρήστες δηλαδή, ή ακόμα πιο σοβαρή περίπτωση και σε διαχειριστές συστήματος οι οποίοι θα προσπαθήσουν αν πραγματοποιήσουν μη εξουσιοδοτημένες ενέργειες όπως είναι για παράδειγμα η απόσπαση μιας λίστας πελατών προς ιδίου όφελος. Εύκολα, λοιπόν, οδηγούμαστε στο συμπέρασμα ότι υπάρχει αυξημένη η ανάγκη για μια τεχνολογική εφαρμογή η οποία να είναι ικανή και να μας επιτρέπει, να παρέχει δηλαδή σε ένα άτομο προστασία από την διαρροή δεδομένων, καθώς επίσης και τις αντίστοιχες αποδείξεις για το ότι πραγματοποιήθηκε μια μη εξουσιοδοτημένη ενέργεια ή όχι (απόδοση ευθυνών).

Αναλυτικότερα η διαρροή δεδομένων μπορεί να πραγματοποιηθεί με πολλούς τρόπους. Η πιο κοινή μέθοδος είναι ένας υπάλληλος να παραβιάσει την πολιτική της εταιρίας και να αντιγράψει ευαίσθητα δεδομένα σε ένα λιγότερο ασφαλές σύστημα, στον προσωπικό του υπολογιστή ή σε μια αφαιρούμενη συσκευή. Άλλοι τρόποι που ενδεχομένως να συναντήσουμε και στους οποίους οφείλεται η διαρροή είναι το ανθρώπινο λάθος, οι τεχνολογικές αστοχίες, δυσαρεστημένους υπαλλήλους, δυσλειτουργία του συστήματος ή ενδεχομένως και κάποια παραβίαση του συστήματος από έναν εισβολέα (hacker).

Σε μία έκθεση που κυκλοφόρησε τον Μάρτιο του 2009 από το Ινστιτούτο Πόουμαν εκτιμάται ότι το 88% των περιστατικών διαρροής δεδομένων οφειλόταν σε χρήση από αμέλεια και 12% οφείλεται σε κακόβουλη πρόθεση.

Οι οργανισμοί και οι επιχειρήσεις δαπανούν άφθονο χρήμα και χρόνο για την εκπαίδευση των υπαλλήλων που αποτελούν το προσωπικό το οποίο χειρίζεται ηλεκτρονικούς υπολογιστές και έχει πρόσβαση σε ευαίσθητες πληροφορίες. Ως εκ τούτου θα υπέθετε κανείς ότι διαρροές δεδομένων, ως αποτέλεσμα ενεργειών από ανυποψίαστους χρήστες θα έπρεπε να είναι πολύ ελάχιστες. Παρόλα αυτά κάτι τέτοιο

δεν ισχύει. Γνωρίζουμε ότι η πλειοψηφία των malware παραβιάσεων σε μια εταιρία οφείλεται σε απρόσεκτες ενέργειες χρηστών.

Σύμφωνα με την έκθεση της Garther εκτιμά τα ακόλουθα σχετικά με την αποκάλυψη των δεδομένων.

Εμπιστευτικά Είδη Δεδομένων	Δεδομένα Πελάτων • Αριθμοί φορολογικού Μητρώου • Αριθμοί Πιστωτικών Καρτών • Αρχεία Υγείας	Δεδομένα Επιχείρησης ή Οργανισμού • Οικονομικά Στοιχεία • Στοιχεία Υπαλλήλων	Πνευματικά Δεδομένα • Πηγές Κώδικα • Σχέδια ανάπτυξης
Ο Κίνδυνος	1:400 Μηνύματα περιέχουν δεδομένα εμπιστευτικού χαρακτήρα		
	1:50 Αρχεία Δικτύου είναι εκτεθειμένα λάθος		
	4:5 Οργανισμοί ή επιχειρήσεις έχουν χάσει δεδομένα σε φορητούς υπολογιστές		
	1:2 Οργανισμοί ή επιχειρήσεις έχουν χάσει δεδομένα σε φορητές συσκευές αποθήκευσης.		

Πίνακας 2: Έκθεση ιστοσελίδας Garner

Μπορούμε συνεπώς να καταλάβουμε από τους παραπάνω αριθμούς, ότι στην απώλεια δεδομένων σε μεγάλο βαθμό συνέβαλαν οι εργαζόμενοι. Αυτό οφείλεται στη χαλαρή πολιτική ασφαλείας την οποία εφάρμοσε ο οργανισμός απέναντι σε συνεργάτες και εργαζόμενους οι οποίοι πραγματοποιούν χρήση των στοιχείων και των πόρων της εταιρίας είτε αυτά είναι υπολογιστές είτε ψηφιακά δεδομένα.

Επίσης έχει παρατηρηθεί ότι ορισμένοι οργανισμοί και επιχειρήσεις επιτρέπουν την χρήση άμεσων μηνυμάτων, web mail, όπως το yahoo, Gmail, κλπ. Ακόμα επιτρέπουν streaming media καθώς και τη κοινή χρήση αρχείων P2P. Τέτοιες περιπτώσεις είναι δυνατόν να συναντήσουμε συνήθως στα κολέγια και στα πανεπιστήμια.

Γιατί οι οργανισμοί και οι επιχειρήσεις να επιτρέπουν τη χρήση web mail και άμεσων μηνυμάτων γνωρίζοντας ότι υπάρχει ο κίνδυνος της απώλειας ευαίσθητων δεδομένων;

Για όλους μας αυτό μπορεί να ακούγεται πολύ λογική σκέψη, παρόλα αυτά και όσο κι αν ηχήσει στα αυτιά μας περίεργα αυτή η συμπεριφορά είναι αποτέλεσμα της πολιτικής που έχει αποφασιστεί να ακολουθήσει η εταιρία. Ακόμα επιχειρήσεις και οργανισμοί με αυστηρές πολιτικές δυσκολεύονται να επιβάλλουν τέτοιους κανόνες αποτελεσματικά. Όταν οι υπάλληλοί τους είχαν την δυνατότητα χρησιμοποίησης τους για πάρα πολλά χρόνια δεν είναι εύκολο να επιβάλλουν αμέσως τέτοιες πολιτικές. Το συγκεκριμένο φαινόμενο το συναντούμε ακόμα και σε κυβερνήσεις και σε εταιρίες υψηλού προφίλ. Είχε παρατηρηθεί στο παρελθόν κατά την κοινή χρήση P2P αρχείων η απώλεια πνευματικών υλικών της εταιρίας και το πέρασμά τους, στα χέρια ανταγωνιστών. Παρόλο που η διαρροή πολλές φορές δεν είναι επίσημη, μπορεί να είναι πολύ επιζήμια για τον οργανισμό.

Γίνεται φανερό ότι η απώλεια δεδομένων και σημαντικών πληροφοριών για μια εταιρία, επιχείρηση ή οργανισμό μπορεί να είναι αρκετά επιζήμια επιφέροντας και νομικές κυρώσεις. Εάν το υλικό το οποίο διέρρευσε περιέχει προσωπικά δεδομένα ή υπόκεινται σε πνευματικά δικαιώματα μπορεί εύλογα να σκεφτεί κάποιος ότι ενδεχομένως να κινηθούν πελάτες της εταιρίας νομικά εναντίον τους. Σκεφτόμαστε

συνεπώς το σοβαρό αντίκτυπο που θα είχε για την φήμη ενός οργανισμού στην αγορά εργασίας. Στον τομέα της πληροφορικής, μπορούμε να δούμε την τεχνική και τον όρο της προστασίας δεδομένων σαν:

α. Αποτροπή Απώλειας Δεδομένων ή Προστασία Απώλειας Δεδομένων.
β. Πρόληψη Διαρροής Δεδομένων ή Προστασία Διαρροής Δεδομένων.
γ. Πρόληψη Απωλειών Πληροφοριών ή Προστασία Απωλειών Πληροφοριών.
δ. Πρόληψη Εκβολής
ε. Παρακολούθηση Περιεχομένου και Φιλτράρισμα.
στ. Παρακολούθηση και Προστασία Περιεχομένου.

Από όλους όμως σαν αρχικά χρησιμοποιούνται το ακρωνύμιο DLP (Data Loss Prevention / Data Leak Prevention).[4]

3.3. Οι συνηθέστερες αιτίες Απώλειας Δεδομένων.

Είναι γεγονός ότι υπάρχουν πολλοί λόγοι για τους οποίους μπορούμε να παρατηρήσουμε το φαινόμενο της διαρροής δεδομένων. Μπορεί να είναι σκόπιμη ενώ άλλες φορές παρατηρούμε ότι είναι από ανθρώπινο λάθος ή ακόμα και από σφάλμα και κακή λειτουργία του συστήματος. Με δεδομένα τα παραπάνω δεν κάνει εντύπωση το γεγονός ότι έχουν παρατηρηθεί πολλές φορές διαρροές δεδομένων. Ορισμένα παραδείγματα είναι:

α. Δημιουργία αναφοράς ή ενός εγγράφου από ένα χρήστη. Ο συγκεκριμένος χρήστης εξάγει τα δεδομένα από ένα ασφαλές σύστημα όπως είναι το δίκτυο του οργανισμού, για να πραγματοποιήσει την εργασία του, σε ένα μη ασφαλές σύστημα όπως είναι η επιφάνεια εργασίας του ηλεκτρονικού υπολογιστή ή μια φορητή συσκευή. Μετά την ολοκλήρωση της εργασίας του, δεν επιστρέφει το αρχείο στο φάκελο που ήταν αρχικά αποθηκευμένος, ούτε καταστρέφει με ασφαλή τρόπο τα αρχεία που χρησιμοποίησε.

β. Δυσαρεστημένοι υπάλληλοι. Υπάρχει περίπτωση ορισμένοι πρώην υπάλληλοι οι οποίοι είναι δυσαρεστημένοι με την διοίκηση και οι οποίοι έχουν πρόσβαση σε ευαίσθητες πληροφορίες, να αποσπάσουν δεδομένα με χρήσιμες πληροφορίες για αυτούς. Είναι γεγονός ότι υπάλληλοι όπως είναι ένας διαχειριστής δικτύου έχει την δυνατότητα έχοντας προνομιακή πρόσβαση σε δεδομένα να ενεργήσει κακόβουλα και να της κλέψει, αποθηκεύοντας τες σε ένα μη ασφαλές σύστημα όπως είναι μια φορητή συσκευή USB stick.

γ. Αναβαθμισμένες εφαρμογές. Στην περίπτωση αυτή μια νέα ή αναβαθμισμένη εφαρμογή τίθεται σε ισχύ σε ένα σύστημα δοκιμών. Ορισμένες προσωπικές πληροφορίες, όπως κωδικοί πρόσβασης και αναγνώρισης, χρησιμοποιούνται για να διαπιστωθεί ότι το όλο σύστημα λειτουργεί σωστά. Στη συνέχεια αφού ολοκληρωθούν οι δοκιμές και συνεχιστεί η διαδικασία της παραγωγής δεν έχει προηγηθεί η αφαίρεση των προσωπικών πληροφοριών αναγνώρισης.

[4] Από το σημείο αυτό θα χρησιμοποιούμε το ακρωνύμιο DLP και θα εννοούμε την Αποτροπή Απώλειας Δεδομένων και όλες τις παραπλήσιες έννοιες.

δ. Διαδικασία για την δημιουργία ασφαλών αντιγράφων ασφαλείας. Το αρχείο το οποίο δημιουργείται σαν αντίγραφο ασφαλείας αποθηκεύεται σε ένα μη ασφαλές περιβάλλον δίνοντας την δυνατότητα σε κάποιον ανεπιθύμητο εισβολέα να το αποσπάσει και να εξετάσει το περιεχόμενο.

ε. Ξεπερασμένο υλικό το οποίο δωρίζεται. Επίσης είναι γνωστό ότι ξεπερασμένων δυνατοτήτων υλικό δύναται να παραδοθεί σε σχολεία ή άλλους οργανισμούς οι οποίοι οι απαιτήσεις τους σε πόρους δεν είναι αυξημένοι. Οπότε δεν πραγματοποιείται σωστή και με βάση των κανόνων ασφαλείας απομάκρυνση του κρίσιμου υλικού από διάφορες ευαίσθητες πληροφορίες.

στ. Δημιουργία εφαρμογής σε διαφορετικό μέρος. Συνεχίζοντας μπορούμε να αναφέρουμε τις περιπτώσεις κατά τις οποίες δημιουργείται μία εφαρμογή και η οποία παρουσιάζει ελλείψεις στην ασφαλή κωδικοποίηση και εμφανίζει σφάλματα διαρροής. Αυτό έχει σαν αποτέλεσμα από την στιγμή που η εφαρμογή τεθεί σε λειτουργία να δίνεται η δυνατότητα σε έναν κακόβουλο εισβολέα να έχει πρόσβαση σε ευαίσθητα δεδομένα που ενδεχομένως να βρίσκονται στην εφαρμογή.

ζ. Ακατάλληλες ρυθμίσεις και ανεπαρκείς έλεγχοι ασφαλείας. Είναι γεγονός ότι σε τμήματα (drivers) τα οποία είναι κοινά μοιρασμένα αυξάνεται ο κίνδυνος της έκθεσης στη περίπτωση που δεν είναι σωστές οι ρυθμίσεις δικαιωμάτων στη δομή των αρχείων και των καταλόγων και θα μπορούσε να επιτρέψει στον καθένα να έχει πρόσβαση στις πληροφορίες. Επίσης στην περίπτωση που ο οργανισμός έχει μια χαλαρή πολιτική έναντι στην φύλαξη των πληροφοριών που του ανήκουν, σύμφωνα με την οποία τα δεδομένα γίνονται εύκολα προσβάσιμα σε όλους.

3.4. Προσδιορισμός Ευαίσθητων Δεδομένων

Όπως αναφέρθηκε και παραπάνω μία από τις βασικές λειτουργίες του DLP είναι η αναζήτηση και καταγραφή των εμπιστευτικών αρχείων. Αναζητούνται και καταγράφονται όλα τα αρχεία από την πιο απλή μορφή τους, όπως είναι για παράδειγμα αρχεία κειμένου με συγκεκριμένες οδηγίες διαβάθμισης, όπου οι διαχειριστές μπορούν να καθορίζουν εάν είναι εμπιστευτικά, έως τα αρχεία με εξελιγμένους μηχανισμούς όπου κατηγοριοποιούν μόνοι τους τα συγκεκριμένα αρχεία ως εμπιστευτικά αρχεία. Οπότε στη περίπτωση που δεν έχουν ήδη κατηγοριοποιηθεί η λύση DLP πραγματοποιεί τον εντοπισμό και τη σήμανσή τους.

Οι εταιρίες πληροφορικής που έχουν αναπτύξει την τεχνολογία και τις λύσεις DLP εφοδιάζουν τις εφαρμογές DLP με εκατοντάδες προκαθορισμένες πολιτικές ασφαλείας DLP που μπορεί να φθάνουν μέχρι και τις 140. Συγκεκριμένα οι πολιτικές DLP έχουν κανόνες για οτιδήποτε, από αριθμούς πιστωτικών καρτών, αριθμούς κοινωνικής ασφάλισης μέχρι και περιορισμούς από διάφορους ρυθμιστικούς νόμους (αναφερόμαστε για την περιοχή των ΗΠΑ κυρίως εξαιτίας της αγοράς και της έδρας

των κυριότερων εκ των εταιριών ανάπτυξης). Ταυτόχρονα θα πρέπει να επισημάνουμε ότι οι εταιρίες είναι πρόθυμες και ικανές να δημιουργήσουν πολιτικές προσαρμοσμένες με βάση τις απαιτήσεις της κάθε εταιρίας ή οργανισμού.

Παρατηρώντας τη μεγάλη χρήση των "κανονικών" εκφράσεων στη data mining, διαπιστώνουμε ότι είναι ένα χρήσιμο εργαλείο καθώς μπορούν να εφαρμοστούν και για DLP. Μπορούμε να είμαστε ακόμα πιο ακριβής όταν η αντιστοίχιση των δεδομένων εφαρμόζεται πάνω σε ένα συγκεκριμένο πλαίσιο. Για παράδειγμα εάν ένας υπάλληλος μισθοδοσίας παρατηρεί τις πληροφορίες και τα δεδομένα των αποδοχών ενός άλλου υπαλλήλου, θεωρείται φυσιολογικό γεγονός και μπορεί να αγνοηθεί. Στη περίπτωση που η ενέργεια αυτή είχε πραγματοποιηθεί από κάποιο άλλο τμήμα (μη αρμόδιο) το DLP θα έπρεπε να σημάνει συναγερμό και ως εκ τούτο θα πρέπει να πραγματοποιηθεί διαβάθμιση στα αρχεία και σε ποιους επιτρέπεται η αντίστοιχη πρόσβαση και επεξεργασία.

Παρατηρώντας τις εταιρίες πληροφορικής και τις εφαρμογές DLP που έχουν αναπτύξει, χρησιμοποιούν τους όρους "δομημένη" αντιστοίχιση δεδομένων και "αδόμητη" αντιστοίχιση δεδομένων.

Δομημένα δεδομένα είναι εκείνα τα οποία βρίσκονται σε καθορισμένες και τυποποιημένες μορφές, όπως είναι για παράδειγμα οι αριθμοί SSN και πιστωτικών καρτών, οι αριθμοί ταυτότητας, ο αριθμός μητρώου κοινωνικών ασφαλίσεων (ΑΜΚΑ), αριθμοί φορολογικού μητρώου (ΑΦΜ) κλπ.

Αδόμητα δεδομένα είναι εκείνα που δεν ακολουθούν μια συγκεκριμένη μορφή και συμπεριλαμβάνουν οτιδήποτε άλλο. Ορισμένα παραδείγματα των αδόμητων δεδομένων είναι πηγές κωδικών, αρχεία πολυμέσων, κλπ. Από τα παραδείγματα γίνεται κατανοητό ότι στα δομημένα δεδομένα η προκαθορισμένη μορφή τους απλοποιεί την κατασκευή της πολιτικής που θα ακολουθηθεί από έναν οργανισμό για την προστασία του. Αντιθέτως στα αδόμητα δεδομένα δεν έχουμε τέτοια επιλογή, για αυτό το λόγο τοποθετούμε ένα «δακτυλικό» αποτύπωμα («fingerprint») εξαιτίας της πολύπλοκης μορφής τους. Τα «δακτυλικά» αποτυπώματα δημιουργούνται χρησιμοποιώντας one way secure hash το οποίο στη συνέχεια σώζεται σε μια βάση δεδομένων. Οι πληροφορίες αυτές στη συνέχεια μπορούν να χρησιμοποιηθούν για τον προσδιορισμό ευαίσθητων δεδομένων και σε κάποια διαφορετική θέση αποθήκευσης. Ανάλογα με το αποτέλεσμα λαμβάνεται η απόφαση κατά πόσο ή όχι δικαιολογείται ο λόγος να σημάνει συναγερμός για το είδος και την διαβάθμιση του αρχείου.

3.5. Μια βαθύτερη ματιά στη λύση DLP.

Υπάρχουν στην παγκόσμια αγορά εταιρίες λογισμικού οι οποίες προσφέρουν στην αγορά συγκεκριμένες λύσεις, συγκεκριμένες υπηρεσίες, προϊόντα, είτε διαθέτουν σε λύσεις για διαφορετικές καταστάσεις, ανάλογα τις επιθυμίες και τις ανάγκες των οργανισμών ή ακόμα και των ιδιωτών. Αν και οι λύσεις αυτές διαφέρουν από εταιρία σε εταιρία όλες επικεντρώνονται σε λύσεις όταν τα δεδομένα βρίσκονται σε 3 διαφορετικές καταστάσεις. Ανάλογα την λύση DLP που θα επιλέξει ένας οργανισμός με βάση την πολιτική ασφαλείας έχουμε την δυνατότητα να παρατηρήσουμε ότι μπορούμε να τα εφαρμόσουμε τις λύσεις:

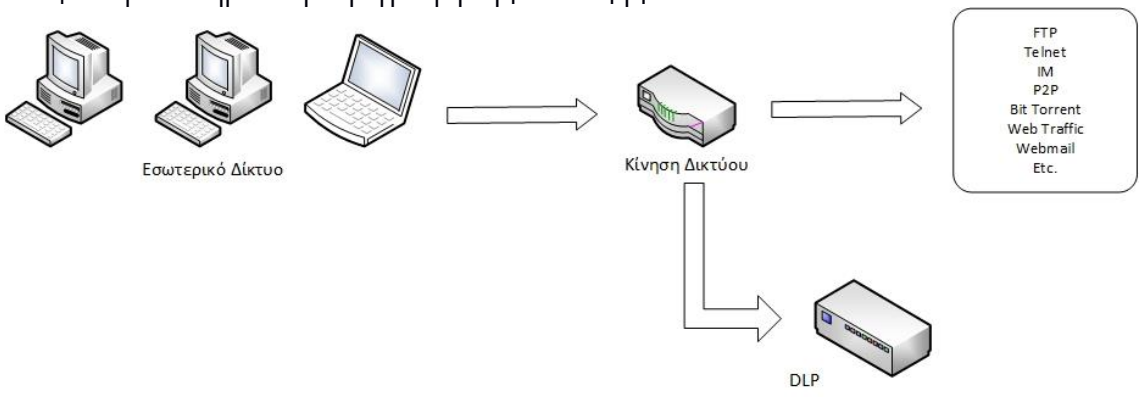
α. Δεδομένα σε Κίνηση (data-in-motion),
β. Δεδομένα σε Αποθήκευση (data at rest) και
γ. Δεδομένα σε Χρήση (data at end-points).

Ενώ τα εργαλεία όπως είναι τα firewalls και τα IDS/IPS ψάχνουν για κάτι που μπορεί να αποτελέσει απειλή για τα δεδομένα, του οργανισμού ή ακόμα και των ιδιωτών, μια λύση DLP θα ενδιαφερθεί πρώτα για τον προσδιορισμό και την αναγνώριση των ευαίσθητων δεδομένων. Αναζητεί και ενδιαφέρεται για το περιεχόμενο που είναι ζωτικής σημασίας για έναν οργανισμό.

Στη θεωρία μπορεί να φαίνεται ότι οι πολιτικές ασφαλείας και οι διαδικασίες που έχουν οριστεί από τους μηχανισμούς ασφαλείας και κατά επέκταση από τη διοίκηση ακολουθούνται σωστά. Όμως μόνο ένας έλεγχος στη πράξη θα είναι σε θέση να διαπιστώσει το κατά πόσο αυτό ισχύει. Για να εφαρμοστεί με επιτυχία μια πολιτική ασφαλείας σε έναν οργανισμός ένας απλός έλεγχος από μόνος του, δεν είναι αρκετός. Παρόλα αυτά ο έλεγχος θα μας δώσει ορατότητα της όλης κατάστασης των δεδομένων, τι είδος και που βρίσκονται αποθηκευμένα, γίνεται επιβεβλημένο να πραγματοποιείται και προληπτικός έλεγχος ώστε να μειωθούν οι διαρροές δεδομένων τόσο τυχαία όσο και εσκεμμένα.

3.5.1 Δεδομένα σε κίνηση

Τα Δεδομένα σε Κίνηση (Data in Motion) αναφέρονται σε μία λύση που επικεντρώνεται στα δεδομένα τα οποία βρίσκονται σε κίνηση από ένα σημείο σε ένα άλλο, και η λύση παρεμβαίνει ανάμεσά στα σημεία ώστε να διαπιστώσει εάν και εφόσον υπάρχουν δεδομένα τα οποία δεν πρέπει να διακινηθούν. Αυτή η χαρακτηριστική λύση DLP εφαρμόζεται σε όλα τα δεδομένα που διακινούνται ενσύρματα. Αυτή τη στιγμή υπάρχουν πολλά πρωτόκολλα που μπορούν να υποστηριχθούν στη λύση αυτή, όπως είναι τα HTTP, FTP, IM, P2P και SMTP. Στον πίνακα παρακάτω παρουσιάζεται μια σχηματική περιγραφή της διάταξης.



Εικόνα 2:Data In Motion

Όπως φαίνεται παραπάνω όλη η κίνηση που πραγματοποιείται στο εσωτερικό δίκτυο διαμέσου των συνηθισμένων καναλιών επικοινωνίας που αναφέρθηκαν ανωτέρω θα πρέπει να διέρχεται από το DLP για επιθεώρηση. Με αυτόν τον τρόπο μας παρέχεται η δυνατότητα να επιβλέψουμε και να αποτρέπουμε μεγάλο αριθμό παρα-

βιάσεων. Για παράδειγμα εάν ένα αρχείο με μία ευαίσθητη πληροφορία μεταφέρθηκε χρησιμοποιώντας FTP, υπάρχουν πολλοί παράμετροι που θα το ανακαλύψουν. Το FTP είναι ένα πρωτόκολλο που χρησιμοποιεί απλό κείμενο και θα πρέπει να είναι στις πρώτες προτεραιότητες ελέγχου για διαβίβαση ευαίσθητων δεδομένων. Ταυτόχρονα οδηγούμαστε στο ερώτημα εάν αυτό το συγκεκριμένο έγγραφο θα πρέπει να αποχωριστεί από τον οργανισμό. Τέλος επίσης σημαντικό απαιτείται να εξακριβωθεί εάν τα εμπλεκόμενα μέρη είναι εξουσιοδοτημένα να βλέπουν τις συγκεκριμένες πληροφορίες και να τις μεταδίδουν. Επίσης ότι άλλο έχει οριστεί και είναι σύμφωνο με την πολιτική ασφαλείας του κάθε οργανισμού. Τα παραπάνω ισχύουν όχι μόνο για το FTP αλλά για τα περισσότερα από τα γνωστά κανάλια επικοινωνίας. Πριν την εμφάνιση του DLP οι επιχειρήσεις και οι οργανισμοί έλεγχαν το δίκτυό τους για τέτοιου είδους παραβάσεις. Αυτό όμως αφορούσε τα email και τη διαδικτυακή δραστηριότητα

Για να παρακολουθήσουν την κίνηση των δεδομένων στο δίκτυο ενός οργανισμού, η λύση DLP χρησιμοποιεί συγκεκριμένες δικτυακές συσκευές (hardware) ή ενσωματωμένη τεχνολογία λογισμικού για να παγιδεύει επιλεκτικά και να αναλύσει την κίνηση του δικτύου. Όταν τα αρχεία στέλνονται (διακινούνται) σε όλο το δίκτυο συνήθως κατανέμεται σε πακέτα. Για να επιθεωρήσει τις πληροφορίες που διακινούνται μέσα σε ένα δίκτυο, μία λύση DLP θα πρέπει να είναι σε θέση να:

α. Παρακολουθεί παθητικά την κίνηση του δικτύου.
β. Αναγνωρίζει και συλλαμβάνει τις σωστές ροές δεδομένων.
γ. Συγκεντρώσει τα πακέτα που συλλαμβάνει.
δ. Ανακατασκευάσει τα αρχεία που μεταφέρονται στις ροές δεδομένων.

Η λύση DLP εφαρμόζει πρώτα την ίδια ανάλυση που πραγματοποιεί και στα δεδομένα σε ακινησία (Data in Rest). Με αυτόν τον τρόπο καθορίζει εάν κάποιο τμήμα του αρχείου περιέχει δεδομένα που περιορίζονται από το σύνολο των κανόνων που έχουν επιλεγεί στην πολιτική ασφαλείας.

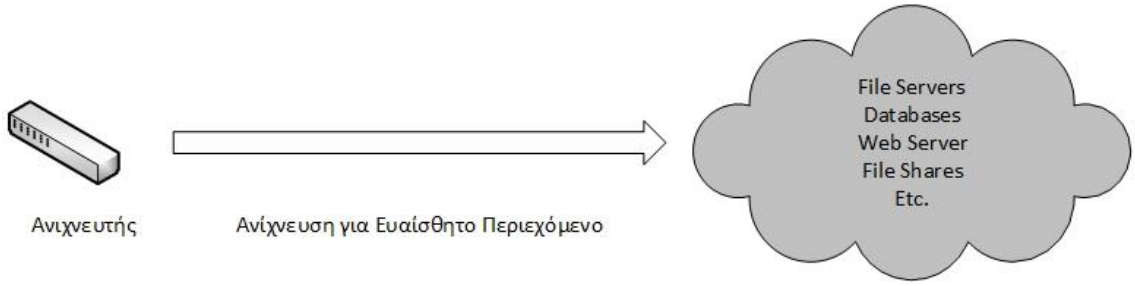
Στο κέντρο αυτής της δυνατότητας είναι η διαδικασία η οποία είναι γνωστή ως deep packet inspection (DPI), η οποία επιτρέπει στο επίπεδο της λύσης DLP – Data in Motion να ολοκληρώσει τον σκοπό του.

Η λύση DLP αναλύει πέρα από τις βασικές πληροφορίες που έχει η επικεφαλίδα ενός πακέτου (η οποία είναι εφάμιλλη με τις πληροφορίες “προς” και “από” που βρίσκονται σε ένα ταχυδρομικό φάκελο) και διαβάζει το περιεχόμενο που μεταφέρεται στο πακέτο (παρόμοια με το γράμμα στο εσωτερικό του φακέλου). Μπορούμε να παρατηρήσουμε ότι η συγκεκριμένη τεχνολογία είναι ακόμα ατελής και εξελίσσεται με τη πάροδο των χρόνων. Η συγκεκριμένη ικανότητα DPI επιτρέπει στην DLP να επιθεωρεί δεδομένα που μεταφέρονται και να καθορίσει το περιεχόμενό τους καθώς, την πηγή και τον προορισμό. Εάν ευαίσθητα δεδομένα εντοπιστούν προς ένα μη εξουσιοδοτημένο προορισμό, η πολιτική της DLP έχει την δυνατότητα να σημάνει συναγερμό και προαιρετικά να μπλοκάρει τα δεδομένα σε πραγματικό ή σε σχεδόν πραγματικό χρόνο και πάλι βασιζόμενο στους κανόνες της πολιτικής ασφαλείας που

έχουν προεπιλεγεί από το τμήμα της διαχείρισης και έχουν αποφασιστεί από την διοίκηση. Βασιζόμενο πάλι στους κανόνες της ακολουθούμενης πολιτικής, η DLP έχει την δυνατότητα να θέσει σε καραντίνα ή να κρυπτογραφήσει τα δεδομένα. Στο σημείο αυτό θα πρέπει να αναφέρουμε ένα σημαντικό παράγοντα προκειμένου να μπορέσει η λύση DLP να παρακολουθήσει το δίκτυο, θα πρέπει τα δεδομένα να είναι αποκρυπτογραφημένα πριν η λύση DLP επιθεωρήσει το περιεχόμενο των δεδομένων. Οδηγούμαστε στο συμπέρασμα ότι η λύση DLP πρέπει να έχει την δυνατότητα να πραγματοποιεί από μόνη της την αποκρυπτογράφηση (έχοντας αυτή τη δυνατότητα με τα αντίστοιχα κλειδιά αποκρυπτογράφησης) ή να υπάρχει μία συσκευή η οποία θα αποκρυπτογραφεί τα προς επιθεώρηση δεδομένα και θα τα κρυπτογραφεί ξανά επιτρέποντάς τα να περάσουν.

3.5.2 Δεδομένα σε Κατάσταση Ηρεμίας

Τα Δεδομένα σε Κατάσταση Ηρεμίας (Data in Rest) είναι ακριβώς όπως υποδηλώνεται και από το όνομα αυτό ισχύει για οτιδήποτε περιέχει δεδομένα καταχωρημένα σε κάποιο μέσο αποθήκευσης όπως είναι για παράδειγμα οι βάσεις δεδομένων. Η συγκεκριμένη λύση DLP έχει δύο χρήσεις. Κύρια χρήση της λύσης αυτής είναι η ανακάλυψη ευαίσθητων δεδομένων σε βάσεις δεδομένων ή αποθετήρια δεδομένων. Αυτή η λύση χρησιμοποιεί τις υπάρχουσες πολιτικές, που έχουν επιλεγεί, και βάση αυτών καθορίζει τις ευαίσθητες πληροφορίες και τις αναζητά ώστε να τις ανακαλύψει. Ταυτόχρονα η συγκεκριμένη σάρωση μπορεί να χρησιμοποιηθεί για να οριστούν fingerprints (“δακτυλικά”) αποτυπώματα στα δεδομένα και στη συνέχεια να χρησιμοποιηθούν σε δεδομένα οπουδήποτε αλλού.



Εικόνα 3:Data In Rest

Όπως απεικονίζεται στην παραπάνω εικόνα, αυτή η συσκευή μπορεί να τοποθετηθεί οπουδήποτε στο δίκτυο με την μοναδική απαίτηση να υπάρχει συνδεσιμότητα με τις IP των Η/Υ (στόχων) που βρίσκονται στο πεδίο εφαρμογής. Επίσης οι λύσεις DLP είναι εξοπλισμένες ώστε να δημιουργούν πολλαπλές εικονικές συνεδρίες ώστε να ελαχιστοποιηθεί η ανάγκη για επιπλέον συσκευές στο δίκτυο. Κάθε εικονική συνεδρία μπορεί να ρυθμιστεί ώστε να ανιχνεύει μια σειρά από διακομιστές (servers) σε ένα συγκεκριμένο δίκτυο. Αυτό είναι ιδανικό για μεγάλα δίκτυα. Ένα μειονέκτημα που μπορούμε να παρατηρήσουμε από την συγκεκριμένη λύση είναι το γεγονός ότι η ενέργεια αυτή εμφανίζει σημαντική επιβάρυνση στο δίκτυο. Παρουσιάζεται δηλαδή υψηλή, σε όγκο δεδομένων, κυκλοφορία, οπότε η χρήση του εύρους ζώνης

(bandwidth) θα παρουσιάζει πρόβλημα. Μία λύση που χρησιμοποιείται είναι η αξιοποίηση της σταδιακής λειτουργίας σάρωσης. Οι διακομιστές (servers) σαρώνονται πλήρως μία φορά και στη συνέχεια σταδιακά πραγματοποιείται έλεγχος μόνο για τις αλλαγές από την τελευταία σάρωση.

Έχει παρατηρηθεί το γεγονός ότι οι πιο κοινές αποκαλύψεις δεδομένων εντοπίζονται κατά την διάρκεια μιας διαδικασίας που ονομάζεται σάρωσης ανακάλυψης (discovery scanning) και έχει διαπιστωθεί ότι αυτές οι αποκαλύψεις αναφέρονται σε κρίσιμα και ευαίσθητα δεδομένα τα οποία έχουν παραμένουν σε DMZ servers χωρίς να το γνωρίζουν οι πελάτες. Παρατηρήθηκε το φαινόμενο όπου δεδομένα πελατών παρέμειναν σε έναν διακομιστή DMZ πάνω από ένα χρόνο.

Όπως γίνεται φανερό από τα παραπάνω μια βασική λειτουργία των λύσεων DLP είναι η δυνατότητα να αναγνωρίζουν και να καταγράφουν συγκεκριμένους τύπους δεδομένων όπως είναι τα αρχεία excel και word τα οποία αποθηκεύονται σε file servers, βάσεις δεδομένων του δικτύου ή ακόμα και στους τερματικούς σταθμούς. Μόλις εντοπιστούν τα αρχεία αυτά, η εφαρμογή DLP θα πρέπει να είναι σε θέση να ανοίξει αυτά τα αρχεία και να ανιχνεύσει το περιεχόμενό τους, ώστε να καθορίσει τί συγκεκριμένα τμήματα από πληροφορίες παρουσιάζονται, όπως είναι για παράδειγμα οι αριθμοί πιστωτικής κάρτας ή αριθμοί κοινωνικής ασφάλισης. Για την εκτέλεση αυτών των λειτουργιών τα περισσότερα συστήματα DLP χρησιμοποιούν Ιχνηλάτες (crawlers), οι οποίες είναι εφαρμογές οι οποίες αναπτύσσονται και εγκαθίστανται απομακρυσμένα σε κάθε ένα τερματικό σταθμό ιχνηλατώντας και αναζητώντας μέσα από τις βάσεις δεδομένων ή στα αποθηκεμένα αρχεία. Η ανίχνευση και ο εντοπισμός της θέσης των δεδομένων βασίζονται σε ένα σύνολο κανόνων και περιορισμών οι οποίες έχουν καθοριστεί και έχουν εισαχθεί από την κονσόλα διαχείρισης της εφαρμογής DLP. Η συλλογή των πληροφοριών αυτών είναι ένα πολύτιμο βήμα το οποίο επιτρέπει στην επιχείρηση να καθορίσει ποιες πληροφορίες “κλειδιά” έχουν εντοπιστεί και εάν η τοποθεσία αποθήκευσης στην οποία βρίσκονται επιτρέπεται από τις υπάρχουσες πολιτικές ασφαλείας, οι διαδικασίες που θα ακολουθήσουν και τέλος αν υπάρχει κίνδυνος να παραβιαστούν οι υπάρχουσες πολιτικές.

3.5.3 Δεδομένα σε Χρήση

Τα δεδομένα σε χρήση ή δεδομένα σε τερματικούς σταθμούς (Data at End-point) βασίζονται στη λύση αντιπροσώπου - πράκτορα (agent)[5] ο οποίος εγκαθίστανται στους τερματικούς σταθμών των χειριστών, σε φορητούς υπολογιστές και παρακολουθεί κάθε πληροφορία η οποία απομακρύνεται χρησιμοποιώντας αφαιρούμενες συσκευές, όπως είναι οι δισκέτες, CD’s, USB’s, κλπ. Επίσης παρέχεται έλεγχος και προστασία ακόμα και από τους χρήστες οι οποίοι εκτυπώνουν διαβαθμισμένα έγγραφα. Λόγω της συγκεκριμένης προσέγγισης, με βάση δηλαδή τον πράκτορα (agent), η μέθοδος αυτή δεν είναι πολύ επιθυμητή στους χρήστες. Στην περίπτωση ενός οργανισμού όμως την διοίκηση δεν θα πρέπει να την απασχολεί το συγκεκριμένο θέμα και να επιλέγει αυτή την λύση. Θα πρέπει να επισημάνουμε ότι η

[5] Στην ξενόγλωσση βιβλιογραφία αναφέρεται ως agent. Συνεπώς θα το αναφέρουμε με το όρο «πράκτορα».

συγκεκριμένη λύση παρέχει μια μεγάλη προστασία εναντίον των δεδομένων που απομακρύνονται μέσω αφαιρούμενων συσκευών. Στο σημείο αυτό μπορούμε να αναφέρουμε, ότι η εφαρμογή της λύσης αυτής είναι συγκρίσιμη με ένα host -based IDS (Intrusion Detection System).

Όπως γίνεται φανερό η συγκεκριμένη μορφή του DLP αποτελεί και την πιο δύσκολη πτυχή της. Η μέθοδος Δεδομένων σε Χρήση (Data In Use) πρωτίστως αναφέρεται στην παρακολούθηση της ροής των δεδομένων και οι οποίες απορρέουν από τις ενέργειες που λαμβάνονται από τους χρήστες στους τερματικούς σταθμούς τους. Οι εργασίες και οι ενέργειες δηλαδή που εκτελούν όπως να αντιγράψουν δεδομένα σε ένα USB stick (thumb drive), είτε στέλνοντας τις πληροφορίες στον εκτυπωτή ή ακόμα αποκόπτοντας και αντιγράφοντας τις πληροφορίες μεταξύ εφαρμογών. Η λύση DLP τυπικά ολοκληρώνεται με την χρήση του λογισμικού που ονομάζεται πράκτορας (agent), οποίος διαχειρίζεται ιδανικά, με τις ίδιες δυνατότητες, από την κεντρική διαχείριση που διαχειρίζεται και ολόκληρη την εφαρμογή DLP, και ο οποίος αναλαμβάνει να εφαρμόσει τις πολιτικές ασφαλείας που έχει επιλέξει ο διαχειριστής δικτύου μετά τις υποδείξεις της διοίκησης. Η εφαρμογή του συνόλου των κανόνων σε ένα τερματικό σταθμό έχει κάποιους εν γένει περιορισμούς, ο πιο σημαντικός είναι να μπορεί ο τερματικός υπολογιστής να επεξεργαστεί τους κανόνες που έχουν εφαρμοστεί. Ανάλογα με τον αριθμό και την πολυπλοκότητα των κανόνων ασφαλείας που επιβάλλονται, μπορεί να είναι αναγκαίο να εφαρμοστούν μόνο ένα μέρος από τον συνολικό κανόνα, το οποίο όμως αφήνει σημαντικά κενά στην συνολική λύση DLP. Δηλαδή να διαθέτει τους πόρους ώστε να μπορεί να εφαρμόζονται οι κανόνες ασφαλείας και να μην αφήνεται

3.6. Χαρακτηριστικά DLP και Λύσεις DLP.

Η δημιουργία και η είσοδος στην αγορά ενός προγράμματος DLP μπορεί να πραγματοποιηθεί με δύο είδη προγραμμάτων και εφαρμογών. Υπάρχει η δυνατότητα ορισμένων προϊόντων και ειδικά κάποιες λύσεις ασφαλείας ηλεκτρονικού ταχυδρομείου (e-mail) οι οποίες προβάλουν βασικές λειτουργίες προστασίας δεδομένων DLP αλλά δεν είναι ολοκληρωμένες λύσεις DLP. Οι διαφορές είναι:

a. Ένα πλήρες πρόγραμμα DLP περιλαμβάνει:

(1) Κεντρική διαχείριση,

(2) Δημιουργία Πολιτικής και

(3) Εκτέλεση Ροής Εργασίας,

Το πλήρες πρόγραμμα είναι προσανατολισμένο στην παρακολούθηση και στην προστασία του περιεχομένου και των δεδομένων. Η διεπαφή με το χρήστη και η λειτουργικότητα είναι προσανατολισμένη στη λύση επιχειρηματικών και τεχνικών

προβλημάτων της προστασίας περιεχομένου βασιζόμενη στην επίγνωσης του περιεχομένου. Δηλαδή στο περιεχόμενο που διαθέτει ο οργανισμός και χειρίζονται οι υπάλληλοί του.

β. Τα χαρακτηριστικά DLP περιλαμβάνουν μερικές από τις δυνατότητες ανίχνευσης και εφαρμογής προστασίας DLP αλλά δεν είναι προσανατολισμένα στο έργο της προστασίας του περιεχομένου των δεδομένων.

Αυτή η διάκριση είναι σημαντική γιατί τα προϊόντα DLP λύνουν συγκεκριμένα προβλήματα των επιχειρήσεων. Εγκαθίστανται δηλαδή για συγκεκριμένο σκοπό και για να εκτελέσουν συγκεκριμένη εργασία. Ένα πλήρες πρόγραμμα DLP διαχειρίζεται είτε από το ίδιο τμήμα του οργανισμού που το ενδιαφέρει η συγκεκριμένη πολιτική είτε διαχειρίζεται από τον διαχειριστή ο οποίος είναι υπεύθυνος και για τις υπόλοιπες λειτουργίες ασφαλείας. Για αυτό το λόγο είμαστε σε θέση να δούμε μη τεχνικό προσωπικό όπως νομικούς να είναι υπεύθυνοι για την προστασία του περιεχομένου. Μέχρι και στελέχη του τμήματος προσωπικού συχνά εμπλέκονται με την διάθεση των DLP ειδοποιήσεων. Ορισμένοι οργανισμοί παρατηρούν ότι οι πολιτικές ασφαλείας της εφαρμογής DLP από μόνες τους είναι πολύ ευαίσθητες ή χρειάζεται να διαχειρίζονται από τμήματα του οργανισμού τα οποία δεν έχουν σχέση με την ασφάλεια, ή χρειάζεται να υποστηρίζουν μια αποκλειστική λύση. Επειδή η εφαρμογή DLP προσανατολίζεται σε ένα καθαρά πρόβλημα του οργανισμού (προστασία του περιεχομένου) γίνεται αντιληπτό ότι διαφοροποιείται από άλλα προβλήματα ασφαλείας (όπως η προστασία του PC ή προστασία του δικτύου) και θα πρέπει να επικεντρώνεται στις αποκλειστικές λύσεις DLP.

Αυτό βέβαια δεν σημαίνει ότι ένα χαρακτηριστικό DLP δεν θα ήταν σωστή λύση για κάποιον, ειδικά για έναν οργανισμό με περιορισμένο εύρος δραστηριοτήτων. Επίσης δε σημαίνει ότι αυτό θα είναι ένας ανασταλτικός παράγοντας και δεν θα αγοραστεί μια σουίτα ασφαλείας που κυκλοφορεί στο εμπόριο, η οποία θα περιλαμβάνει επιπλέον και εφαρμογή DLP, εφόσον η DLP διαχείριση είναι ξεχωριστή και αποκλειστική για DLP. Σε ελάχιστο χρονικό διάστημα θα παρατηρήσουμε ότι όλο και περισσότερες σουίτες των μεγάλων εταιριών να περιλαμβάνουν αναλύσεις DLP σαν ξεχωριστό τμήμα ή να εκτελείται ταυτόχρονα μαζί με κάποιο άλλο πρόγραμμα. Στο σημείο αυτό θα πρέπει να τονίσουμε ότι η δημιουργία κεντρικής πολιτικής, η διαχείριση και η ροή εργασίας θα πρέπει να είναι αποκλειστική για την εφαρμογή του DLP και να είναι διαχωρισμένη από άλλες λειτουργίες ασφαλείας.

Ταυτόχρονα ένα ακόμα θέμα που θα πρέπει να θυμόμαστε για τη εφαρμογή DLP, είναι ότι είναι πολύ αποτελεσματική σε εσφαλμένες διαδικασίες και λάθη ενός οργανισμού (όπως για παράδειγμα ανταλλαγή μέσω FTP ιατρικών αρχείων τα οποία δεν είναι κρυπτογραφημένα).

3.7. Επίγνωση του Περιεχομένου

Στο σημείο αυτό χρειάζεται να κάνουμε έναν διαχωρισμό μεταξύ περιεχομένου και πλαισίου. Ένα από τα καθοριστικά χαρακτηριστικά των εφαρμογών DLP είναι

η επίγνωση του περιεχομένου. Είναι σαφές ότι είναι η ικανότητα των προϊόντων αυτών να αναλύουν βαθιά τα περιεχόμενα των δεδομένων χρησιμοποιώντας μια ποικιλία τεχνικών και είναι πολύ διαφορετική από την ανάλυση του γενικού πλαισίου. Για να γίνει ευκολότερα κατανοητό ας σκεφτούμε το γενικό πλαίσιο σαν ένα φάκελο και το περιεχόμενο σαν μια επιστολή. Το πλαίσιο περιλαμβάνει στοιχεία όπως η πηγή, ο προορισμός, το μέγεθος, τον δικαιούχο, τον αποστολέα, τις πληροφορίες κεφαλίδας, τα μεταδεδομένα, το χρόνο, τη μορφή, και οτιδήποτε άλλο σύντομο από το περιεχόμενο της ίδιας της επιστολής. Το γενικό πλαίσιο είναι πολύ χρήσιμο και κάθε εφαρμογή DLP θα πρέπει να συμπεριλαμβάνει αντίστοιχη ανάλυση σαν μέρος της συνολικής ανάλυσης.

Μια πιο προηγμένη έκδοση της ανάλυσης περιεχομένου είναι μια επιχειρηματική ανάλυση πλαισίου η οποία περιλαμβάνει βαθύτερη ανάλυση του περιεχομένου, το περιβάλλον που βρίσκεται την στιγμή της ανάλυσης και την χρήση του περιεχομένου εκείνη τη στιγμή.

Ας σημειωθεί ότι η γνώση του περιεχομένου περιλαμβάνει ανταλλαγή κίνησης μέσα στο περιεχόμενο και ανάλυση του. Το πλεονέκτημα της είναι, ότι ενώσω χρησιμοποιούμε το περιεχόμενο, δεν είμαστε περιορισμένοι από αυτό. Για να γίνει πιο σαφές εάν θέλουμε να προστατεύσουμε ένα κομμάτι από ευαίσθητα δεδομένα, θα θέλουμε να το προστατεύουμε παντού, όχι μόνο στα προφανή αποθηκευτικά σημεία ευαίσθητων δεδομένων που έχουν από πριν προκαθοριστεί. Προστατεύουμε τα δεδομένα, όχι το φάκελο, επομένως γίνεται περισσότερο κατανοητό ότι πρέπει να ανοίξουμε το φάκελο, να το διαβάσουμε και να αποφασίσουμε πως θα το αντιμετωπίσουμε. Αυτό είναι το δυσκολότερο και πιο χρονοβόρο από την βασική ανάλυση του περιεχομένου και είναι ένα καθοριστικό χαρακτηριστικό για μια εφαρμογή DLP.

3.8. Ανάλυση Περιεχομένου

Αναλυτικότερα το πρώτο βήμα στην ανάλυση περιεχομένου είναι η “σύλληψη” του φακέλου και το άνοιγμά του. Η εφαρμογή τότε χρειάζεται να αναλύσει το πλαίσιο (χρειάζεται και για την ανάλυση) και να εξευρενήσει μέσα σε αυτό. Για ένα απλό κείμενο ηλεκτρονικού ταχυδρομείου αυτό είναι εύκολο, αλλά όταν θέλουμε να δούμε μέσα σε δυαδικά αρχεία, αυτό είναι λίγο πιο πολύπλοκο. Για να υλοποιηθεί αυτή η λύση όλες οι εφαρμογές DLP χρησιμοποιούν file cracking. Αναφορικά file cracking (διάσπαση αρχείου) είναι η τεχνολογία που χρησιμοποιείται για να διαβάσει και να καταλάβει τα αρχεία ακόμα και αν το περιεχόμενο βρίσκεται κάτω από πολλά επίπεδα. Για παράδειγμα είναι συνηθισμένο για τον cracker να διαβάσει ένα φύλλο Excel το οποίο έχει ενσωματωθεί σε ένα αρχείο word το οποίο έχει συμπιεστεί. Η εφαρμογή χρειάζεται να αποσυμπιέσει το αρχείο .zip, να διαβάσει το αρχείο word, να το αναλύσει, να βρει το αρχείο Excel, να το διαβάσει και να το αναλύσει. Άλλες καταστάσεις μπορούν να γίνουν ακόμα πιο πολύπλοκες όπως ένα αρχείο .pdf ενσωματωμένο μέσα σε ένα αρχείο CAD. Πολλές από τις σημερινές εφαρμογές υποστηρίζουν γύρω στους 300 τύπους αρχείων, με ενσωματωμένο περιεχόμενο, με πολλαπλές γλώσσες, διπλά byte για χαρακτήρες ασιατικών γλωσσών καθώς και την ανάλυση απλού κειμένου από μη αναγνωρισμένους τύπους αρχείων. Κάποια εργαλεία

υποστηρίζουν ανάλυση από κρυπτογραφημένα δεδομένα εάν η κρυπτογράφηση του οργανισμού χρησιμοποιείται μαζί με τα κλειδιά ανάκτησης και τα περισσότερα εργαλεία μπορούν να αναγνωρίσουν πρότυπη (standard) κρυπτογράφηση και να τη χρησιμοποιήσουν αυτή σαν κανόνας πλαισίου για να μπλοκάρουν ή να θέσουν σε καραντίνα το περιεχόμενο.

3.9. Τεχνικές Ανάλυσης Περιεχομένου.

Μόλις αποκτηθεί πρόσβαση στο περιεχόμενο, υπάρχουν επτά κύριες τεχνικές αναλύσεων που χρησιμοποιούνται για να βρεθούν παραβιάσεις πολιτικής. Κάθε μία από αυτές, όπως είναι φυσιολογικό, έχει πλεονεκτήματα και μειονεκτήματα:

3.9.1 Τεχνική Βασισμένη σε κανόνες και Ρυθμιστικές Εκφράσεις

Η τεχνική βασισμένη σε κανόνες και ρυθμιστικές εκφράσεις (Rule – Based/Regular Exressions) θεωρείται η πιο συνηθισμένη τεχνική ανάλυσης η οποία είναι διαθέσιμη και στις εφαρμογές DLP και σε εργαλεία που διαθέτουν χαρακτηριστικά DLP. Συγκεκριμένα αναλύουν το περιεχόμενο σύμφωνα με συγκεκριμένους κανόνες όπως είναι για παράδειγμα ο αριθμός των 16 ψηφίων τον οποίο συναντούμε στις πιστωτικές κάρτες, ιατρικούς κωδικούς ή άλλες αναλύσεις κειμένων. Κατά συνέπεια οι περισσότερες εφαρμογές DLP περιέχουν ρυθμιστικές εκφράσεις μαζί με τους επιπρόσθετους κανόνες ανάλυσης (π.χ. ένα όνομα κοντά σε μια διεύθυνση, κοντά σε έναν αριθμό πιστωτικής κάρτας).

Είναι καλύτερο σαν ένα πρώτο φίλτρο ή για την ανίχνευση εύκολα αναγνωρίσιμων κομματιών από συγκεκριμένα δεδομένα όπως είναι οι αριθμοί πιστωτικών καρτών, αριθμοί κοινωνικής ασφάλισης και κωδικούς υγείας.

α. Πλεονεκτήματα: Εύκολα επεξεργάσιμος κανόνας, είναι εύκολος να ρυθμιστεί. Οι περισσότερες εφαρμογές παρέχονται με ένα αρχικό πακέτο κανόνων. Η τεχνολογία είναι κατανοητή και εύκολα ενσωματώνεται σε ένα μεγάλο εύρος εφαρμογών.

β. Μειονεκτήματα: Είναι επιρρεπής σε υψηλά ποσοστά λαθεμένων συναγερμών. Μικρή προστασία σε αδόμητα ευαίσθητα δεδομένα, όπως είναι η πνευματική ιδιοκτησία.

3.9.2. Αποτυπώματα σε Δάση Δεδομένων.

Τα αποτυπώματα σε Βάση Δεδομένων (Database Fingerprint), μερικές φορές καλούνται Λεπτομερής Αντιστοίχιση Δεδομένων (Exact Data Matching). Αυτή η τεχνική χρησιμοποιεί είτε σε μια βάση δεδομένων ή σε τρέχοντα δεδομένα από μια βάση δεδομένων και αναζητώντας μόνο επακριβές αντιστοιχήσεις. Για παράδειγμα θα μπορούσε να δημιουργηθεί μια πολιτική η οποία αναζητά αριθμούς πιστωτικών καρτών μόνο στη βάση δεδομένων των πελατών, έτσι θα αγνοεί τους υπαλλήλους της εταιρίας που θα θέλουν οι ίδιοι να αγοράσουν μέσω διαδικτύου. Πιο προχωρημένα εργαλεία αναζητούν συνδυασμούς πληροφοριών, όπως είναι το πρώτο όνομα

ή η μονογραφή μαζί με το επίθετο, μαζί και με τον αριθμό της πιστωτικής κάρτας ή τον αριθμό της κοινωνικής ασφάλισης.

Είναι καλύτερο για, βάσεις δεδομένων, με δομημένες πληροφορίες δεδομένων.

α. Πλεονεκτήματα: Πολύ χαμηλός αριθμός λανθασμένων συναγερμών (κοντά στο 0). Επιτρέπει την προστασία ευαίσθητων δεδομένων των πελατών, ενώ επιτρέπει να αγνοεί άλλα, παρόμοια δεδομένα που χρησιμοποιούνται από τους υπαλλήλους (όπως προσωπικές πιστωτικές κάρτες για αγορές μέσω διαδικτύου).

β. Μειονεκτήματα: Από την άλλη πλευρά οι τρέχουσες συνδέσεις μπορεί να επηρεάσουν την απόδοση της βάσης δεδομένων. Όπως επίσης και οι μεγάλες βάσεις δεδομένων ενδεχομένως να επηρεάσουν την απόδοση του προϊόντος.

3.9.3. Λεπτομερής Αντιστοίχιση Αρχείου

Με την λεπτομερή αντιστοίχιση αρχείου (Exact File Matching) λαμβάνουμε το Hash του αρχείου και παρακολουθούμε για κάθε αρχείο το οποίο ταιριάζει ακριβώς στο συγκεκριμένο αποτύπωμα. Ορισμένοι θεωρούν ότι αυτό είναι τεχνική ανάλυσης πλαισίου από τη στιγμή που το ίδιο το περιεχόμενο δεν αναλύεται.

Είναι καλύτερο για αρχεία πολυμέσων ή άλλα δυαδικά αρχεία στα οποία δεν είναι δυνατή η ανάλυση κειμένου.

α. Πλεονεκτήματα: Λειτουργεί με οποιαδήποτε τύπο αρχείου, χαμηλά ποσοστά λαθεμένων συναγερμών ακόμα και με αρκετά μεγάλο hash.

β. Μειονεκτήματα: Δεν υπάρχει τίποτα το ιδιαίτερο να αναφερθεί σαν μειονέκτημα. Δεν αξίζει να χρησιμοποιηθεί για αρχεία που έχουν υποστεί επεξεργασία όπως στάνταρ έγγραφα κειμένου και αρχεία πολυμέσων που έχουν ήδη εκδοθεί ή διανεμηθεί δωρεάν στο διαδίκτυο.

3.9.4. Μερική ταύτιση αρχείου

Αυτή η τεχνική αναζητά για μια πλήρη ή μερική ταύτιση προστατευόμενου αρχείου. Με αυτό τον τρόπο μπορεί να δημιουργηθεί μια πολιτική που προστατεύει ευαίσθητα δεδομένα και η εφαρμογή DLP μπορεί να αναζητάει είτε ολόκληρο το κείμενο από κάποιο αρχείο, είτε ορισμένες μόνο προτάσεις. Για παράδειγμα μπορεί να έχει δημιουργηθεί ένα επιχειρηματικό πλάνο για ένα καινούργιο προϊόν τότε η εφαρμογή DLP θα μπορούσε να σημάνει συναγερμό εάν ένας υπάλληλος αντέγραφε μία παράγραφο μέσα σε ένα απλό μήνυμα. Οι περισσότερες λύσεις βασίζονται στην τεχνική γνωστή σαν cyclical hashing, όταν λαμβάνεις το hash από ένα τμήμα του κειμένου, το οποίο υπάρχει ένα προκαθορισμένος αριθμός χαρακτήρων, τότε παίρνοντας άλλο ένα hush και συνεχίζοντας μέχρι να ολοκληρωθεί όλο το κείμενο. Πολλά προϊόντα χρησιμοποιούν το cyclical hashing σαν βάση και προσθέτουν πιο προχωρημένες εύκαμπτες αναλύσεις.

Μπορεί να θεωρηθεί ότι είναι καλύτερο για προστασία ευαίσθητων αρχείων ή παρόμοιου περιεχομένου όπως είναι τα αρχεία CAD (μαζί με τις επικεφαλίδες κειμένων) και πηγές κώδικα. Αδόμητα δηλαδή δεδομένα τα οποία θεωρούνται όμως ευαίσθητα.

α. Πλεονεκτήματα: Γίνεται φανερό ότι παρέχεται η δυνατότητα προστασίας αδόμητων δεδομένων. Γενικά χαμηλό ποσοστό εσφαλμένων συναγερμών.

β. Μειονεκτήματα: Αντίθετα μπορούμε να αναφέρουμε ότι παρουσιάζει περιορισμένη δυνατότητα στο μέγεθος των κειμένων που μπορεί να προστατεύσει. Κοινές στερεότυπες εκφράσεις μπορεί να επιφέρουν λαθεμένους συναγερμούς. Πρέπει να γνωρίζουν ακριβώς πιο αρχείο πρέπει να προστατεύσουν.

3.9.5. Στατιστική Ανάλυση.

Με την στατιστική ανάλυση (Statistical Analysis) πραγματοποιείται χρησιμοποίηση της γνώσης των μηχανών, όπως η ανάλυση Bayesian, και άλλων στατιστικών τεχνικών για να αναλύσουμε το σώμα του περιεχόμενου. Με αυτόν τον τρόπο έχουμε την δυνατότητα να βρούμε παραβιάσεις στην πολιτική μέσα σε κάποιο κείμενο, που μοιάζει με το κείμενο που θέλουμε να προστατεύσουμε. Αυτή η κατηγορία περιλαμβάνει ένα μεγάλο εύρος στατιστικών τεχνικών που ποικίλουν σε βαθμό σε ότι αφορά την εφαρμογή τους και την αποτελεσματικότητά τους. Κάποιες τεχνικές είναι παρόμοιες με αυτές που χρησιμοποιούνται στο μπλοκάρισμα των spam.

Είναι καλύτερο για αδόμητα περιεχόμενα, όπου η τεχνική της ταύτισης του εγγράφου μπορεί να είναι αναποτελεσματική. Για παράδειγμα, μια θέση αποθήκευσης μηχανολογικών σχεδίων τα οποία είναι ανέφικτο να φορτωθούν για την μερική ταύτιση κειμένου, λόγο μεγάλου όγκο δεδομένων.

α. Πλεονεκτήματα: Μπορεί να δουλέψει περισσότερα με «νεφελώδη» περιεχόμενα, στα οποία δεν είμαστε σε θέση να απομονώσουμε τα ακριβή έγγραφα για να πραγματοποιηθεί ο έλεγχος εάν ταιριάζουν. Μπορεί να επιβάλλουν πολιτικές όπως «συναγερμός σε οτιδήποτε εξέρχεται υπό την μορφή εγγράφου από αυτόν τον κατάλογο».

β. Μειονεκτήματα: Επιρρεπείς σε λαθεμένους συναγερμούς και λαθεμένα αποτελέσματα. Απαιτεί ένα μεγάλο μέρος του περιεχομένου της πηγής. Όσο μεγαλύτερο τόσο το καλύτερο.

3.9.6. Εννοιολογική.

Η εννοιολογική (Conceptual/Lexicon) τεχνική χρησιμοποιεί ένα συνδυασμό από λεξικά, κανόνες και άλλες αναλύσεις για να προστατεύσουν ένα «νεφελώδες» περιεχόμενο που μοιάζει με «ιδέα». Για παράδειγμα, μια πολιτική η οποία προειδοποιεί για την κίνηση που μοιάζει με εκμετάλλευση εμπιστευτικών πληροφοριών και η οποία χρησιμοποιεί φράσεις κλειδιά, μέτρημα λέξεων καθώς και θέσεις για να εντοπιστούν ενδεχόμενες παραβιάσεις.

Στην περίπτωση αυτή είναι καλύτερο για εντελώς αδόμητα δεδομένα που δεν υπάρχει απλή κατηγοριοποίηση με βάση αντίστοιχα γνωστά έγγραφα, βάσεις δεδομένων ή άλλες γνωστές πηγές.

α. Πλεονεκτήματα: Δεν είναι όλες οι εταιρικές πολιτικές ή το περιεχόμενό τους, που μπορεί να περιγραφή χρησιμοποιώντας συγκεκριμένα παραδείγματα. Η εννοιολογική ανάλυση μπορεί να βρει χαλαρές παραβιάσεις από ορισμένες πολιτικές και οι οποίες δεν μπορούν να ανιχνευθούν από άλλες τεχνικές ή καν να παρακολουθηθούν.

β. Μειονεκτήματα: Στις περισσότερες περιπτώσεις δεν υπάρχουν έτοιμοι κανόνες και η εταιρία που θα δημιουργήσει και θα αναπτύξει μια εφαρμογή DLP πρέπει να τα δημιουργήσει από την αρχή, καταβάλλοντας επιπρόσθετη και σημαντική προσπάθεια, οπότε όπως είναι φυσιολογικό επακόλουθο, κοστίζει και περισσότερο. Εξαιτίας των χαλαρών κανόνων είναι πολύ επιρρεπής σε λαθεμένους συναγερμούς και λαθεμένα αποτελέσματα.

3.9.7 Κατηγορίες

Οι κατηγορίες κατασκευάζονται από πριν, με κανόνες και καταλόγους για τα πιο κοινά είδη ή τύπους ευαίσθητων δεδομένων, όπως είναι οι πιστωτικές κάρτες, αριθμούς κοινωνικής ασφάλισης, αριθμός φορολογικού μητρώου.

Η τεχνική αυτή είναι καλύτερη για οτιδήποτε ταιριάζει με την αντίστοιχη κατηγορία που προσφέρεται. Τυπικά είναι εύκολο να περιγραφεί το περιεχόμενο προσωπικών δεδομένων ή η προστασία συγκεκριμένων εμπιστευτικών δεδομένων βάσει συγκεκριμένων οδηγιών που έχουν δοθεί από την διοίκηση.

α. Πλεονεκτήματα: Είναι εξαιρετικά απλό να ρυθμιστεί. Μας δίνεται η δυνατότητα να εξοικονομηθεί χρόνος στη δημιουργία μιας πολιτικής. Στη συνέχεια οι κατηγορίες αυτές στις πολιτικές μπορεί να αποτελέσουν την βάση για πιο προχωρημένες – αναβαθμισμένες πολιτικές, πιο συγκεκριμένες για έναν οργανισμό. Είναι αξιοπρόσεκτο ότι για πολλούς οργανισμούς οι κατηγορίες αυτές μπορούν να καλύψουν ένα μεγάλο ποσοστό από τις ανάγκες τους στη προστασία δεδομένων.

β. Μειονεκτήματα: Όπως είναι αναμενόμενο είναι ένα μέγεθος, ένα είδος για όλα, με αποτέλεσμα να μπορεί να μην ταιριάζει σε κάποιες περιπτώσεις. Λειτουργούν μόνο με ευκρινές περιεχόμενο και κανόνες οι οποίοι είναι εύκολα κατηγοροποιήσιμοι.

Αυτές οι 7 τεχνικές αποτελούν την βάση για τις περισσότερες εφαρμογές DLP που κυκλοφορούν στην αγορά. Όπως είναι φυσιολογικό επακόλουθο δεν συμπεριλαμβάνουν όλα τα προϊόντα όλες τις τεχνικές, καθώς επίσης μπορεί να υπάρξουν σημαντικές διαφορές μεταξύ των εφαρμογών. Οι περισσότερες εφαρμογές μπορούν να συνδέουν τεχνικές, να κατασκευάζουν πολύπλοκες – σύνθετες πολιτικές από τους συνδυασμούς του περιεχομένου και των τεχνικών ανάλυσης συναφούς περιεχομένου.

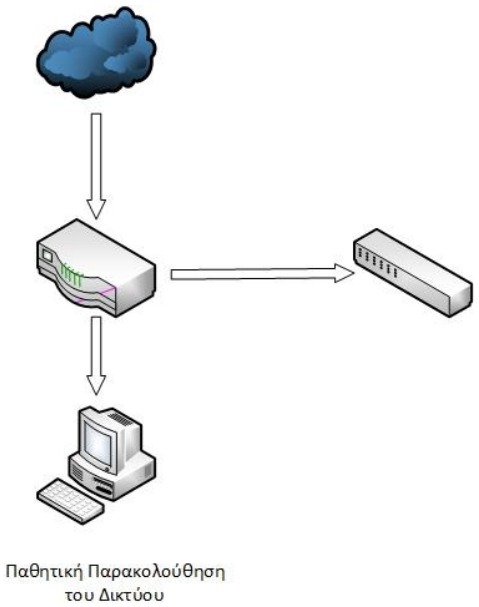
3.10 Αρχιτεκτονική της Τεχνικής.

3.10.1 Δεδομένα σε Κίνηση.

Αρχικά οι περισσότεροι οργανισμοί ξεκίνησαν την ανάπτυξη των εφαρμογών DLP με λύσεις βασιζόμενες στο δίκτυο και προέβαλαν την προστασία για συστήματα είτε έχοντας διαχείριση ή ακόμα και χωρίς διαχείριση. Είναι φανερό ότι τυπικά είναι πιο εύκολο να ξεκινήσει κάποιος με ανάλογες εφαρμογές και στη συνέχεια να αναπτυχθεί αυτόνομα. Οι αρχικές εφαρμογές έφταναν μέχρι το σημείο της παρακολούθησης και της προειδοποίησης. Στη συνέχεια όλες οι εφαρμογές που συμπεριλαμβάνουν προηγμένες τεχνικές, συμπεριλαμβάνονται στην υπάρχουσα υποδομή του δικτύου και προβάλουν ασφάλεια και όχι μόνο παρακολούθηση και έλεγχο.

3.10.1.1. Παρακολούθηση Δικτύου.

Στην καρδιά των περισσοτέρων εφαρμογών DLP βρίσκεται η παθητική παρακολούθηση του δικτύου. Ο συγκεκριμένος σχεδιασμός βασίζεται στην ανάπτυξη της εφαρμογής DLP ακριβώς στην πύλη (gateway) ή κοντά σε αυτήν, πάνω σε μια Switched Port Analyzer. Με αυτόν τον τρόπο γίνεται φανερό ότι από εκεί μπορεί να πραγματοποιεί, πλήρη σύλληψη των πακέτων, ανακατασκευή συνεδριών και ανάλυση περιεχομένου σε πραγματικό χρόνο. Η απόδοση είναι πιο πολύπλοκη και λεπτή από αυτή που οι δημιουργοί λογισμικού συζητούν. Οι χρήστες που καταλήγουν στην υιοθέτηση μιας εφαρμογής DLP συνήθως ενημερώνουν και επιθυμούν από την σύνδεση Ethernet που διαθέτουν την πλήρη αξιοποίηση των δυνατοτήτων που αυτή προσφέρει. Δηλαδή επιθυμούν να έχουν διαθέσιμο προς χρησιμοποίηση όλο το φάσμα των gigabit που ,τους προσφέρει η σύνδεσή τους. Παρόλα αυτά είναι γεγονός ότι το συγκεκριμένο επίπεδο απόδοσης ενός δικτύου, δηλαδή της πλήρης κάλυψης της διαθέσιμης χωρητικότητας μεταφοράς, είναι αχρείαστο για τους περισσότερους οργανισμούς εκτός ορισμένων εξαιρέσεων κατά τις οποίες κάποιος οργανισμός θα έχει αυξημένη τηλεπικοινωνιακή κίνηση.

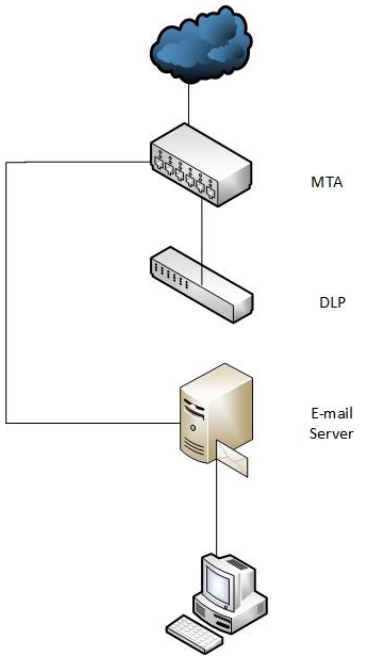


Εικόνα 4:Παθητική Παρακολούθηση Δικτύου

Το DLP είναι ένα εργαλείο το οποίο παρακολουθεί την επικοινωνία των υπαλλήλων και δεν παρακολουθεί την κυκλοφορία web εφαρμογών. Στην πραγματικότητα έχει παρατηρηθεί ότι οι μικρές επιχειρήσεις κανονικά τρέχουν κάτω από 50 Mbytes/s της σχετικής κυκλοφορίας, οι μεσαίου μεγέθους επιχειρήσεις τρέχουν από 50 – 200 Mbytes/s και οι μεγάλες επιχειρήσεις γύρω στα 300 MB/s (σε μερικές περιπτώσεις

μέχρι και 500). Εξαιτίας της αύξησης της ανάλυσης του περιεχομένου, όλα τα προϊόντα δεν τρέχουν πλήρως όλα τα πακέτα.

3.10.1.2 Ενσωμάτωση Ηλεκτρονικού Ταχυδρομείου.



Εικόνα 5: Ενσωμάτωση Ηλεκτρονικού Ταχυδρομείου

Το επόμενο βήμα είναι η ενσωμάτωση στο ηλεκτρονικό ταχυδρομείο (e-mail). Όπως γνωρίζουμε το e-mail αποθηκεύεται ή προωθείται, με αποτέλεσμα να έχουμε την δυνατότητα να εφαρμόσουμε πολλές επιλογές, όπως είναι για παράδειγμα η «καραντίνα», η ενσωμάτωση κρυπτογραφίας καθώς και το φιλτράρισμα χωρίς οι επιλογές αυτές να δημιουργούν δυσκολίες, αποφεύγοντας το μπλοκάρισμα της κίνησης. Ταυτόχρονα οι περισσότερες εφαρμογές ενσωματώνουν ένα MTA (Mail Transport Agent) μέσα στο προϊόν, επιτρέποντας απλά να το προσθέσουμε ως ένα επιπλέον βήμα στην αλυσίδα των e-mail. Αρκετοί δημιουργοί επίσης ενσωματώνουν απευθείας μαζί με την κύρια υπάρχουσα επιλογή MTA, διάφορες εφαρμογές ασφαλείας ηλεκτρονικού ταχυδρομείου (e-mail) για καλύτερη απόδοση. Στο σημείο αυτό είναι σκόπιμο να αναφέρουμε ένα μειονέκτημα της συγκεκριμένης προσέγγισης, το οποίο είναι ότι δεν αποκτάει πρόσβαση σε ολόκληρο το ηλεκτρονικό ταχυδρομείο (e-mail). Ακόμα στη περίπτωση που χρησιμοποιούμε Exchange Server ολόκληρα τα μηνύματα ποτέ δεν περνάνε μέσω του MTA από τη στιγμή που δεν υπάρχει λόγος να σταλεί η «κίνηση» εκτός δικτύου. Για να παρακολουθηθεί το εσωτερικό δίκτυο χρειάζεται να ενσωματωθεί απευθείας ο Exchange Server, το οποίο είναι εκπληκτικά σπάνιο στην αγορά. Τέλος μια πλήρη ενσωμάτωση είναι διαφορετική από μία απλή σάρωση αρχείων καταγραφής, το οποίο ονομάζουν ορισμένες εταιρίες εσωτερική υποστήριξή ταχυδρομείου. Μια σωστή ενσωμάτωση ηλεκτρονικού ταχυδρομείου (e-mail) είναι απολύτως κρίσιμη εάν θέλουμε να πραγματοποιήσουμε φιλτράρισμα, σε αντίθεση από την απλή παρακολούθηση.

3.10.1.3 Ενσωμάτωση Φιλτράρισμα ή Μπλοκάρισμα στον Μεσολαβητή.

Είναι σχεδόν σίγουρο ότι ο καθένας ο οποίος επιθυμεί να αναπτύξει μια εφαρμογή DLP θέλει να ξεκινήσει μπλοκάροντας όλη την κίνηση. Είναι αδιαμφισβήτητο γεγονός ότι δεν θα πάρει πολύ χρόνο από το να δούμε όλα τα ευαίσθητα δεδομένα να κυκλοφορούν στην περιοχή του διαδικτύου, πριν λάβουμε κάποια μέτρα ασφαλείας. Από την άλλη μεριά όμως η επιλογή να μπλοκάρουμε τελείως την κυκλοφορία δεν αποτελεί την πιο εύκολη και εύχρηστη εφαρμογή σε έναν οργανισμό, ειδικά όταν επιτρέπουμε μόνο τη καλή «κίνηση», μπλοκάρουμε την κακή, και λαμβάνοντας την απόφαση χρησιμοποιώντας την ανάλυση περιεχομένου σε πραγματικό χρόνο. Το ηλεκτρονικό ταχυδρομείο (e-mail) όπως αναφέραμε είναι αρκετά εύκολο

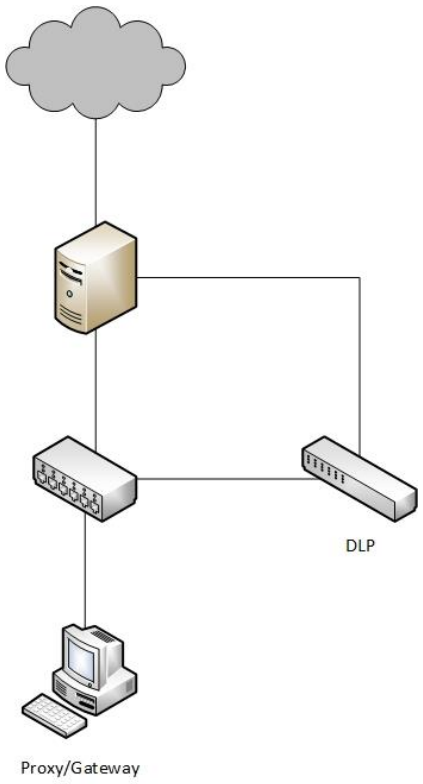
στο να φιλτράρεται. Δεν είναι ακριβώς σε πραγματικό χρόνο αφού είναι μέσω proxy. Πέρα από το ηλεκτρονικό ταχυδρομείο (e-mail) η περισσότερη επικοινωνιακή κίνηση είναι «συγχρονισμένη», τα πάντα τρέχουν δηλαδή σε πραγματικό χρόνο. Επομένως εάν θέλουμε να το φιλτράρουμε το οτιδήποτε θα πρέπει είτε να γεφυρώσουμε τη κίνηση, είτε να το προωθήσουμε (proxy) ή είτε να το «δηλητηριάσουμε» από έξω.

α. Γέφυρα.

Με μια γέφυρα (bridge) απλά έχουμε ένα σύστημα με δύο κάρτες δικτύου (network cards) που εκτελεί ανάλυση περιεχομένου στη μέση. Εάν παρατηρήσουμε κάτι κακό, η γέφυρα διακόπτει την σύνδεση για αυτή την περίοδο. Παρόλα αυτά η γεφύρωση δεν είναι η καλύτερη προσέγγιση για μια εφαρμογή DLP δεδομένου ότι μπορεί να μην σταματήσει όλη την διαβαθμισμένη κίνηση πριν αυτή διαρρεύσει. Μπορεί να παρομοιαστεί με έναν άνθρωπο ο οποίος κάθεται σε μία πόρτα με ένα μεγεθυντικό φακό βλέποντας οτιδήποτε περνάει, συγκεντρωμένος δηλαδή σε ένα σημείο. Την στιγμή που θα είχαμε αυξημένη κίνηση για να πραγματοποιήσουμε μια εμπεριστατωμένη απόφαση, ενδεχομένως να έχουμε χάσει το ενδιαφερόμενο μέρος.

β. Μεσολαβητής (Proxy)

Γνωρίζουμε με απλούς όρους ότι μεσολαβητής (proxy) είναι ένα πρωτόκολλο/εφαρμογή που τοποθετεί σε συγκεκριμένη ουρά την κυκλοφορία πριν την περάσει, επιτρέποντας βαθύτερη ανάλυση. Παρατηρούμε τις πύλες (gateways) των μεσολαβητών (proxys) ως επί το πλείστο για HTTP, FTP και IM πρωτόκολλα. Λίγες εφαρμογές DLP ενσωματώνουν τους δικούς τους μεσολαβητές (proxys). Παρατηρείται η ενδεχόμενη ενσωμάτωσή τους με τις ήδη υπάρχουσες gateways/proxy από την στιγμή που οι περισσότεροι χρήστες, προτιμούν την ενσωμάτωση με τα υπάρχουσα εργαλεία που διαθέτουν. Η ένταξη για web gateways τυπικά είναι μέσου του πρωτοκόλλου iCAP, επιτρέποντας στον proxy να μεταβιβάζει την κίνηση ώστε να την στέλνει στο DLP για ανάλυση και να κόβει την επικοινωνία εάν υπάρχει παραβίαση. Αυτό σημαίνει ότι δεν χρειάζεται να προσθέσουμε ένα ξεχωριστό υλικό (hardware) μπροστά από το δίκτυό και επίσης αποφεύγεται η δυσκολία της δημιουργίας ξεχωριστού δικτύου για την εσωτερική ανάλυση. Εάν η gateway συμπεριλαμβάνει μια ανάστροφη μεσολαβητή SSL μπορούμε να «μυριστούμε» (sniff) και SSL συνδέσεις. Σε αυτή την περίπτωση θα χρειαστούμε να πραγματοποιήσουμε ορισμένες αλλαγές στους τερματικούς σταθμούς εξαιτίας των πιστοποι-



Εικόνα 6:Μεσολαβητής (Proxy)

ητικών ασφαλείας. Στη συνέχεια χρησιμοποιούμε με τον ίδιο τρόπο το κρυπτογραφημένο δίκτυο. Για IM θα χρειαστούμε έναν IM proxy και μια εφαρμογή DLP η οποία θα υποστηρίζει οποιοδήποτε πρωτόκολλο IM χρησιμοποιούμε.

γ. Δηλητηρίαση TCP (TCP Poisoning).

Η τελευταία μέθοδος του φιλτραρίσματος είναι η δηλητηρίαση TCP (TCP Poisoning). Πραγματοποιείται η παρακολούθηση της κίνησης του δικτύου και όταν παρατηρήσουμε κάποια παραβίαση της πολιτικής ασφαλείας, αποστέλλουμε «εκχύνουμε» ένα πακέτο επανεκκίνησης (TCP reset πακέτο) για να κόψουμε την σύνδεση. Αυτή η μέθοδος δουλεύει για κάθε TCP πρωτόκολλο αλλά δεν είναι πολύ αποτελεσματική. Ένα μειονέκτημα που μπορεί να παρατηρηθεί είναι ότι ορισμένα πρωτόκολλα θα συνεχίζουν την προσπάθεια αποκατάστασης της σύνδεσης. Για παράδειγμα εάν το TCP δηλητηριάσει ένα μήνυμα ηλεκτρονικού ταχυδρομείου, ο εξυπηρετητής (server) θα συνεχίσει να στέλνει το μήνυμα για 3 μέρες και για κάθε 15 λεπτά. Επίσης άλλο ένα μειονέκτημα είναι παρόμοιο με αυτό της «γεφύρωσης». Την στιγμή που δεν τοποθετούνται όλα στην ουρά, και παρατηρήσουμε κάποια παραβίαση, μπορεί να είναι ήδη πολύ αργά. Μπορούμε τέλος να αναφέρουμε ότι είναι μια καλή μέθοδος για να καλυφθούν τα κενά από μη σταθερά πρωτόκολλα, αλλά θα χρειαστούμε όσο τον δυνατόν περισσότερους μεσολαβητές (proxy).

3.10.1.4. Εσωτερικά Δίκτυα

Μπορούμε να σημειώσουμε ότι τεχνικά υπάρχει η δυνατότητα να παρακολουθηθεί εσωτερικά ένα δίκτυο, παρόλα αυτά μία εφαρμογή DLP σπάνια χρησιμοποιείται για την κίνηση του εσωτερικού δικτύου εκτός από το ηλεκτρονικό ταχυδρομείο (e-mail). Οι πύλες (gateways) στις οποίες θα τοποθετηθεί θα παρουσιάσουν ενδείξεις συμφόρησης. Κατά συνέπεια η παρακολούθηση του εσωτερικού δικτύου είναι μια αποθαρρυντική προοπτική από θέμα κόστους, απόδοσης, καθώς πολιτικής διαχείρισης αληθινών ή ψευδών ενδείξεων.

3.10.1.5. Κατανεμημένη και Ιεραρχημένη Ανάπτυξη

Η σημερινή ανάπτυξη της τεχνολογίας, με τις επιλογές που μας έχει προσφέρει, ειδικότερα στους οργανισμούς, δίνει την δυνατότητα σε αυτούς ότι μέγεθος και αν έχουν, είτε μεσαίοι είτε μεγάλοι να διαθέτουν πολλαπλές τοποθεσίες και πύλες (gateways) στο διαδίκτυο (web). Μια εφαρμογή DLP θα πρέπει να υποστηρίζει, την παρακολούθηση πολλαπλών σημείων, η οποία θα συμπεριλαμβάνει μια μίξη από παθητική παρακολούθηση του δικτύου, των σημείων μεσολάβησης (proxy), των εξυπηρετητών ηλεκτρονικού ταχυδρομείου (e-mail server) και των απομακρυσμένων τοποθεσιών. Μολονότι η επεξεργασία και η ανάλυση μπορούν να μεταφορτωθούν σε απομακρυσμένα σημεία, θα πρέπει να αποσταλούν τα συμβάντα πίσω σε ένα κεντρικό εξυπηρετητή (server) διαχείρισης για καθορισμό της ροής εργασίας, για υποβολή αναφορών – εκθέσεων, για έρευνα και αρχειοθέτηση. Τα απομακρυσμένα γραφεία

είναι συνήθως εύκολα να υποστηριχθούν, από την στιγμή που προωθούνται οι πολιτικές από πάνω προς τα κάτω και οι αναφορές στη συνέχεια προς τα πίσω πάλι.

Ορισμένες εφαρμογές DLP είναι περισσότερο αναπτυγμένες και δίνουν την δυνατότητα να υποστηρίζουν ιεραρχικές αναπτύξεις για οργανισμούς που επιθυμούν να διαχειρίζονται το DLP διαφορετικά σε κάθε ξεχωριστό τμήμα το οποίο βρίσκεται σε διαφορετική τοποθεσία ή ακόμα και σε κάθε διαφορετικό τμήμα του οργανισμού. Δεν θα πρέπει όμως να μας διαφεύγει το γεγονός ότι όλες οι διεθνείς οργανισμοί που διαθέτουν παραρτήματα σε χώρες διαφορετικές από αυτήν της εθνικότητάς τους, υποχρεώνονται να συμμορφώνονται με τους νόμους περί παρακολούθησης που ισχύουν στις διάφορες χώρες. Επίσης η ιεραρχική διαχείριση υποστηρίζει ακόμα συντονισμό με τις τοπικές πολιτικές από την κεντρική διοίκηση και την επιβολή της σε διαφορετικές περιφέρειες που βρίσκονται σε διαφορετικές τοποθεσίες, τρέχοντας στους δικούς τους εξυπηρετητές (server) διαχείρισης και επικοινωνώντας πίσω σε έναν κεντρικό εξυπηρετητή διαχείρισης. Μπορούμε να παρατηρήσουμε ότι τα πρώτα προϊόντα υποστήριζαν μόνο την διαχείριση ενός εξυπηρετητή (server). Τώρα μπορούμε να αναφέρουμε ότι διαθέτουμε τις επιλογές να αντιμετωπίσουμε όλες αυτές τις διάσπαρτες καταστάσεις, υιοθετώντας μία μίξη εταιρικών, περιφερειακών, τμημάτων και μονάδων πολιτικών, υποβολής αναφορών καθώς και ιεραρχικής ανάπτυξης.

3.10.2 Δεδομένα σε κατάσταση Ηρεμίας.

Είναι γεγονός ότι υπάρχει η δυνατότητα να συλληφθούν οι διαρροές στο δίκτυο. Ωστόσο αυτές είναι μόνο ένα μικρό κομμάτι του προβλήματος. Πολλοί οργανισμοί ακόμα και ιδιώτες θεωρούν εξίσου πολύτιμο, αν όχι το πολυτιμότερο, το να καταλάβουν που αποθηκεύονται όλα αυτά τα δεδομένα αρχικά. Το συγκεκριμένο το ονομάζουμε ανεύρεση Περιεχομένου (content discovery). Τα εργαλεία αναζήτησης που διαθέτει ένας οργανισμός, μπορεί να είναι σε θέση να μας βοηθήσουν, αλλά είναι γεγονός ότι δεν είναι αποτελεσματικά, για το συγκεκριμένο είδος του προβλήματος. Επίσης τα εργαλεία ταξινόμησης των δεδομένων της επιχείρησης μπορούν επίσης να βοηθήσουν, ωστόσο δεν φαίνεται να λειτουργεί αποτελεσματικά για την ανεύρεση παραβιάσεων κάποιας συγκεκριμένης πολιτικής. Έτσι βλέπουμε πολλούς δημιουργούς να χρησιμοποιούν τα χαρακτηριστικά της ανεύρεσης περιεχομένου στις εφαρμογές DLP.

Αξίζει, επιπλέον να αναφερθούμε ότι το μεγαλύτερο πλεονέκτημα της ανεύρεσης περιεχομένου σε μια εφαρμογή DLP, είναι η ότι επιτρέπει να πάρουμε μια απλή πολιτική και να την εφαρμόσουμε σε όλα τα δεδομένα ανεξαρτήτως του μέρος όπου αυτά βρίσκονται αποθηκευμένα, ανεξάρτητα πως διανέμονται και ανεξάρτητα πως χρησιμοποιούνται. Για παράδειγμα μπορούμε να ορίσουμε μια πολιτική η οποία να απαιτεί την κρυπτογράφηση των αριθμών πιστωτικών καρτών πριν αποσταλούν με ηλεκτρονικό ταχυδρομείο και να μην διαμοιράζονται με HTTP ή HTTPS, να αποθηκεύονται μόνο σε συγκεκριμένους εγκεκριμένους διακομιστές και να αποθηκεύονται

σε σταθμούς εργασίας και φορητούς υπολογιστές μόνο των υπαλλήλων του λογιστικού τμήματος. Όλα αυτά μπορούν να καθοριστούν σε μια ενιαία πολιτική στον κεντρικό διακομιστή διαχείρισης.

Είναι χρήσιμο να επισημανθεί επίσης ότι η ανεύρεση περιεχομένου αποτελείται από τρία στοιχεία:

α. Ανεύρεση στον τερματικό σταθμό εργασίας.

Είναι κατανοητό ότι Ανιχνεύει σταθμούς εργασίας και φορητούς υπολογιστές για περιεχόμενα τα οποία παραβιάζουν τις συγκεκριμένες πολιτικές ασφαλείας.

β. Ανεύρεση Αποθηκευμένων:

Ανιχνεύει μαζικές αποθηκεύσεις, συμπεριλαμβανομένων των διακομιστών (Server) αρχείων, SAN και NAS.

γ. Ανεύρεση Server:

Ανίχνευση συγκεκριμένων εφαρμογών σε αποθηκευμένα δεδομένα σε email Server, συστήματα διαχείρισης εγγράφων και βάσεις δεδομένων (δεν αποτελεί χαρακτηριστικό των περισσοτέρων εφαρμογών DLP αλλά έχει ξεκινήσει να εμφανίζεται σε ορισμένες εφαρμογές Παρακολούθησης Δραστηριότητας Βάσεων Δεδομένων).

3.10.2.1. Τεχνικές Ανεύρεση Περιεχομένου.

Προχωρώντας μπορούμε να διαπιστώσουμε ότι υπάρχουν 3 βασικές τεχνικές για ανεύρεση περιεχομένου (Content Discovery Techniques):

α. Απομακρυσμένη Ανίχνευση.

Στην απομακρυσμένη ανίχνευση (Remote Scanning) πραγματοποιείται μια σύνδεση με τον διακομιστή (Server) ή με την συσκευή που χρησιμοποιείται για τον διαμοιρασμό αρχείων ή πρωτόκολλα εφαρμογών, και στη συνέχεια η ανίχνευση εκτελείται από απόσταση. Ουσιαστικά είναι η τοποθέτηση ενός απομακρυσμένου δίσκου και η σάρωση του από ένα διακομιστή οποίος λαμβάνει πολιτικές και στέλνει τα αποτελέσματα στον κεντρικό διακομιστή, ο οποίος περιέχει την κεντρική πολιτική. Για ορισμένους οργανισμούς αυτό είναι μια συσκευή, για άλλες είναι ένας κοινός διακομιστής και για μικρότερους οργανισμούς μπορεί να είναι ενσωματωμένο στον κεντρικό διακομιστή διαχείρισης.

β. Ανίχνευση βασισμένη σε αντιπρόσωπο – πράκτορα.

Ένας πράκτορας (agent) εγκαθίστανται στο σύστημα (Server) για να ανιχνεύει τυχόν παραβιάσεις της πολιτικής. Η συγκεκριμένη ανίχνευση πραγματοποιείται σε τοπικό επίπεδο. Οι πράκτορες είναι συγκεκριμένη πλατφόρμα και χρησιμοποιεί τους κύκλους της τοπικής CPU. Παρόλα αυτά μπορεί να εκτελέσει ανίχνευση ταχύτερα ειδικά για μεγάλους αποθηκευτικούς χώρους. Τέλος για τους τερματικούς

σταθμούς εργασίας αυτός θα μπορούσε να είναι ο ίδιος που χρησιμοποιείται για την εφαρμογή του ελέγχου Data in Use.

γ. Ανίχνευση από πράκτορα εγκατεστημένο στη μνήμη.

Υπάρχει η δυνατότητα αντί για να εγκαταστήσουμε πλήρως έναν πράκτορα, τον εγκαθιστούμε στη μνήμη για να πραγματοποιήσει την ανίχνευση, στη συνέχεια σταματάει τη λειτουργία του χωρίς να αφήνει τίποτα να λειτουργεί ή να αποθηκευτεί στο τοπικό σύστημα. Αυτό προσφέρει τις δυνατότητες του πράκτορα στη περίπτωση που δεν θέλουμε να λειτουργεί συνέχεια.

Από όλα τα παραπάνω γίνεται κατανοητό ότι κάθε μία από αυτές τις τεχνολογίες μπορεί να λειτουργήσει με οποιαδήποτε τρόπο, οι οργανισμοί τυπικά θα αναπτύξουν μια μίξη η οποία εξαρτάται από την πολιτική ασφαλείας, τις απαιτήσεις καθώς και την διαθεσιμότητα και υποστήριξη των υποδομών. Εντούτοις γίνεται κατανοητό ότι είναι φυσιολογικό να υπάρξουν και ορισμένοι περιορισμοί της τεχνολογίας για κάθε προσέγγιση και οι οποίοι περιορισμοί όπως είναι αναμενόμενο καθοδηγούν την ανάπτυξη. Μπορούμε συγκεκριμένα να αναφέρουμε:

α. Απομακρυσμένη Ανίχνευση.

Μπορεί να αυξήσει σημαντικά την κίνηση και έχει όρια στην επίδοση βασιζόμενα στο bandwidth του δικτύου καθώς επίσης στις επιδόσεις του στόχου και στην ανίχνευση. Ορισμένες εφαρμογές DLP μπορούν να ανιχνεύσουν μόνο gigabytes ανά μέρα. Έχουν δηλαδή την δυνατότητα να ανιχνεύσουν μερικές εκατοντάδες, αλλά όχι terabytes ανά μέρα. Επομένως ορισμένους διακομιστές (Server) περιορίζονται από αυτά τα πρακτικά όρια. Οπότε είναι εύκολα αντιληπτό ότι είναι ανεπαρκή για μεγάλους αποθηκευτικούς χώρους.

β. Πράκτορες, προσωρινοί ή μόνιμοι.

Επιπροσθέτως κατά την χρησιμοποίηση πράκτορα, περιορίζεται από την υπολογιστική ισχύ και την μνήμη του συστήματος προορισμού. Κατά συνέπεια πραγματοποιείται περιορισμός του αριθμού των πολιτικών που μπορεί να εφαρμοστεί καθώς και περιορισμό στους τύπους της ανάλυσης περιεχομένου που μπορούν να χρησιμοποιηθούν. Για παράδειγμα, οι περισσότεροι αντιπρόσωποι που βρίσκονται στους τερματικούς σταθμούς (end point) δεν είναι διαθέσιμοι για μερικό ταίριασμα εγγράφων ή “δακτυλικών” αποτυπωμάτων σε βάθος σε μεγάλες βάσεις δεδομένων. Το γεγονός αυτό είναι αναμενόμενο αφού οι στόχοι του αντιπροσώπου τερματικού σταθμού (end point) είναι πιο περιορισμένοι.

γ. Τέλος αξίζει να σημειωθεί ότι οι πράκτορες δεν υποστηρίζουν όλες τις πλατφόρμες.

3.10.2.2 Ενέργειες και Επιβολές στα Δεδομένα σε κατάσταση ηρεμίας.

Στη συνέχεια είναι αναμενόμενο να προσδιοριστούν και να καθοριστούν οι δυνατότητες και οι ενέργειες που μπορούμε να πραγματοποιήσουμε μόλις ανακαλυφθεί παραβίαση μιας πολιτικής ασφαλείας (Data at Rest Enforcement). Η εφαρμογή DLP μπορεί να πραγματοποιήσει διάφορες ενέργειες, οι κυριότερες εκ των οποίων αναλύονται παρακάτω:

α. Ειδοποίηση/Αναφορά.

Κατά την ειδοποίηση/αναφορά (Alert/Report), δημιουργείται ένα περιστατικό στο κεντρικό διακομιστή διαχείρισης, όπως ακριβώς γίνεται και με την παραβίαση του δικτύου.

β. Προειδοποίηση.

Κατά την προειδοποίηση (Warn) πραγματοποιείται ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείου (email) ότι μπορεί να γίνεται παραβίαση της πολιτικής.

γ. Καραντίνα και Ειδοποίηση.

Όταν πραγματοποιείται Καραντίνα και Ειδοποίηση (Quarantine/ Notify) γίνεται μετακίνηση του αρχείου στον κεντρικό διακομιστή διαχείρισης, αφήνοντας ένα αρχείο κειμένου για το πως μπορεί να γίνει η ανάκτηση του αρχείου.

δ. Καραντίνα και Κρυπτογράφηση.

Όταν πραγματοποιείται Καραντίνα και Κρυπτογράφηση (Quarantine / Encrypt) του αρχείου στη θέση του, συνήθως αφήνοντας ένα απλό κείμενο περιγράφοντας πώς να ζητηθεί η αποκρυπτογράφηση.

ε. Καραντίνα/Έλεγχος Πρόσβασης.

Στην περίπτωση που επιβάλλεται Καραντίνα και έλεγχος Πρόσβασης (Quarantine/ Access Control), πραγματοποιείται αλλαγή του ελέγχου πρόσβασης για να περιοριστεί η πρόσβαση στο αρχείο.

στ. Μετακίνηση ή Διαγραφή:

Σύμφωνα με την Μετακίνηση ή Διαγραφή (Remove/Delete), αυτή είτε μετακινεί το αρχείο στον κεντρικό διακομιστή διαχείρισης χωρίς ειδοποίηση ή απλά το διαγράφει.

Γίνεται επομένως εύκολα αντιληπτό ότι ένας συνδυασμός διαφορετικών αρχιτεκτονικών ανάπτυξης, τεχνικών ανεύρεσης και επιλογών εφαρμογής, δημιουργούν έναν ισχυρό συνδυασμό για τη προστασία δεδομένων σε κατάσταση ηρεμίας και στηρίζοντας ταυτόχρονα τις πρωτοβουλίες συμμόρφωσης. Με βάση πάντα τις πολιτικές ασφαλείας που έχει επιλέξει η διοίκηση και εφαρμόζονται ιεραρχικά.

3.10.3 Δεδομένα σε Χρήση.

Επιπροσθέτως αναφέρουμε στο σημείο αυτό και τα δεδομένα τα οποία χρησιμοποιούνται σε πραγματικό χρόνο από τους χρήστες. Μια εφαρμογή DLP συνήθως ξεκινά από το δίκτυο γιατί αυτός είναι ο πιο οικονομικός τρόπος να πάρουμε ευρύτερη κάλυψη. Η παρακολούθηση του δικτύου είναι μη παρεμβατική. Στο δίκτυο παρεμβαίνουμε μόνο όταν υπάρχουν SSL. Με αυτόν τον τρόπο προσφέρεται ορατότητα σε καθένα σύστημα στο δίκτυο, είτε διαχείρισης, είτε διαχειριζόμενο, σε διακομιστή ή σε σταθμός εργασίας. Παρόλα αυτά το φιλτράρισμα είναι πιο δύσκολο αλλά πάλι είναι απλό στο δίκτυο (ειδικά για ηλεκτρονικό ταχυδρομείο) και καλύπτει όλα τα συστήματα που συνδέονται με το δίκτυο. Επομένως γίνεται σαφές ότι αυτό δεν είναι μια ολοκληρωμένη λύση. Δεν προστατεύει τα δεδομένα όταν κάποιος τα παίρνει εκτός γραφείου με ένα laptop, και δεν μπορεί να αποτρέψει τους ανθρώπους από το να αντιγράψουν δεδομένα σε φορητές αποθηκευτικές συσκευές όπως τα USB Sticks. Για να μετακινηθούμε από μια εφαρμογή όπου προστατεύει τις διαρροές σε μια εφαρμογή κατά την οποία προστατεύονται οι πληροφορίες και τα δεδομένα, γίνεται εύκολα αντιληπτό ότι οι εφαρμογές θα πρέπει να επεκταθούν όχι μόνο στα δεδομένα και στις πληροφορίες που αποθηκεύονται αλλά και στους σταθμούς εργασίας όπου τα δεδομένα θα χρησιμοποιηθούν από τους χρήστες. Αξίζει να σημειωθεί ότι παρότι υπάρχουν μεγάλες προόδους στη DLP στους τερματικούς σταθμούς, η εφαρμογή μόνο στα τερματικά δεν συνίσταται για τους περισσότερους χρήστες.

Παράλληλα προσθέτοντας έναν πράκτορα (endpoint) σε μια εφαρμογή DLP όχι μόνο μας δίνεται η δυνατότητα να ανακαλύψουμε αποθηκευμένο περιεχόμενο, το οποίο βρίσκεται στους τερματικούς σταθμούς, είτε εκ παραδρομής είτε εσκεμμένα, αλλά πιθανότατα να προστατευθούν και τα συστήματα τα οποία δεν είναι πλέον στο δίκτυο καθώς επίσης προστατεύουν δεδομένα τα οποία χρησιμοποιούνται ενεργά. Ενώ είναι εξαιρετικά ισχυρή δυνατότητα, υπάρχουν πολλά μειονεκτήματα στην εφαρμογή της. Οι πράκτορες πρέπει να εκτελεστούν στο πλαίσιο των περιορισμών των πόρων ενός τυπικού φορητού υπολογιστή καθώς διατηρείται η ευαισθητοποίηση του περιεχομένου. Κάτι τέτοιο όμως μπορεί να είναι δύσκολο εάν έχουμε μεγάλες πολιτικές όπως “προστασία όλων των 10 εκατομμυρίων αριθμών από τη βάση δεδομένων μας”. Αντιθέτως θα μπορούσαμε να εφαρμόσουμε κάτι πιο απλό όπως “προστάτεψε οποιαδήποτε αριθμό πιστωτικής κάρτας”, το οποίο θα προκαλέσει λανθασμένους συναγερμούς κάθε φορά που κάποιος υπάλληλος επισκέπτεται ένα ηλεκτρονικό κατάστημα (e-Shop).

3.10.3.1 Βασικές Δυνατότητες

Τα υπάρχοντα προϊόντα διαφέρουν σε μεγάλο βαθμό ως προς την λειτουργικότητά τους, αλλά μπορούμε να διακρίνουμε 3 βασικές δυνατότητες.

α. Παρακολούθηση και επιβολή εντός της στοίβας δικτύου.

Αυτό επιτρέπει την επιβολή των κανόνων του δικτύου χωρίς εφαρμογή κεντρικής διαχείρισης. Οι εφαρμογές θα πρέπει να είναι σε θέση να χρησιμοποιήσουν το ίδιο τους κανόνες που εφαρμόζονται εάν το σύστημα ήταν σε διαχείριση δικτύου είτε εφαρμόζεται και με ξεχωριστούς κανόνες σχεδιασμένοι για συστήματα τα οποία δε βρίσκονται σε διαχείριση δικτύου.

β. Παρακολούθηση και επιβολή εντός του πυρήνα του συστήματος (system kernel).

Χρησιμοποιώντας την συγκεκριμένη δυνατότητα πραγματοποιείται απευθείας σύνδεση μέσα στον πυρήνα του λειτουργικού συστήματος με αποτέλεσμα να μπορούμε να παρακολουθούμε την δραστηριότητα του χρήστη, όπως αντιγραφή και επικόλληση ευαίσθητου περιεχομένου. Αυτό επίσης μπορεί να επιτρέψει στις εφαρμογές DLP να ανιχνεύσουν και επομένως να μπλοκάρουν παραβιάσεις πολιτικής όταν ο χρήστης λαμβάνει ευαίσθητα δεδομένα και προσπαθεί να τα κρύψει από τον εντοπισμό, πιθανότατα με την κρυπτογράφηση ή τροποποιώντας την πηγή του εγγράφου.

γ. Παρακολούθηση και επιβολή εντός του συστήματος αρχείων.

Η συγκεκριμένη δυνατότητα επιτρέπει την παρακολούθηση και την επιβολή ενεργειών βασιζόμενα στο μέρος που βρίσκονται αποθηκευμένα τα δεδομένα. Για παράδειγμα μπορούμε να εφαρμόσουμε τοπική ανεύρεση και να αποτρέψουμε μεταφορά ευαίσθητων δεδομένων σε μη κρυπτογραφημένες φορητές συσκευές (USB Flash Drive).

Οι συγκεκριμένες επιλογές και δυνατότητες έχουν απλοποιηθεί, και τα περισσότερα πρώιμα προϊόντα επικεντρώνονται στις δυνατότητες (α) και (γ) για να λυθεί το πρόβλημα της φορητής αποθήκευσης και να προστατεύσει συσκευές σε δίκτυα χωρίς διαχείριση. Η δεύτερη δυνατότητα, η ενσωμάτωση στον πυρήνα του συστήματος είναι πιο πολύπλοκη και υπάρχουν μια σειρά από προσεγγίσεις για να πραγματοποιηθεί αυτή η λειτουργία.

3.10.3.2. Περιπτώσεις Χρήσεων

Είναι γεγονός ότι η εφαρμογή DLP για τερματικούς σταθμούς (endpoint) εξελίσσεται για να υποστηρίξει μερικές κρίσιμες περιπτώσεις χρήσεως.

Πιο συγκεκριμένα μπορεί να πραγματοποιηθεί η εφαρμογή των κανόνων σε τερματικά που ισχύουν σε ένα δίκτυο και για τερματικά που βρίσκονται εκτός της διαχείρισης του δικτύου ή την τροποποίηση των κανόνων για πιο “εχθρικά” δίκτυα.

Επίσης μπορεί να εφαρμοστεί περιορισμός των ευαίσθητων περιεχομένων σε φορητές συσκευές αποθήκευσης, συμπεριλαμβανομένων αποσπώμενες φορητές συσκευές (USB drives), CD/DVD drives, καθώς και άλλες συσκευές όπως smartphones ή PDA’s.

Ταυτόχρονα περιορίζει την αντιγραφή και επικόλληση ευαίσθητου περιεχομένου.

Επιπλέον πραγματοποιείται ο περιορισμός εφαρμογών που μπορεί να χρησιμοποιούν ευαίσθητα δεδομένα. Για παράδειγμα επιτρέπεται μόνο κρυπτογράφηση, μαζί με την εγκεκριμένη λύση από την διοίκηση, όχι εργαλεία κατεβασμένα από το διαδίκτυο τα οποία δεν επιτρέπει ανάκτηση δεδομένων του οργανισμού.

Τέλος πραγματοποιείται η ελεγχόμενη χρήση του ευαίσθητου περιεχομένου για την υποβολή εκθέσεων συμμόρφωσης σε περίπτωση που διαπιστωθεί παραβίαση της πολιτικής ασφαλείας.

Δεν πρέπει να λησμονήσουμε επίσης της πρόσθετες δυνατότητες στους τερματικούς σταθμούς (Endpoint) που μπορεί να εφαρμοστούν. Μπορούμε σε συνεργασία με την διοίκηση ενός οργανισμού να συνοψίσουμε τις επιθυμητές λειτουργίες μιας εφαρμογής σε ένα τερματικό σταθμό. Όπως προκύπτει μπορούμε να αναφέρουμε τις παρακάτω λειτουργίες:

α. Οι αντιπρόσωποι – πράκτορες (agent) και οι κανόνες ασφαλείας που εφαρμόζονται στους τερματικούς υπολογιστές πρέπει να διαχειρίζονται κεντρικά από τον ίδιο διαχειριστικό DLP εξυπηρετητή (server), ο οποίος ελέγχει, τα δεδομένα σε κίνηση και τα δεδομένα σε αποθήκευση είτε είναι μέσω δικτύου, είτε τα δεδομένα προκύπτουν μετά από έρευνα και ανακάλυψη.

β. Ταυτόχρονα θα πρέπει να ενσωματωθούν οι πολιτικές που δημιουργούνται και η διαχείριση της πολιτικής στις ήδη υπάρχουσες πολιτικές, σε ένα ενιαίο περιβάλλον εργασίας.

γ. Επιπλέον τα περιστατικά θα πρέπει να αναφέρονται και να διαχειρίζονται από τον κεντρικό εξυπηρετητή διαχείρισης.

δ. Οι πράκτορες (agent) που χρησιμοποιούνται στους τερματικούς σταθμούς θα πρέπει να χρησιμοποιούν τις ίδιες τεχνικές ανάλυσης περιεχομένου καθώς και τους ίδιους κανόνες όπως και στους δικτυακούς εξυπηρετητές.

ε. Οι κανόνες και οι πολιτικές θα πρέπει να προσαρμόζονται ανάλογα με το μέρος που βρίσκονται. Δηλαδή εάν βρίσκονται και εφαρμόζονται εντός ή εκτός δικτύου. Όταν οι τερματικοί σταθμοί είναι σε ένα διαχειριζόμενο δίκτυο με πύλες DLP, οι τοπικοί κανόνες θα πρέπει να παραλείπονται για βελτίωση των επιδόσεων.

στ. Επίσης η ανάπτυξη των πρακτόρων (agent) θα πρέπει να ενσωματώνονται μαζί με τα ήδη υπάρχοντα εργαλεία ανάπτυξης λογισμικού των οργανισμών.

ζ. Η αναβάθμιση της πολιτικής ασφαλείας θα πρέπει να προσφέρει επιλογές για ασφαλή διαχείριση μέσω του διαχειριστικού εξυπηρετητή της εφαρμογής DLP, ή από υπάρχοντα εργαλεία αναβάθμισης λογισμικού του οργανισμού.

Από την άλλη πλευρά όπως είναι αναμενόμενο υπάρχουν και ορισμένοι περιορισμοί όταν χρησιμοποιούνται σε τερματικούς σταθμούς. Στην πραγματικότητα, οι επιδόσεις και ο περιορισμός σε αποθήκευση, σε έναν τερματικό σταθμό, θα περιορίζει τους υποστηριζόμενους τύπους ανάλυσης περιεχομένου και τον αριθμό των τύπων πολιτικής οι οποίοι εφαρμόζονται τοπικά. Για ορισμένους οργανισμούς αυτό μπορεί να μην έχει σημασία, εξαρτάται πάντα από το είδος της πολιτικής που εφαρμόζεται αλλά σε πολλές περιπτώσεις τα τερματικά επιβάλλουν συγκεκριμένους περιορισμούς στις πολιτικές στα δεδομένα που βρίσκονται σε χρήση (data in use).

3.11 Καθορισμός Πρόληψης Διαρροής Δεδομένων

Οι περισσότερες λύσεις DLP περιλαμβάνουν μια σειρά από τεχνολογίες που διευκολύνουν 3 βασικούς στόχους:

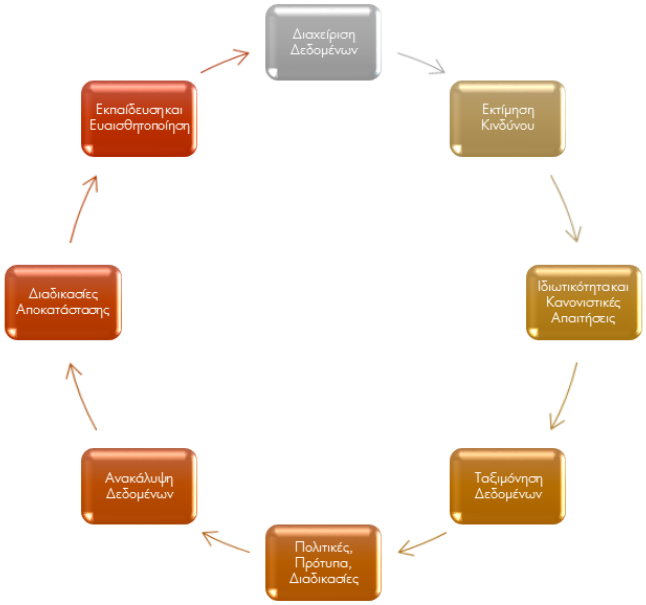
α. Εντοπισμός και κατηγοριοποίηση ευαίσθητων δεδομένων που είναι αποθηκευμένα σε έναν οργανισμό.

β. Παρακολούθηση και έλεγχος της κίνησης των ευαίσθητων πληροφοριών μεταξύ των δικτύων του οργανισμού.

γ. Παρακολούθηση και έλεγχος της κίνησης ευαίσθητων πληροφοριών σε σχέση με τα συστήματα του τελικού χρήστη.

3.11.1 Τι χαρακτηριστικά διαθέτει μια εφαρμογή DLP.

Είναι γεγονός ότι με την ύπαρξη πολλών δημιουργών λογισμικού να υπάρχουν και πολλές επιλογές για μια εφαρμογή DLP. Μια πιθανή δημοσιοποίηση ευαίσθητων δεδομένων θα είχε πέρα από τις νομικές ευθύνες και επιπτώσεις στην φήμη του οργανισμού με όλες τις συνεπακόλουθες συνέπειες. Ένα μοναδικό μοντέλο χαρακτηριστικών είναι το παρακάτω:



Εικόνα 7:Μοντέλο Χαρακτηριστικών DLP

3.11.2 Διαχείριση Δεδομένων

Η Διαχείριση Δεδομένων περιλαμβάνει την συνολική διαχείριση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων μέσα σε έναν οργανισμό. Επομένως υπάρχει η ευθύνη, για την ασφάλεια και την προστασία των δεδομένων, για την παρακολούθηση της ροής των δεδομένων, της διαδρομής δηλαδή όπου αποστέλλονται τα δεδομένα. Είναι μια αρκετά πολύπλοκη διαδικασία ειδικά σε έναν μεγάλο οργανισμό.

Λόγο της σπουδαιότητας απαιτείται ένα όργανο από την διοίκηση του οργανισμού ή ακόμα και μια επιτροπή που θα καθορίζουν τις πολιτικές και τις διαδικασίες. Όπως είναι αναμενόμενο σε μεγάλους οργανισμούς τα στελέχη αυτά θα πρέπει να είναι άτομα τα οποία γνωρίζουν στο μέγιστο βαθμό τη λειτουργία του οργανισμού και τον τρόπο δράσεως του, τους στόχους που βάζει η διοίκησή του και γενικά την κουλτούρα του οργανισμού.

Δεν διαχειρίζεται τα δεδομένα άμεσα αλλά είναι υπεύθυνη για την δημιουργία των πολιτικών και των κανόνων, την μέθοδο και τον τόπο της αποθήκευσης, την πρόσβαση και την διαχείριση των δεδομένων. Ομοίως χρειάζεται να καθορίζει και τις ευθύνες των ιδιοκτητών ή των διαχειριστών των δεδομένων και να περιγράψει την υποχρέωση που έχουν για τα δεδομένα και συγκεκριμένα τον τρόπο επεξεργασίας τους, την αποθήκευσή τους, της αρχειοθέτησής τους και της μετάδοσής τους στο εξωτερικό του οργανισμού και εκτός αυτού.

3.11.3 Εκτίμηση Κινδύνου

Είναι γεγονός ότι για να ξεκινήσει η υλοποίηση μιας εφαρμογής DLP απαιτείται να εντοπίσουμε όλα τα είδη δεδομένων εντός του δικτύου του οργανισμού καθώς και τον εντοπισμό των απειλών και των τρωτών σημείων που σχετίζονται με την διαρροή δεδομένων. Τέτοια δεδομένα που περιέχουν κρίσιμες και σημαντικές πληροφορίες είναι, προσωπικά στοιχεία (οικονομικά επιχειρηματικά, προσωπικού νομικά και κανονιστικά) προσωπικά στοιχεία αναγνώρισης, (αριθμοί κοινωνικής ασφάλισης, στοιχεία πιστωτικής κάρτας, προσωπικά δεδομένα υγείας), πνευματική ιδιοκτησία (διπλώματα ευρεσιτεχνίας, εμπορικά σήματα, σχέδια ανάπτυξης προϊόντων). Όπως γίνεται φανερό όλα τα παραπάνω απαιτείται να προσδιοριστούν ώστε να προστατευθούν. Μόλις εντοπιστεί η πληροφορία, χρειάζεται να πραγματοποιηθεί μια ανάλυση της διαδρομής ώστε να εντοπιστούν όλες οι συσκευές και όλα τα συστήματα από τα οποία τα δεδομένα διέρχονται και αποθηκεύονται. Για παράδειγμα το τμήμα ανθρωπίνου δυναμικού χρησιμοποιεί πληροφορίες για τους εργαζόμενους. Επομένως αυτή η πληροφορία αποθηκεύεται σε έναν κεντρικό εξυπηρετητή (server) και χρησιμοποιεί έναν δεύτερο εξυπηρετητή σε μια ιδιόκτητη βάση δεδομένων. Στη συνέχεια για να αποκτήσει πρόσβαση σε αυτές τις πληροφορίες ο υπάλληλος του τμήματος Ανθρωπίνου Δυναμικού συνδέεται δια μέσου του εσωτερικού δικτύου του οργανισμού με την βοήθεια του φυλλομετρητή (web browser) στον εξυπηρετητή (αρχιτεκτονική τριών επιπέδων). Επομένως στο συγκεκριμένο παράδειγμα οι συσκευές

μεταφοράς και αποθήκευσης είναι ο τερματικός σταθμός εργασίας του εργαζομένου, τα στοιχεία του δικτύου σύνδεσης με τον εξυπηρετητή, ο ίδιος ο εξυπηρετητής και ο εξυπηρετητής που διατηρεί την βάση δεδομένων. Συνεπώς κάθε ένα από αυτά τα συστήματα πρέπει να αξιολογηθούν για να προσδιοριστούν οι απειλές και τα τρωτά σημεία που ενδεχομένως να θέσουν σε κίνδυνο τα δεδομένα. Αυτή η αξιολόγηση απαιτείται να πραγματοποιηθεί για όλους τους τύπους των δεδομένων που χρησιμοποιούνται στο εσωτερικό του οργανισμού. Μια ολοκληρωμένη εφαρμογή DLP πρέπει τελικά να προστατεύει όλα τα πιθανά σημεία κινδύνου του οργανισμού.

3.11.4 Ιδιωτικότητα και Κανονιστικές Απαιτήσεις.

Ένα επόμενο στάδιο σε μια εφαρμογή DLP είναι ο προσδιορισμός των κανονιστικών απαιτήσεων. Έχοντας την πλήρη κατανόηση και αντίληψη των κανονισμών που ισχύουν στον οργανισμό καθώς και ποια είδη ελέγχων ασφαλείας απαιτούνται, χρειάζεται να προσδιορίσουμε στη συνέχεια τις κανονιστικές απαιτήσεις. Είναι γεγονός ότι πολλοί οργανισμοί δεν έχουν πλήρη κατανόηση των αναγκών τους ή οι απαιτήσεις τους δεν συμμορφώνονται με τους κανονισμούς που ισχύουν. Οπότε εμφανίζεται το φαινόμενο οι περισσότεροι οργανισμοί να λειτουργούν σε κατάσταση μη – συμμόρφωσης.

Η αναγνώριση των κανονιστικών απαιτήσεων υποστηρίζει την ασφάλεια στις προτεραιότητες σύστημα – πόροι για μεταποίηση ή και για διαβίβαση ευαίσθητων πληροφοριών. Αυτό επίσης βοηθάει να εστιαστεί το πεδίο της ασφάλειας ελέγχων.

Η αναγνώριση των απαιτήσεων της προστασίας των προσωπικών δεδομένων είναι απαραίτητος για έναν οργανισμό ώστε να διασφαλιστούν ότι οι στόχοι και οι υποχρεώσεις του για προστασία των προσωπικών δεδομένων και του απορρήτου, υποστηρίζονται από τις πρακτικές του, προστατεύοντας με αυτόν τον τρόπο τις εμπιστευτικές πληροφορίες από κακόβουλη χρήση και τον οργανισμό από ευθύνες που θα προκύψουν καθώς και από προβλήματα δημοσίων σχέσεων. Αν και όπως είναι γνωστό το κάθε κράτος έχει νόμους και κανόνες που προστατεύουν τα προσωπικά δεδομένων των πολιτών του, όλοι οι οργανισμοί διατηρούν πολιτικές και διαδικασίες προστασίας προσωπικών δεδομένων για να αυξήσουν το επίπεδο εφησυχασμού των πελατών του. Συνεπώς μια σωστή εφαρμογή DLP θα πρέπει να προβεί σε αξιολόγηση της ιδιωτικότητας ώστε να διασφαλιστεί ότι όλα τα δεδομένα προστατεύονται με βάση τις πολιτικές του οργανισμού. Οπότε εάν οι πολιτικές δεν τηρούνται ή δεν εφαρμόζονται υπάρχει το ενδεχόμενο να διαρρεύσουν ευαίσθητες πληροφορίες.

3.11.5 Ταξινόμηση Δεδομένων

Στη συνέχεια χρειάζεται η ταξινόμηση των δεδομένων. Κατά την διαδικασία της ταξινόμησης, οργανώνονται τα δεδομένα σύμφωνα με την αξία και την ευαισθησία για τον οργανισμό. Η ταξινόμηση των δεδομένων παρέχει σωστή ιεράρχηση των στοιχείων και των πόρων του οργανισμού, με αποτέλεσμα να οδηγηθούμε στο σωστό επίπεδο ελέγχου και το οποίο θα πρέπει να εφαρμόζεται ανάλογα σε κάθε

σύστημα. Συνεπώς τα δεδομένα θα ήταν σωστό να κατηγοριοποιούνται από την άποψη της κρισιμότητας μέσα στο εσωτερικό του οργανισμού δηλαδή δημόσια, εμπιστευτικά, μυστικά και ιδιωτικών φορέων. Οι απαιτήσεις που έχει ένας οργανισμός θα πρέπει να οδηγούν τις διαδικασίες ταξινόμησης και θα πρέπει απευθείας να οδηγούν στις κατηγορίες των δεδομένων. Από την στιγμή που έχουν καθοριστεί τα απαιτούμενα δεδομένα που χρειάζεται ένας οργανισμός, μπορεί να πραγματοποιηθεί η κατάταξη σε κατηγορίες. Μια εφαρμογή DLP τυπικά θα πρέπει να έχει την δυνατότητα να πραγματοποιεί σε ότι αφορά την ταξινόμηση των δεδομένων:

α. Ανάπτυξη προτύπου για την ταξινόμηση των δεδομένων ή ανάπτυξη της πολιτικής για ταξινόμηση δεδομένων.

β. Προσδιορισμό τύπου δεδομένων από τα τμήματα του οργανισμού.

γ. Αναγνώριση του διαχειριστή, του θεματοφύλακα και του χρήστη για κάθε τύπο δεδομένων.

δ. Αναγνώριση και προσδιορισμός των συστημάτων διατήρησης, μετατροπής ή αποθήκευσης για κάθε τύπου δεδομένων.

ε. Καθορισμό των κριτηρίων για το πώς τα δεδομένα θα πρέπει να ταξινομούνται και να επισημαίνονται.

στ. Δημιουργία προγράμματος ευαισθητοποίησης των οργανισμών.

Επίσης η ταξινόμηση των δεδομένων θα προσθέτει επιπλέον στοιχεία ελέγχου για να περιορίσει την πρόσβαση και την κυκλοφορία των ευαίσθητων δεδομένων που διακινούνται εντός του οργανισμού.

3.11.6 Πολιτικές, Πρότυπα και Διαδικασίες

Οι πολιτικές, τα πρότυπα, και οι διαδικασίες είναι βασικά στοιχεία για μια σωστή και αποτελεσματική εφαρμογή της στρατηγικής ενός προγράμματος DLP. Εξασφαλίζουν ότι τα στοιχεία του οργανισμού προστατεύονται σε επίπεδο ανάλογο της αξίας τους. Είναι ζωτικής σημασίας όχι μόνο η δημιουργία πολιτικής, προτύπων και διαδικασιών αλλά και η εξασφάλιση ότι ενημερώνονται σε τακτική βάση. Σε μια εφαρμογή DLP η πολιτική είναι το σημείο εκκίνησης για ένα οργανισμό πριν από την καθιέρωση των προτύπων και των διαδικασιών, που επιτρέπουν στην εφαρμογή DLP να λειτουργεί πιο αποτελεσματικά και με ασφάλεια. Τα πρότυπα είναι υποχρεωτικές δραστηριότητες, δράσεις, κανόνες και κανονισμοί που σχεδιάζονται για να παρέχουν στις πολιτικές DLP την υποστήριξη, τη δομή καθώς και όταν απαιτηθεί συγκεκριμένες κατευθύνσεις ώστε να είναι αποτελεσματικά και ουσιαστικά. Οι διαδικασίες διευκρινίζουν τις λεπτομέρειες για το πώς οι πολιτικές DLP και τα πρότυπα υποστήριξης εφαρμόζονται πραγματικά σε ένα λειτουργικό περιβάλλον.

3.11.7 Ανακάλυψη Δεδομένων

Ανεξάρτητα από όλους τους ελέγχους ασφαλείας που εφαρμόζονται σε έναν οργανισμό, υπάρχουν αρκετές πιθανότητες διαρροής πνευματικής ιδιοκτησίας. Για αυτό το λόγο η εκτίμηση ανακάλυψης δεδομένων απαιτείται να διεξάγεται σε περιοδική βάση. Η εκτίμηση ανακάλυψης δεδομένων εξαρτάται σε μεγάλο βαθμό σε ένα εργαλείο που θα έχει τη δυνατότητα, είτε της παρακολούθησης του δικτύου του οργανισμού, είτε της σάρωσης των δεδομένων ή και των δύο δυνατοτήτων. Αν και αυτός ο στόχος εξαρτάται σε ένα εργαλείο ανακάλυψης, υπάρχουν πολλά εμπορικά ή μη εμπορικά διαθέσιμα προϊόντα. Η ανακάλυψη δεδομένων αποτελεί βασικό στοιχείο της εφαρμογής DLP.

3.11.8 Διαδικασίες Αποκατάστασης

Μια σημαντική πρόκληση για όλες τις εφαρμογές DLP είναι να καθορίσει ποια στοιχεία διαρροής δεδομένων είναι έγκυρα και ποια δεδομένα δημιουργούν λαθεμένους συναγερμούς. Στο σημερινό περιβάλλον των οργανισμών ο όγκος των δεδομένων που διακινούνται μέσω του δικτύου και αποθηκεύονται σε δίσκους είναι τεράστιος. Παρά το γεγονός αυτό, η πρόκληση χρειάζεται να αντιμετωπιστεί και οι διαδικασίες να εφαρμοστούν πριν γίνει η διαρροή. Από την στιγμή όμως που διαπιστωθεί παράβαση πρέπει να μπορεί να εφαρμοστεί η σωστή μεθοδολογία και η αιτία της παράβασης να προσδιοριστεί με ακρίβεια. Εφόσον υπήρξε παράβαση απαιτείται να πραγματοποιηθεί έρευνα ώστε να καθοριστεί εάν έχει παραβιαστεί η πολιτική του οργανισμού. Για την επιτυχία αυτού του σκοπού, χωρίς να πραγματοποιηθεί αναταραχή στο εργασιακό περιβάλλον, η διαδικασίες καθώς και οι επεξεργασίες πρέπει να είναι σε θέση ώστε να αποκαταστήσουν το θέμα αποτελεσματικά. Μια ισχυρή διαδικασία επίλυσης πρέπει να είναι αυτοματοποιημένη, αποδοτική και έγκαιρη ώστε να διαχειριστεί και να επιλύσει το ζήτημα πριν ο οργανισμός υποστεί κάποια βλάβη.

3.11.9 Εκπαίδευση και Ευαισθητοποίηση

Όλα τα παραπάνω που αναφέρθηκαν δεν θα έχουν καμία απολύτως επιτυχία, εάν η εφαρμογή DLP δεν αλληλεπιδρά με τα στελέχη και τους υπαλλήλους του οργανισμού, έτσι ώστε να υπάρχει μια ισχυρή γνώση για το ποιες διαδικασίες είναι ακατάλληλες και θα μπορούσαν να είναι επιβλαβής για τον οργανισμό. Είναι γνωστό ότι όλες οι παραβάσεις που πραγματοποιούνται δεν είναι με κακή πρόθεση. Όπως για παράδειγμα, όταν ένας εργαζόμενος εργάζεται από το σπίτι του και αποστέλλει με απλό ηλεκτρονικό ταχυδρομείο ευαίσθητα δεδομένα με το απλό δημόσιο λογαριασμό του. Παρά το γεγονός του ότι δεν έχει κακή πρόθεση, η δράση του είναι κακή. Επομένως η συνεχής εκπαίδευση θα βοηθήσει να ενισχυθεί η σωστή συμπεριφορά και να παρέχει στους υπαλλήλους οδηγίες για το πώς να χειρίζονται σωστά τα ευαίσθητα δεδομένα. Οπότε όταν οι οργανισμοί εκπαιδεύουν τα στελέχη τους ώστε να τους τονίζουν τους κινδύνους απώλειας δεδομένων, οι παραβιάσεις θα μειωθούν

σημαντικά. Με το πέρασμα του χρόνου και καθώς οι εργαζόμενοι εξοικειωθούν περισσότερο με την πολιτική του οργανισμού καθώς και τις πρακτικές του η συνολική ευαισθητοποίηση σε θέματα ασφαλείας θα αυξηθεί σε όλο τον οργανισμό.

3.12 Πώς πραγματοποιείται η επιλογή μιας στρατηγικής DLP.

3.12.1 Καθορισμός ανάγκες και προετοιμασία του οργανισμού

Πριν ξεκινήσουμε να ασχοληθούμε με ποια εφαρμογή DLP θα επιλέξουμε, είναι αναγκαίο να κατανοήσουμε για πιο λόγο χρειαζόμαστε μια τέτοια εφαρμογή, πώς σκοπεύουμε να την χρησιμοποιήσουμε, την διαδικασία λειτουργία της στον οργανισμό σε ότι αφορά την δημιουργία πολιτικών και την διαχείριση συμβάντων.

α. Προσδιορίζεται το προσωπικό από τα τμήματα του οργανισμού που αναγκαιούν να συμμετέχουν και δημιουργούμε μια επιτροπή επιλογής. Συνήθως υπάρχει η τάση να συμπεριλαμβάνονται δύο ειδών στελεχών του οργανισμού. Τα στελέχη τα οποία δημιουργούν και χειρίζονται ευαίσθητα δεδομένα, που χρειάζεται να προστατευθούν, και τα στελέχη τα οποία θα επιφορτιστούν με την προστασία των δεδομένων αυτών καθώς και με τον έλεγχό τους. Συνεπώς γίνεται φανερό ότι τα στελέχη που είναι κάτοχοι των δεδομένων είναι οι υπάλληλοι ή τα στελέχη του οργανισμού. Ενώ τα στελέχη που επιφορτίζονται με την προστασία των δεδομένων συνήθως συμπεριλαμβάνουν τα τμήματα προσωπικού (ανθρωπίνου δυναμικού), πληροφορικής καθώς και την ασφάλεια πληροφορικής, το νομικό τμήμα και το τμήμα διαχείρισης κινδύνων. Μόλις καθοριστούν τα μέρη τα οποία εμπλέκονται, πραγματοποιείται η πρώτη επαφή για να προσδιοριστούν τα επόμενα βήματα.

β. Καθορίζεται τι χρειάζεται να προστατευθεί. Το πρώτο βήμα είναι να καταγραφούν όσο γίνεται πιο συγκεκριμένα το είδος και τα δεδομένα τα οποία θέλουμε να προστατεύσουμε με την εφαρμογή DLP. Συνήθως τα είδη των δεδομένων χωρίζονται σε τρεις κατηγορίες. Τα προσωπικά στοιχεία (τα οποία συμπεριλαμβάνουν ιατρικά στοιχεία, οικονομικά καθώς και άλλα προσωπικά στοιχεία), οικονομικά στοιχεία του οργανισμού, καθώς και την πνευματική ιδιοκτησία. Τα δύο πρώτα είδη όπως έχουμε ήδη αναφέρει αποτελούνται από δομημένα δεδομένα και οδηγούμαστε εύκολα στην επιλογή της εφαρμογής που θα επιλέξουμε ώστε να έχουμε αποτελέσματα. Τα πνευματικά δικαιώματα όμως δεν είναι τόσο δομημένα και απαιτείται διαφορετική ανάλυση του περιεχομένου τους. Ακόμα και αν θέλουμε να προστατεύσουμε όλα τα είδη του περιεχομένου, χρησιμοποιούμε αυτή την διαδικασία για να καθορίσουμε και να δώσουμε προτεραιότητα, πρώτα στα χαρτιά.

γ. Καθορίζεται πώς θέλουμε να τα προστατεύσουμε και επιλέγουμε τα προσδοκόμενα αποτελέσματα. Σε αυτό το βήμα είναι το σημείο στο οποίο απαιτείται να απαντήσουμε σε δύο βασικές ερωτήσεις. Πρώτα από όλα σε ποια φάση και κα-

νάλια θέλουμε να προστατεύσουμε τα δεδομένα. Στο σημείο αυτό χρειάζεται να αποφασιστεί εάν επιθυμούμε απλή παρακολούθηση των ηλεκτρονικών ταχυδρομείων ή θέλουμε ολοκληρωμένη προστασία των δεδομένων σε κίνηση, των δεδομένων σε κατάσταση ηρεμίας και των δεδομένων σε χρήση. Θα πρέπει να είμαστε πολύ συγκεκριμένοι σε ότι αφορά στην καταγραφή των δυνατοτήτων του δικτύου των αποθηκευτικών μέσων που βρίσκονται τα δεδομένα καθώς και των τερματικών σταθμών εργασίας. Το δεύτερο που θα χρειαστεί να αποφασιστεί είναι τι είδους επιβολή, τι αντιμετώπιση δηλαδή θα έχει και θα εκτελείται από την εφαρμογή. Παρακολούθηση και ειδοποίηση μόνο; Φιλτράρισμα ηλεκτρονικού ταχυδρομείου; Αυτόματη κρυπτογράφηση; Μπορούμε να γίνουμε πιο συγκεκριμένη για την αντιμετώπιση και αργότερα, απλά καλό θα είναι να έχουμε μια ιδέα στο σημείο αυτό του τι θα μπορούσαμε να αναμένουμε. Επιπροσθέτως ας μην λησμονούμε ότι οι ανάγκες αλλάζουν με τη πάροδο του χρόνο κατά συνέπεια θα ήταν καλό οι απαιτήσεις να διαχωριστούν και επανεκτιμηθούν σε σύντομο χρονικό διάστημα. Για παράδειγμα μετά από 6 μήνες από την εγκατάσταση, μια ενδιάμεση 12 έως 18 μήνες από την εγκατάσταση και μίας μακράς διάρκειας μέχρι 3 χρόνια από την ανάπτυξη.

δ. Συνοπτική περιγραφή των διαδικασιών και των εργασιών. Ένα από τα μεγαλύτερα εμπόδια που μπορεί να μας εμφανιστεί για την ανάπτυξη και την λειτουργία μιας εφαρμογής DLP είναι η σωστή προετοιμασία του οργανισμού. Στο σημείο αυτό θα πρέπει να ορίσουμε τις διαδικασίες, για την δημιουργία πολιτικών ασφαλείας καθώς επίσης και τις διαδικασίες αντιμετώπισης περιστατικών κατά τις οποίες εμπλέκονται εσωτερικοί και εξωτερικοί εισβολείς. Ποια τμήματα του οργανισμού έχουν το δικαίωμα να ζητήσουν την προστασία των δεδομένων τους; Ποιος είναι υπεύθυνος για την κατασκευή της πολιτικής ασφαλείας; Όταν μια πολιτική ασφαλείας παραβιαστεί, ποια είναι η διαδικασία για την αποκατάστασή της; Πότε ειδοποιείται το τμήμα διαχείρισης προσωπικού; Πότε το τμήμα νομικών συμβούλων; Ποιος χειρίζεται κάθε μέρα την πολιτική των παραβιάσεων; Αυτός ο ρόλος είναι ρόλος τεχνικός ασφαλείας ή όχι όπως είναι το γραφείο παραπόνων; Οι απαντήσεις σε αυτά τα ερωτήματα θα μας οδηγήσουν κατευθείαν σε διαφορετικές εφαρμογές DLP οι οποίες θα ικανοποιούν τις ανάγκες που προκύπτουν από τις διαδικασίες.

Με την ολοκλήρωση της φάσης αυτής θα πρέπει να έχουν καθοριστεί ποια μέρη είναι τα ενδιαφερόμενα και εμπλέκονται, ώστε στη συνέχεια να δημιουργηθεί μια επιτροπή αξιολόγησης και επιλογής, προσδιορίζουμε και δίνουμε προτεραιότητα στα δεδομένα που θέλουμε να προστατεύσουμε και σε ποια ακριβώς θέση θέλουμε να τα προστατεύσουμε και απαιτήσεις διαδικασιών για την κατασκευή πολιτικών και περιστατικών αποκατάστασης.

3.12.2 Επίσημες Απαιτήσεις

Αυτή η φάση μπορεί να πραγματοποιηθεί από μια μικρότερη ομάδα που θα έχει οριστεί και θα λειτουργεί υπό την εποπτεία από την επιτροπή επιλογής. Αυτή η ομάδα μετατρέπει σε αυτή τη φάση τις γενικές κατευθύνσεις που ορίστηκαν στην

προηγούμενη φάση, σε συγκεκριμένα ειδικά τεχνικά χαρακτηριστικά καθώς και οποιασδήποτε απαιτήσεις προκύπτουν και θεωρηθούν ότι πρέπει να συμπεριληφθούν. Στο σημείο αυτό θα πρέπει να καθοριστούν τα κριτήρια καταλόγου, της πύλης (gateway) που θα χρησιμοποιηθεί, ο αποθηκευτικός χώρος, οι ιεραρχικές αναπτύξεις, τα τελικά σημεία των τερματικών σταθμών κοκ. Στη συνέχεια μπορούν πάντα να πραγματοποιηθούν βελτιώσεις σε αυτές τις απαιτήσεις που έχουν επιλεγεί αφού θα έχουμε μια πρώτη εικόνα για το πώς λειτουργούν οι εφαρμογές.

Μετά το πέρας των φάσεων αυτών πρέπει να συνταχθεί μια επίσημη αναφορά τύπου RFI (αίτημα για πληροφορίες) η οποία θα δοθεί στους κατασκευαστές καθώς και μια πρόχειρη αναφορά τύπου RFP η οποία θα ξεκαθαριστεί στη φάση της αξιολόγησης και στη συνέχεια θα εκδοθεί.

3.12.3 Αξιολόγηση Εφαρμογών

Στο σημείο αυτό γίνεται κατανοητό ότι όπως και με πολλά προϊόντα, είναι δύσκολο μερικές φορές, μέσα από τη προώθησή του και το marketing αν πραγματικά το χρειαζόμαστε και αν πραγματικά καλύπτει τις ανάγκες μας. Τα παρακάτω προτεινόμενα βήματα βοηθούν να ελαχιστοποιηθεί ο κίνδυνος μιας λάθος απόφασης και μας παρέχει την σιγουριά ότι πραγματοποιήσαμε την σωστή επιλογή.

α. Έκδοση της Αναφοράς RFI: Οι μεγαλύτεροι οργανισμοί θα πρέπει να έχουν εκδώσει μια αναφορά RFI και η οποία θα αποσταλεί δια μέσου των καθιερωμένων καναλιών επικοινωνίας και θα μας φέρει σε επαφή απευθείας με ορισμένους κατασκευαστές της εφαρμογής DLP.

β. Εκτέλεση μιας έντυπης αξιολόγησης: Πριν από την εισαγωγή οποιασδήποτε εφαρμογής ελέγχουμε ποιες ταιριάζουν με τα RFI και τα RFP. Στόχος είναι να δημιουργήσουμε μια λίστα με 3 αντικείμενα τα οποία ταιριάζουν στις απαιτήσεις μας. Θα πρέπει να αναζητάμε και πηγές έρευνας εκτός για να πραγματοποιηθεί η σύγκριση.

γ. Συνάντηση με 3 κατασκευαστές καθώς και η πραγματοποίηση μιας παρουσίασης και μιας αξιολόγησης κινδύνων: Όλοι οι κατασκευαστές μιας εφαρμογής DLP θα είναι πρόθυμοι να έρθουν και να εγκαταστήσουν σε δοκιμαστική έκδοση για λίγες μέρες την εφαρμογή τους στο δίκτυο σε κατάσταση παρακολούθησης με τους βασικούς κανόνες. Καλό θα ήταν να δοκιμαστούν οι εφαρμογές όσο αυτό είναι εφικτό κατά το ίδιο χρονικό διάστημα, με την ίδια κίνηση δικτύου. Αυτή θα είναι και η ευκαιρία για να βρεθούμε και με τους κατασκευαστές και να πάρουμε απευθείας συγκεκριμένες απαντήσεις, σε τυχόν απορίες που θα μας έχουν δημιουργηθεί. Ορισμένοι κατασκευαστές επιθυμούν και προσπαθούν να έχουν επίσημη αναφορά RFP πριν από την διάθεση των πόρων τους για την ζωντανή παρουσίαση ειδικά για μικρές επιχειρήσεις.

δ. Οριστικοποίηση της αναφοράς RFP και επίδοσή της στους υποψήφιους κατασκευαστές: Στο σημείο αυτό χρειάζεται να έχουμε καταλάβει εντελώς τις συγκεκριμένες απαιτήσεις μας και να εκδώσουμε το επίσημο RFP.

ε. Αξιολόγηση των απαντήσεων των RFP καθώς και έναρξη των δοκιμών των προϊόντων: Ανακεφαλαίωση και αξιολόγηση των αποτελεσμάτων RFP και απόρριψη όποιων δεν πληρούν τις ελάχιστες απαιτήσεις. Στη συνέχεια είμαστε σε θέση να καλέσουμε τους κατασκευαστές για δοκιμές στον οργανισμό. Για να πραγματοποιηθεί μια σωστή αξιολόγηση της εφαρμογής, την τοποθετούμε στο δίκτυό μας σε κατάσταση παθητικής παρακολούθησης και ενεργοποιούμε κάποιους απλούς κανόνες οι οποίοι θα ενεργοποιηθούν και στην συνέχεια. Αυτό θα μας βοηθήσει να αξιολογήσουμε τις εφαρμογές ταυτόχρονα, ενεργοποιώντας τους ίδιους κανόνες στις ίδιες συνθήκες του δικτύου. Τέλος θα πρέπει να δοκιμάσουμε οτιδήποτε ειδικό χαρακτηριστικό βρίσκεται στην κορυφή της λίστας των απαιτήσεων μας.

στ. Επιλογή, διαπραγμάτευση και αγορά: Από την στιγμή που θα έχουμε τελειώσει όλες τις δοκιμές που έχουμε αποφασίσει να πραγματοποιήσουμε, υποβάλουμε τα αποτελέσματα στην επιτροπή επιλογής, ώστε να ξεκινήσει η διαδικασία των διαπραγματεύσεων και της αγοράς.

3.12.4 Εσωτερικοί Έλεγχοι

Οι εσωτερικοί έλεγχοι στον οργανισμό είναι το τελευταίο βήμα για να ανακαλυφθούν τυχόν προβλήματα και δυσλειτουργίες στην διαδικασία της επιλογής μας. Συνεπώς και αφού έχουμε βεβαιωθεί ότι έχουμε δοκιμάσει την εφαρμογή όσο τον δυνατόν πληρέστερα, μπορούμε να δοκιμάζουμε αν είμαστε σε θέση τα εξής:

α. Δημιουργία πολιτικής και ανάλυσης περιεχομένου. Προσπαθούμε να παραβιάσουμε τις πολιτικές που έχουμε θέσει, προσπαθούμε να τις αποφύγουμε, να πιέσουμε την εφαρμογή ώστε να μάθουμε τα όριά της.

β. Ολοκλήρωση του ηλεκτρονικού ταχυδρομείου.

γ. Διαδικασία αντιμετώπισης περιστατικών. Επανεξετάζουμε την διεπαφή της εφαρμογής μαζί με τους χειριστές που θα είναι υπεύθυνοι για την λειτουργία της εφαρμογής.

δ. Ολοκλήρωση του καταλόγου.

ε. Ενσωμάτωση του αποθηκευτικού χώρου στις κύριες πλατφόρμες ώστε να δοκιμαστούν οι επιδόσεις και η συμβατότητα των δεδομένων κατά την προστασία τους όταν βρίσκονται σε στάση και αποθήκευση.

στ. Λειτουργία των τερματικών σταθμών εργασίας όπως ακριβώς επιθυμούμε και θέλουμε.

ζ. Απόδοση του δικτύου. Απαιτείται να ελέγξουμε όχι μόνο το εύρος ζώνης αλλά και κάθε απαίτηση για την ενσωμάτωση της εφαρμογής στο δίκτυο μας και τον συντονισμό της. Μήπως για παράδειγμα χρειαστεί ένα προ-φιλτράρισμα της κίνησης του δικτύου. Επίσης μήπως χρειαστεί συνδυασμός πρωτοκόλλων και συγκεκριμένης πόρτας.

η. Ενσωμάτωση πύλης δικτύου.

θ. Τις ενέργειες που θα απαιτηθούν για να επιβληθούν οι πολιτικές της εφαρμογής.

3.13 Εφαρμογή μιας λύσης DLP

Εκείνο που έχει ιδιαίτερη σημασία για να πραγματοποιήσουμε με επιτυχία την ανάπτυξη μιας ολοκληρωμένης εφαρμογής DLP είναι η υλοποίηση ορισμένων σημαντικών προπαρασκευαστικών διαδικασιών, όπως για παράδειγμα η ανάπτυξη της πολιτικής ασφαλείας, η ανάλυση των καθημερινών διαδικασιών του οργανισμού καθώς και λεπτομερείς απογραφή και ανάλυση του τύπου των δεδομένων που χρησιμοποιούνται από τον οργανισμό. Αυτές οι ενέργειες απαιτούν την συμμετοχή μιας ευρείας βάσης ενδιαφερομένων τόσο από το τμήμα των προγραμματιστών μιας εταιρίας ανάπτυξης λογισμικού ή του τμήματος προγραμματιστών του οργανισμού, καθώς επίσης και των τμημάτων του οργανισμού που υποστηρίζει.

3.13.1 Οργάνωση των Δεδομένων, των Τοποθεσιών και των Διαδρομών.

Είναι γεγονός ότι έχει παρατηρηθεί το φαινόμενο, οι οργανισμοί να μην γνωρίζουν όλα τα είδη καθώς και τις θέσεις των πληροφοριών που κατέχουν. Είναι πολύ σημαντικό, πριν από την επιλογή μιας εφαρμογής DLP, να αναγνωρίζουν και να ταξινομούν τους ευαίσθητους τύπους δεδομένων, καθώς και την ροή που θα έχουν τα δεδομένα αυτά από σύστημα σε σύστημα και από χρήστη σε χρήστη. Η διαδικασία αυτή θα πρέπει να δώσει μια ταξινόμηση των δεδομένων ή ένα σύστημα ταξινόμησης το οποίο θα πρέπει να μπορεί να ανιχνευθεί από τις διάφορες ενότητες DLP όπως πραγματοποιείται σάρωση και λαμβάνοντας δράση ενεργειών για πληροφορίες που εκπίπτουν στις διάφορες ταξινομήσεις βάση των πολιτικών ασφαλείας και οι οποίες βρίσκονται εκτός ταξινόμησης. Όταν θα πραγματοποιηθεί η ανάλυση των κρίσιμων επιχειρησιακών διαδικασιών θα πρέπει να δώσει όλες τις απαιτούμενες πληροφορίες. Η συγκεκριμένη ταξινόμηση μπορεί να περιλαμβάνει κατηγορίες όπως είναι για παράδειγμα, ιδιωτικοί πελάτες, δεδομένα υπαλλήλων, οικονομικά στοιχεία καθώς και πνευματική ιδιοκτησία. Από την στιγμή που έχουν ταυτοποιηθεί τα δεδομένα και ταξινομηθεί κατάλληλα η περαιτέρω ανάλυση της διαδικασίας θα πρέπει να διευκολύνει την πρωταρχική θέση αποθήκευσης των δεδομένων και το κλειδί των διαδρομών των δεδομένων. Συχνά πολλαπλά αντίγραφα των δεδομένων καθώς και παραλλαγές τους, βρίσκονται διάσπαρτα σε εξυπηρετητές σε ολόκληρο τον οργανισμό, σε μεμονωμένους σταθμούς εργασίας καθώς και άλλα αποθηκευτικά μέσα. Τα αντίγραφα γίνονται πολλές φορές για να διευκολύνουν τον έλεγχο μιας εφαρμογής χωρίς πρώτα να έχουν καθοριστεί τα δεδομένα από το ευαίσθητο περιεχόμενο που περιέχουν. Έχοντας μια σωστή ιδέα, από την ταξινόμηση των δεδομένων καθώς και την θέση όπου αποθηκεύονται για πρώτη φορά οι πληροφορίες, αποδεικνύεται χρήσιμο τόσο για την επιλογή όσο και για την τοποθέτηση της εφαρμογής DLP. Από την στιγμή που θα εγκατασταθεί η εφαρμογή DLP, είναι σε θέση να βοηθήσει στον εντοπισμό των δεδομένων και των διαδρομών που ακολούθησαν.

Θα πρέπει επίσης να προσθέσουμε ότι απαιτείται να κατανοήσουμε τον κύκλο ζωής των δεδομένων ενός οργανισμού. Η κατανόηση του κύκλου ζωής από το σημείο προέλευσης, μέσα από την επεξεργασία των δεδομένων, την συντήρησή τους,

την αποθήκευσή τους, και την τελική διάθεσή τους θα μας χρησιμεύσει στην περαιτέρω αποκάλυψη αποθηκευμένων δεδομένων καθώς και των διαδρομών μετάδοσή τους.

Επιπλέον πρόσθετες πληροφορίες θα πρέπει να συλλέγονται με την καταγραφή όλων των σημείων εξόδου των δεδομένων, από τη στιγμή που δεν είναι όλες οι διαδικασίες του οργανισμού τεκμηριωμένες και δεν είναι όλες οι κινήσεις δεδομένων αποτέλεσμα μιας καθιερωμένης και τυποποιημένης διαδικασίας. Η ανάλυση των κανόνων των firewall και των router μπορεί να βοηθήσουν σε αυτή την προσπάθεια.

3.13.2 Καθιέρωση Υψηλού επιπέδου Πολιτικών και Διαδικασιών

Όταν οι πληροφορίες έχουν εντοπιστεί και κατηγοριοποιηθεί, οι πολιτικές θα πρέπει να δημιουργηθούν ή να τροποποιηθούν ώστε να οριστούν συγκεκριμένες ταξινομήσεις και ο κατάλληλος χειρισμός σε κάθε κατηγορία. Οι πολιτικές ταξινόμησης δεδομένων πρέπει να παραμένουν όσο το δυνατόν απλούστερες.

Μόλις τοποθετηθεί η πολιτική, θα πρέπει να καθιερωθεί ένα υψηλού επιπέδου πλάνο ροής εργασίας. Αυτό το πλάνο θα πρέπει να περιλαμβάνει τις κατηγορίες των δεδομένων οι οποίες έχουν στοχοποιηθεί, τις ενέργειες που θα γίνουν (και από ποιον) στην αντιμετώπιση της παραβίασης, οι διεργασίες κλιμάκωσης καθώς και κάθε άλλη διαδικασία απαιτείται για αιτήσεις εξαίρεσης. Η διαδικασία θα πρέπει επίσης να είναι καθιερωμένη για ώρες πέρα του ωραρίου καθώς και την περίοδο των διακοπών, κατά τις οποίες τα άτομα-κλειδιά μπορεί να μην είναι διαθέσιμα. Κατά συνέπεια είναι αρκετά σημαντικό η διαδικασία μετά από ώρες να έχει καθαρό και καλά τεκμηριωμένο τρόπο ενεργείας, εμπλέκοντας άτομα τα οποία μπορούν να πραγματοποιούν κατάλληλες, βάσιμες αποφάσεις και επιλογές με αποτέλεσμα η κάθε απόφαση που λαμβάνεται για την παροχή μιας εξαίρεσης μετά το ωράριο να είναι βάσιμη. Στη συνέχεια η εξαίρεση αυτή επανεξετάζεται από τα ενδιαφερόμενα μέλη το συντομότερο δυνατόν αυτά είναι διαθέσιμα. Γίνεται φανερό ότι θα πρέπει να υπάρχει μια επίσημη διαδικασία διαχείρισης των εξαιρέσεων καθιερώνοντας ότι τα δικαιολογητικά έγγραφα που συνοδεύουν μια παρόμοια αίτηση, παρέχουν τις συναφή πληροφορίες που απαιτούνται για την εν λόγω εξαίρεση. Είναι επίσης σημαντικό να εξασφαλίσουμε ότι υπάρχει η κατάλληλη διαδικασία διαχείρισης περιστατικών και είναι λειτουργική για κάθε μία από τις κατηγορίες των κανόνων πριν από την κοινοποίηση – δημοσιοποίηση.

3.13.3 Εκτέλεση

Συνεχίζοντας και φτάνοντας στη φάση της υλοποίησης, οι οργανισμοί θα πρέπει πρώτα να εξετάσουν σοβαρά να εκτελέσουν την εφαρμογή DLP σε κατάσταση παρακολούθησης. Προτείνεται η συγκεκριμένη προσέγγιση διότι αυτό θα επιτρέψει στο σύστημα να συντονιστεί και να αναγνωρίσει τυχόν επιπτώσεις στις καθημερινές διαδικασίες του οργανισμού, καθώς και στην ήδη υπάρχουσα κουλτούρα όπως αυτή έχει οργανωθεί. Δημιουργείται ένας συναγερμός (alert) ώστε να καταδεί-

ξουν αλλαγές στη συμπεριφορά. Είναι γενικά καλύτερη προσέγγιση από το να πραγματοποιηθεί πλήρες μπλοκάρισμα της ροή των δεδομένων και κατά συνέπεια να εκτροχιαστούν όλες οι διαδικασίες του οργανισμού. Από την στιγμή που η ηγεσία ενός οργανισμού έχει συγκεκριμένες ανησυχίες, που αφορά την ποσότητα και το είδος των ευαίσθητων δεδομένων που εξέρχονται του δικτύου του, μόλις ενεργοποιηθεί το σύστημα και ξεκινήσει ή η διαδικασία του πραγματικού blocking ξεκινήσει πάρα πολύ νωρίς, μπορεί να δημιουργήσει ακόμα μεγαλύτερα προβλήματα με τη διακοπή ή την παρεμπόδιση κρίσιμων εργασιών του οργανισμού. Συνεπώς εάν πραγματοποιηθεί σωστός και λεπτομερείς σχεδιασμός οι διεργασίες αυτές θα αναγνωριστούν και θα εντοπιστούν κατά την διάρκεια του σταδίου της προετοιμασίας. Παρόλα αυτά είναι συχνό το φαινόμενο ορισμένα πράγματα που δεν έχουν προβλεφθεί να εμφανίζονται έρχονται γρήγορα όταν η εφαρμογή DLP ενεργοποιηθεί.

3.13.4 Αποκατάσταση των Παραβιάσεων

Οι εφαρμογές DLP γενικά παρέχουν μια μεγάλη διαχείριση από χρήσιμες πληροφορίες σε ότι αφορά την τοποθεσία και την διαδρομή μεταφοράς των ευαίσθητων δεδομένων. Παρόλα αυτά μερικές φορές μπορεί να έχουμε την δημιουργία και την επικράτηση του πανικού. Στην περίπτωση που κάποιος οργανισμός πανικοβληθεί από τον όγκο και την έκταση του αποτυπώματος των ευαίσθητων δεδομένων που χάθηκαν, μπορεί να εκτελέσει βιαστικές κινήσεις για να προχωρήσει μπροστά προσπαθώντας να αντιμετωπίσει όλα τα θέματα που προέκυψαν μια και έξω, κάτι το οποίο θα ήταν καταστροφικό. Είναι σημαντικό μια επιχείρηση να είναι προετοιμασμένη να χρησιμοποιήσει μια προσέγγιση βασισμένη στο κίνδυνο και στις καταστροφές που μπορεί να αντιμετωπίσει, έτσι ώστε να προτεραιοποιήσει και να αντιμετωπίσει τα ευρήματα κατά τον πλέον πρόσφορο τρόπο. Γίνεται φανερό ότι όλα τα στελέχη που βρίσκονται σε θέσεις κλειδιά θα πρέπει να εμπλέκονται σε αυτή την διαδικασία Η ανάλυση και οι επακόλουθες αποφάσεις που ελήφθησαν, όσο αφορά την διαδικασία, θα πρέπει να είναι καλά τεκμηριωμένη και να διατηρείται σε αναμονή σε μελλοντικούς ελέγχους ή έρευνες.

3.13.5 Συνέχιση προγράμματος DLP.

Η εφαρμογή DLP θα πρέπει να παρακολουθείται συχνά, συνεπώς ότι προκύπτει που αφορά τους περιοδικούς κινδύνους, τη συμμόρφωση καθώς και τις ιδιωτικές αναφορές θα πρέπει να παρέχονται στους κατάλληλους ενδιαφερόμενους (πχ διαχείριση κινδύνου, διαχείριση συμμόρφωσης, διαχείριση προσωπικού). Οι κανόνες DLP θα πρέπει να συνεχίσουν να αναθεωρούνται και να βελτιστοποιούνται. Είναι λογικό ότι μια εφαρμογή DLP δεν είναι σε θέση να ενημερώσει τους διαχειριστές ότι ένας κανόνας είναι υπερβολικά ευρύς για τα δεδομένα και μπορεί να έχει σημαντική επίδραση στην απόδοση σε ότι αφορά ολόκληρη την υποδομή του DLP. Ο οργανισμός θα πρέπει να διασφαλίσει ότι όλα τα εμπλεκόμενα-ενδιαφερόμενα στελέχη είναι επιμελείς και ευαισθητοποιημένοι ώστε να αναφέρουν κάθε ένα νέο δεδομένο

ή τύπο δεδομένου που μπορεί να μην αντιπροσωπεύεται στο υπάρχον πακέτο κανόνων DLP. Τέλος είναι εξίσου σημαντικό να συνεχιστούν τα προγράμματα εκπαίδευσης και ευαισθητοποίησης, τα οποία θα πραγματοποιούνται μέσω της δυνατότητας αναφορών και προειδοποιήσεων της εφαρμογής DLP.

3.14 Κεντρική Διαχείριση, Πολιτική Διαχείρισης και Ροή Εργασίας.

Όπως έχουμε ήδη αναφέρει όλες οι εφαρμογές DLP που υπάρχουν και κυκλοφορούν αυτή τη στιγμή περιλαμβάνουν περιβάλλον κεντρικής διαχείρισης για την δημιουργία, εφαρμογή και διαχείριση των πολιτικών, την ροή εργασιών που θα ακολουθηθεί καθώς και την υποβολή εκθέσεων με τα εκάστοτε αποτελέσματα. Τα συγκεκριμένα χαρακτηριστικά είναι πολύ σημαντικά στην διαδικασία επιλογής της κατάλληλης εφαρμογής. Αντί να αναφέρουμε όλες τις υπάρχουσες εφαρμογές και να καλύψουμε όλες τις περιπτώσεις που αυτές περιλαμβάνουν θα αρκεστούμε στο να αναφέρουμε τις αρχικές ρυθμίσεις και την εμφάνιση των κύριων και κοινών χαρακτηριστικών.

α. Περιβάλλον Χρήστη

Παρατηρώντας την εφαρμογή DLP διαπιστώνουμε ότι σε αντίθεση με άλλα εργαλεία για την ασφάλεια, μπορεί να χρησιμοποιηθεί συχνά και από μη τεχνικό προσωπικό, το οποίο μπορεί να είναι από την διοίκηση μέχρι και χαμηλόβαθμο προσωπικό, από το νομικό τμήμα του οργανισμού καθώς και από τους επικεφαλής των εκάστοτε τμημάτων του οργανισμού. Κατά συνέπεια γίνεται κατανοητό ότι η διεπαφή εφαρμογής και χρήστη θα πρέπει να λαμβάνει υπόψιν της όλο αυτό το μίγμα του προσωπικού τεχνικών ή μη. Επομένως θα πρέπει να είναι εύκολα προσαρμόσιμη για να καλύψει τις ανάγκες της κάθε συγκεκριμένης ομάδας χειριστών. Λόγω της πολυπλοκότητας και του όγκου των πληροφοριών η εφαρμογή DLP θα πρέπει να είναι σε θέση να διαχειριστεί με την διεπαφή του χρήστη ώστε να μπορεί να δημιουργεί ή να διαγράφει ένα αντικείμενο DLP. Για παράδειγμα με την επισήμανση από τον χρήστη της επικεφαλίδας σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο παραβιάζει την πολιτική ασφαλείας μπορεί να μας γλυτώσει από αρκετό χρόνο που θα δαπανηθεί σε άσκοπες αναλύσεις. Μια διεπαφή DLP θα πρέπει να έχει τα παρακάτω στοιχεία:

(1) Οθόνη Διαχείρισης: Αναφερόμαστε στο πεδίο το οποίο περιέχει όλα τα στοιχεία που μπορεί να επιλέξει ο χρήστης και τις προεπιλογές που διαθέτει για τους χειριστές τεχνικούς ή μη. Μεμονωμένα στοιχεία ή ειδικά στοιχεία μπορεί να είναι διαθέσιμα μόνο σε εξουσιοδοτημένους χρήστες ή σε εξουσιοδοτημένες ομάδες του οργανισμού. Συνήθως αποθηκεύονται στους καταλόγους του οργανισμού. Η οθόνη διαχείρισης αποτελεί το κύριο περιβάλλον εργασίας και θα πρέπει να επικεντρωθεί στις χρήσιμες και ενδιαφέρουσες πληροφορίες που ενδιαφέρουν τον συγκεκριμένο χρήστη και να μην είναι απλά μια γενική εικόνα του συστήματος. Τα εμφανή στοιχεία περιλαμβάνουν αριθμούς και κατανομές παραβιάσεων με βάση την

σοβαρότητα καθώς και άλλες υψηλού επιπέδου πληροφορίες, για να πραγματοποιηθεί μια σύνοψη του συνολικού κινδύνου για τον οργανισμό.

(2) Σειρά Διαχείρισης Περιστατικών: Η σειρά διαχείρισης περιστατικών είναι από τις πιο σημαντικές λειτουργίες της διεπαφής. Η συγκεκριμένη επιλογή είναι αυτή που χρησιμοποιούν οι χρήστες του περιστατικού για να παρακολουθούν και να διαχειρίζονται τα περιστατικά παραβίασης. Η σειρά πρέπει να είναι συνοπτική, προσαρμόσιμη και εύκολο να διαβαστεί με μια γρήγορη ματιά.

(3) Εμφάνιση Μεμονωμένου Περιστατικού: Στην περίπτωση αυτή ένας χειριστής ο οποίος αναζητά βαθύτερα μέσα σε ένα μεμονωμένο περιστατικό, θα πρέπει να έχει στην οθόνη του ευκρινώς και συγκεκριμένα συνοπτικά την αιτία της παραβίασης, ο χρήστης που εμπλέκεται, την κρισιμότητα, τη βαρύτητα (η κρισιμότητα βασίζεται στο σε ποια από όλες τις εφαρμοζόμενες πολιτικές έχει γίνει η παραβίαση και πόσα από τα δεδομένα εμπλέκονται), πρόσφατα περιστατικά και ότι άλλες πληροφορίες απαιτούνται για να παρθεί μια σωστή απόφαση αντιμετώπισης του περιστατικού.

(4) Σύστημα Διαχείρισης : Περιλαμβάνει την τυπική κατάσταση του συστήματος καθώς και το περιβάλλον διαχείρισης, το οποίο περιλαμβάνει τους χρήστες και τις ομάδες που έχουν δημιουργηθεί.

(5) Ιεραρχική διαχείριση : Περιλαμβάνει την κατάσταση του συστήματος για διαχείριση απομακρυσμένα της εφαρμογής DLP όπως είναι η επιβολή της πολιτικής, απομακρυσμένα γραφεία και τερματικούς σταθμούς εργασίας, συμπεριλαμβανομένων και της σύγκρισης του ποιοι κανόνες είναι ενεργοποιημένοι και που.

(6) Αναφορές : Το συγκεκριμένο περιλαμβάνει μια συνένωση προ – δημιουργημένων αναφορών καθώς και εργαλεία για να διευκολύνουν την ad hoc αναφορά.

(7) Δημιουργία Πολιτικής και Διαχείριση: Μετά την λειτουργία της Σειράς Διαχείρισης Περιστατικών, αυτή είναι η πιο σημαντική λειτουργία του διακομιστή της κεντρικής διαχείρισης. Περιλαμβάνει την δημιουργία και την διαχείριση των πολιτικών.

Τέλος θα πρέπει να αναφέρουμε στο σημείο αυτό ότι η διεπαφή της εφαρμογής του DLP θα πρέπει ευανάγνωστη και εύκολη στην προσπέλαση και στην πλοήγηση. Κάτι τέτοιο μπορεί να ακούγεται βασικό και περιττό παρόλα αυτά είμαστε εξοικειωμένοι με εργαλεία ασφαλείας που έχουν σχεδιαστεί απλοϊκά και λιτά και στα οποία χρησιμοποιείται η τεχνική ικανότητα του διαχειριστή. Από την στιγμή που μια εφαρμογή DLP ενδεχομένως να χρησιμοποιηθεί και πέρα από τα στενά πλαίσια της ασφάλειας και πολύ πιθανό και εκτός των ορίων του τμήματος πληροφορικής, η διαπεπαφή του χειρισμού απαιτείται να λειτουργεί για ένα μεγαλύτερο εύρος χειριστών.

3.15 Τα οφέλη από ένα πρόγραμμα DLP.

Εφαρμόζοντας ένα πρόγραμμα DLP αναμένουμε να αποκομίσουμε ορισμένα οφέλη, τα οποία βοηθούν την επιχείρηση να θωρακιστεί έναντι ορισμένων κινδύνων που έχουν αντίκτυπο στην όλη υπόσταση ενός οργανισμού. Επομένως ενδεικτικά μπορούμε να αναφέρουμε ότι:

α. Αποτροπή Διαρροής Δεδομένων: Αποτροπή τυχαίας ή κακόβουλης απώλειας δεδομένων από κατόχους πληροφοριών ή ακόμα και hachers ακόμα και όταν τα δεδομένα είναι κρυπτογραφημένα.

β. Μείωση του κόστους έρευνας και αποκατάσταση της φήμης του οργανισμού: Μειώνεται ο χρόνος απόκρισης σε μια πιθανή διαρροή στη διερεύνηση της απώλειας των δεδομένων. Επίσης μπορεί να μειώσει και το κόστος της ανοικοδόμησης της φήμης του οργανισμού μετά τη ζημιά.

γ. Διευκόλυνση της έγκαιρης ανίχνευσης κινδύνων καθώς και μείωσης τους: Εφαρμόζοντας το πρόγραμμα θα βοηθήσει στον εντοπισμό της διαρροής δεδομένων και θα συμβάλει στην διασφάλιση ότι οι πληροφορίες είναι αποθηκευμένες στην κατάλληλη θέση και με τον κατάλληλο τρόπο.

δ. Αίσθηση ασφαλείας στην διοίκηση του οργανισμού: Ο έλεγχος που θα πραγματοποιείται από την εφαρμογή DLP θα βοηθήσει ώστε να βεβαιωθούν τα ανώτερα διευθυντικά στελέχη ότι έχουν εφαρμοστεί οι κατάλληλες εγγυήσεις ασφαλείας, επιτρέποντας τους να συγκεντρωθούν σε άλλα κρίσιμα ζητήματα του οργανισμού.

3.16 Τα οφέλη για την επιχείρηση.

Γίνεται κατανοητό όπως και με οποιοδήποτε άλλο σύνολο εφαρμογών μέτρων ασφαλείας, μια εφαρμογή DLP θα πρέπει να στηρίζει τους στόχους της επιχείρησης και να παρέχει απτό όφελος για την επιχείρηση.

Παρακάτω τονίζονται ορισμένα από τα πιο άμεσα οφέλη μιας καλά προσαρμοσμένης εφαρμογής DLP.

α. Προστασία κρίσιμων επιχειρηματικών ψηφιακών δεδομένων καθώς και δεδομένα με πνευματική ιδιοκτησία. Ο κύριος σκοπός του DLP είναι η προστασία των δεδομένων τα οποία θεωρούνται κρίσιμα για την επιχείρηση. Οι επιχειρήσεις διατηρούν πολλά είδη πληροφοριών που πρέπει να τα προστατεύσουν για ανταγωνιστικούς, κανονιστικούς (νομικούς) και τέλος για λόγους φήμης. Δεδομένα όπως, προσωπικά στοιχεία πελατών, αρχεία που αφορούν το ίδιο το προσωπικό της επιχείρησης, πληροφορίες για την υγεία, απόρρητα οικονομικά αρχεία, αρχεία που αφορούν την σχεδίαση προϊόντος, αρχεία με διάφορα επιχειρηματικά σχέδια και μελλοντικές

ενέργειες, αρχεία ιδιωτικής έρευνας είναι μερικά μόνο παραδείγματα αντιπροσωπευτικά για το είδος των αρχείων που διατηρούνται.

β. Βελτίωση συμμόρφωσης: Η εφαρμογή DLP μπορεί να βοηθήσει έναν οργανισμό να βελτιωθεί σε ότι αφορά τις απαιτήσεις συμμόρφωσης, να ακολουθήσει δηλαδή καλύτερα τις εντολές και τις οδηγίες, σε ότι αφορά την προστασία και την παρακολούθηση δεδομένων που περιέχουν προσωπικές και οικονομικές πληροφορίες πελατών. Συνήθως μια εφαρμογή DLP τυπικά, έρχεται με εγκατεστημένους ορισμένους κανόνες από πριν, οι οποίοι περιέχουν τύπους δεδομένων, σύμφωνα με τους οποίους πραγματοποιείται συμμόρφωση προς τους συγκεκριμένους κανόνες. Τέτοιοι τύποι δεδομένων είναι, η μορφή μιας πιστωτικής κάρτας visa για παράδειγμα ή ο αριθμός κοινωνικής ασφάλισης. Αξιοποιώντας το σύνολο των κανόνων μπορεί να απλοποιηθούν οι προσπάθειες για την προστασία των δεδομένων που υπόκεινται σε αυτούς τους κανονισμούς.

γ. Μείωση του κινδύνου παραβίασης δεδομένων. Μειώνοντας τον κίνδυνο διαρροής δεδομένων, έχει ως αποτέλεσμα την μείωση του οικονομικού κινδύνου. Το γεγονός αυτό πετυχαίνετε από την εξασφάλιση ότι δεν θα καταβληθούν οικονομικές αποζημιώσεις εξαιτίας κάποιας παράνομης δημοσίευσης προσωπικών δεδομένων ή υποκλοπής πρότυπων αναπτυξιακών σχεδίων από ανταγωνιστές.

δ. Βελτίωση της εκπαίδευσης και της ευαισθητοποίησης: Παρόλο που οι περισσότερες επιχειρήσεις έχουν αναπτύξει και συντάξει πολιτικές ασφαλείας, είναι αναμενόμενο ότι μπορούν να ξεχαστούν με την πάροδο του χρόνου. Ένας συναγερμός από μία εφαρμογή DLP, ακόμα και το μπλοκάρισμα στην κίνηση δεδομένων τα οποία παραβιάζουν μια πολιτική, παρέχει μια συνεχή εκπαίδευση βοηθώντας με αυτόν τον τρόπο τους χρήστες να διασφαλίσουν μια συνείδηση των πολιτικών ασφαλείας που αφορούν ευαίσθητα δεδομένα και θα πρέπει να εφαρμόζουν.

ε. Βελτίωση των επιχειρηματικών διαδικασιών. Ένα από τα πλεονεκτήματα του DLP είναι η σχεδίαση νέων πολιτικών, ο έλεγχος και οι δοκιμές, τα οποία βοηθούν να ανακαλυφθούν ρωγμές στις διαδικασίες που ακολουθεί ο οργανισμός. Συχνά το στάδιο της απλής αξιολόγησης και της κατηγοριοποίησης της διαδικασίας του οργανισμού στο πλαίσιο μιας εφαρμογής DLP μπορεί να δημιουργήσει ιδέες για την επιχείρηση.

στ. Βελτιστοποίηση του αποθηκευτικού χώρου στο δίσκο και του εύρος δικτύου. Άλλο ένα σημαντικό πλεονέκτημα μιας εφαρμογής DLP είναι η αναγνώριση των στάσιμων αρχείων (και που δεν υπάρχει λόγος να χρησιμοποιηθούν) καθώς και των βίντεο συνεχούς ροής (streaming video) τα οποία καταναλώνουν ένα μεγάλο μέρος των πόρων πληροφορικής, όπως είναι ο αποθηκευτικός χώρος και το εύρος δικτύου. Εκκαθάριση παλαιών αρχείων, μη χρησιμοποιούμενων καθώς και των βίντεο συνεχούς ροής μπορούν να μειώσουν τις απαιτήσεις σε αποθηκευτικό χώρο για τα

αντίγραφα ασφαλείας (backup) καθώς και για το εύρος ζώνης του δικτύου που χρησιμοποιείται.

ζ. Εντοπισμός κακόβουλου λογισμικού: Ακόμα άλλο ένα πλεονέκτημα του DLP είναι ο εντοπισμός κακόβουλου λογισμικού, το οποίο προσπαθεί να μεταδώσει ευαίσθητα δεδομένα δια μέσου ηλεκτρονικού ταχυδρομείου ή μέσω μιας σύνδεσης στο διαδίκτυο (internet). Μια δικτυακή εφαρμογή DLP μπορεί να μας βοηθήσει να περιορίσουμε την ζημιά από ένα κακόβουλο λογισμικό, με τον εντοπισμό ψεύτικων εκπομπών εκτός επιχείρησης τα οποία περιέχουν ευαίσθητα δεδομένα. Κάτι τέτοιο όμως δεν είναι εγγυημένο και δεν συμβαίνει πάντα εξαιτίας του γεγονότος ότι οι εκπομπές αυτές μπορεί να είναι κρυπτογραφημένες. Παρόλα αυτά ακόμα και σε αυτή την περίπτωση, ένα σύστημα το οποίο έχει σαν κανόνα το συναγερμό ή το μπλοκάρισμα της ροής δεδομένων τα οποία δε μπορούν να αποκρυπτογραφηθούν, μπορεί να αποδειχθεί τελικά ότι από πίσω βρίσκεται η πραγματοποίηση μιας επίθεσης κακόβουλου λογισμικού.

3.17 Κίνδυνοι και Θέματα Ασφαλείας.

Όπως κάθε πολύπλοκη εφαρμογή πληροφορικής, έτσι και η εφαρμογή ενός DLP προγράμματος, εάν δεν διαχειριστεί σωστά, μπορεί να παρουσιάσει έναν αριθμό από κινδύνους για την επιχείρηση. Πολλοί από τους κινδύνους μπορεί να έχουν άμεσο αντίκτυπο στην λειτουργία της επιχείρησης, επομένως είναι πολύ σημαντικό να ληφθούν όλα εκείνα τα απαραίτητα μέτρα για να περιοριστεί το φαινόμενο αυτό σε όλους όσους εμπλέκονται στην διαδικασία. Ο Πίνακας 3, παρουσιάζει μια λίστα με τους κινδύνους στις βασικές λειτουργίες οι οποίες σχετίζονται με την εφαρμογή του DLP.

Επιχειρησιακοί – Λειτουργικοί Κίνδυνοι που σχετίζονται με την Υλοποίηση της DLP		
Κίνδυνος	Αντίκτυπο	Στρατηγική Περιορισμού
Λανθασμένος συντονισμός στην ενότητα του DLP για το δίκτυο.	▪ Διαταραχή - Διακοπή στις διαδικασίες της επιχείρησης. ▪ Απώλεια χρόνου και χρήματος. ▪ Ζημιά στις σχέσεις με τους πελάτες ή με τους συνεργάτες. ▪ Απώλεια υποστήριξης ενδιαφερομένων για τον οργανισμό.	▪ Η σωστή ρύθμιση και δοκιμή του συστήματος DLP θα πρέπει να γίνεται πριν από την ενεργοποίηση του πραγματικού κλειδώματος του περιεχομένου. ▪ Η ενεργοποίηση του συστήματος στην λειτουργία μόνο της παρακολούθησης θα επιτρέψει τη σωστή ρύθμιση, καθώς επίσης θα δίνεται η ευκαιρία να ειδοποιούνται οι χρήστες ότι έχουν πραγματοποιήσει διαδικασία η οποία δεν συμμορφώνεται με τους κανόνες έτσι ώστε να

		μπορούν να προσαρμοστούν ανάλογα. ▪ Με τη συμμετοχή των κατάλληλων στελεχών από τον οργανισμό και των ενδιαφερόμενων από την πληροφορική στον σχεδιασμό και την παρακολούθηση των σταδίων θα συμβάλει στη διασφάλιση ότι οι διαταραχές στις διαδικασίες θα αναμένονται και θα αντιμετωπίζονται. Τέλος, η θέσπιση ορισμένων μέσων προσβασιμότητας σε περίπτωση που υπάρχει κρίσιμο περιεχόμενο το οποίο πρέπει να χρησιμοποιηθεί και εμποδίζεται εκτός ωραρίου, όταν ο υπεύθυνος της εφαρμογής DLP δεν είναι διαθέσιμος.
Λάθος μέγεθος των τμημάτων DLP για το Δίκτυο.	▪ Πακέτα δικτύου που χάνονται ή απορρίπτονται μέσω των οποίων επιτρέπεται να περνάνε δεδομένα ανεξέλεγκτα.	▪ Η εξασφάλιση ότι το μέγεθος της μονάδας DLP είναι κατάλληλο για το μέγεθος της κίνησης του δικτύου είναι ένα κρίσιμο στοιχείο το οποίο θα πρέπει να εξεταστεί στο σχεδιασμό. Ωστόσο, είναι εξίσου σημαντικό να παρακολουθούνται οι ενότητες DLP του δικτύου για να διασφαλιστεί ότι η κυκλοφορία του δικτύου δεν αυξάνεται με την πάροδο του χρόνου σε ένα σημείο, και να καθιστά τη μονάδα αναποτελεσματική.
Υπερβολικές εκθέσεις και λαθεμένοι θετικοί συναγερμοί.	▪ Σπατάλη του χρόνου του προσωπικού. ▪ Διαφυγή έγκυρων απειλών. ▪ Τάση να αγνοούνται οι καταγραφές αρχείων με την πάροδο του χρόνου.	▪ Παρόμοια με ένα λάθος διαμορφωμένο σύστημα ανίχνευσης εισβολής (IDS), η εφαρμογή DLP μπορεί να εγγράψει σημαντικό αριθμό λαθεμένων θετικών συναγερμών, που ξεπερνούν το προσωπικό το οποίο μπορεί να παρακολουθήσει τις έγκυρες ειδοποιήσεις.

		▪ Αποφυγή υπερβολικής χρήσης λύσεων που στηρίζονται σε πρότυπα που επιτρέπουν ελάχιστη προσαρμογή. Το μεγαλύτερο χαρακτηριστικό μιας εφαρμογής DLP είναι η δυνατότητα να προσαρμόζουμε κανόνες ή πρότυπα σε συγκεκριμένα οργανωτικά μοτίβα δεδομένων. ▪ Είναι επίσης σημαντικό το σύστημα να αναπτύσσεται σε φάσεις, με έμφαση πρώτα στις περιοχές υψηλού κινδύνου. ▪ Προσπαθώντας να παρακολουθήσει πάρα πολλά μοτίβα δεδομένων ή επιτρέποντας πάρα πολλά σημεία ανίχνευσης μπορεί γρήγορα από νωρίς να σπαταλήσει πόρους.
Επιπλοκές με το λογισμικό ή με την επίδοση του συστήματος (ή εμπλοκές).	▪ Καθυστερήσεις στο σύστημα ▪ Υποβάθμιση των επιδόσεων ▪ Διάρρηξη – σπάσιμο της εφαρμογής DLP ή άλλων ελέγχων και διεργασιών.	Τα συστήματα DLP, ιδιαίτερα τα crawlers και οι end-point agents, μπορεί να έρχονται σε επιπλοκή με το λογισμικό άλλου συστήματος και με την απόδοση τους. Τα δικαιώματα πρέπει να ελεγχθούν κατά τον σχεδιασμό και των δοκιμών πριν την αποστολή. Η ιδανική περίπτωση θα ήταν η διάθεση ενός μόνιμου περιβάλλον δοκιμών. Να πραγματοποιηθεί έλεγχος με τον κατασκευαστή για ήδη γνωστές επιπλοκές. Βεβαιωνόμαστε ότι οι crawlers είναι σωστά ρυθμισμένοι και συντονισμένοι, και ότι η λειτουργία τους έχει προγραμματιστεί με τέτοιο τρόπο ώστε να αποφευχθεί η λειτουργία του συστήματος σε υψηλό ρυθμό λειτουργίας. Επίσης καλό θα ήταν να αποφεύγονται όταν αυτό είναι εφικτό, οι σαρώσεις end-point κατά τις ώρες αιχμής ή όταν τα συστήματα λειτουργούν

		με απομακρυσμένη σύνδεση. Ακόμα θα πρέπει να εξασφαλιστεί ότι όλα τα patches και οι αναβαθμίσεις έχουν δοκιμαστεί μέσα στο περιβάλλον δοκιμής πριν από την ανάπτυξη στη παραγωγή.
Αλλαγές στις καθημερινές διαδικασίες ή στις υποδομές πληροφορικής καθιστώντας τις ρυθμίσεις DLP αναποτελεσματικές.	Μείωση της αποτελεσματικότητας DLP λόγω παράκαμψης των ελέγχων DLP.	Ο διαχειριστής της εφαρμογής DLP ή ένας αντιπρόσωπος θα πρέπει να συμμετέχουν στην διαδικασία αλλαγής ρυθμίσεων για να εξασφαλιστεί ότι οι αλλαγές που πραγματοποιήθηκαν δεν παρακάμπτουν ή υποβαθμίζουν τις δυνατότητες DLP. Επιπλέον, οι επιχειρήσεις θα πρέπει να είναι καλά προετοιμασμένες για αλλαγές που σχετίζονται με τη DLP για τη μείωση του κινδύνου της εκ προθέσεως παράκαμψης του συστήματος DLP στο όνομα της αποτελεσματικότητας και της ταχύτητας.
Λανθασμένη τοποθέτηση των τμημάτων DLP στο δίκτυο.	Χαμένα ή άνευ ελέγχου ροές δεδομένων.	Είναι σημαντικό να διασφαλιστεί η σωστή τοποθέτηση των τμημάτων DLP του δικτύου. Χρειάζεται να έχουμε στη διάθεσή μας τον ακριβή χάρτη του δικτύου, και ότι τα τμήματα τοποθετούνται στο τελευταίο σημείο εξόδου των δεδομένων, που επιθυμούν οι οργανισμοί να παρακολουθούν.
Αστοχία των τμημάτων DLP.	Τα δεδομένα δεν μπορούν να ελεγχθούν εξαιτίας της μερικής ή της πλήρης αποτυχίας των τμημάτων.	Τα τμήματα DLP μπορεί να αποτύχουν, αλλά δεν αναφέρουν πάντα την κατάσταση τους στην κονσόλα. Είναι σημαντικό να γίνεται περιοδικός έλεγχος για να εξασφαλιστεί ότι τα τμήματα και τα συναφή φίλτρα τους αποδίδουν όπως αναμενόταν.
Λαθεμένες ρυθμίσεις ή λαθεμένες υπηρεσίες ενεργού καταλόγου.	Αδυναμία να εντοπιστεί παραβίαση και να εμφανιστεί στους κατάλληλους τελικούς χρήστες.	Η υπηρεσία καταλόγου είναι το κλειδί σύνδεσης μεταξύ μιας διεύθυνσης δικτύου και ενός πραγματικού χρήστη, και οι περισσότεροι οργανισμοί θα θέλουν να έχουν αυτή η διεργασία για τον, σε αντίθεση με την χειροκίνητη ανακάλυψη αυτής της

		πληροφορίας, η οποία μπορεί να είναι χρονοβόρα και δεν είναι πάντα πραγματοποιήσιμη. Οργανισμοί που στερούνται ή έχουν ελλιπή υπηρεσία καταλόγου θα πρέπει να εξετάσουν πρώτα πως θα αντιμετωπίσουν αυτό το κενό αυτού του κενού πριν από την υλοποίηση μιας εφαρμογής DLP.

Πίνακας 3:Κίνδυνοι από Λάθος Εφαρμογή DLP

3.18 Περιορισμοί DLP.

Όπως διαπιστώνουμε παραπάνω, μία λύση DLP μπορεί να βοηθήσει κατά πολύ μια επιχείρηση, έτσι ώστε να αποκτήσει μεγαλύτερη γνώση και εμπειρία στον έλεγχο των ευαίσθητων δεδομένων, οι ενδιαφερόμενοι, είτε αυτοί είναι επιχείρηση, είτε οργανισμός, είτε ιδιώτης, θα πρέπει να είναι σε θέση να καταλάβουν τους περιορισμούς, τα κενά και τις αδυναμίες μιας εφαρμογής DLP. Η κατανόηση αυτών των περιορισμών είναι το πρώτο που χρειάζεται κατά την ανάπτυξη της στρατηγικής των πολιτικών που θα ακολουθηθούν, έτσι ώστε να αντισταθμιστούν οι περιορισμοί που προκύπτουν λόγο της τεχνολογίας. Μερικοί από τους σημαντικότερους περιορισμούς που είναι κοινοί για όλες τις μορφές της εφαρμογής DLP είναι οι παρακάτω:

α. Κρυπτογράφηση: Οι εφαρμογές DLP μπορούν να ελέγξουν κρυπτογραφημένες πληροφορίες αφού όμως πρώτα έχουν αποκρυπτογραφηθεί. Για να πραγματοποιηθεί αυτό οι DLP agent (πράκτορες), οι συσκευές δικτύου και οι crawlers πρέπει να έχουν πρόσβαση, και να είναι σε θέση να χρησιμοποιήσουν, το αντίστοιχο κλειδί αποκρυπτογράφησης. Στην περίπτωση που οι χρήστες έχουν την δυνατότητα να χρησιμοποιούν προσωπικά προγράμματα κρυπτογράφησης των οποίων τα κλειδιά δεν είναι γνωστά στον οργανισμό, ώστε να τα εφαρμόσει η επιλογή DLP, τότε τα αρχεία δεν μπορούν να αναλυθούν. Συνεπώς για να περιοριστεί αυτός ο κίνδυνος, η πολιτική που θα εφαρμόζεται θα πρέπει να απαγορεύει την εγκατάσταση και την χρησιμοποίηση κρυπτογραφικών λύσεων οι οποίες δεν θα έχουν κεντρική διαχείριση, δεν θα έχει εγκατασταθεί από τον διαχειριστή του δικτύου καθώς τέλος οι χρήστες θα πρέπει να είναι ενημερωμένοι και εκπαιδευμένοι, στο ό,τι οτιδήποτε δε μπορεί να αποκρυπτογραφηθεί για επιθεώρηση (που σημαίνει ότι η εφαρμογή DLP έχει το κλειδί αποκρυπτογράφησης), τελικά θα μπλοκάρεται.

β. Γραφικά: Η λύση DLP δεν μπορεί έξυπνα να ερμηνεύσει αρχεία γραφικών. Ένα σύντομο μπλοκάρισμα ή χειροκίνητη επιθεώρηση όλων των συγκεκριμένων αρχείων, θα εξαλείψει ένα σημαντικό κενό στον έλεγχο των πληροφοριών του οργανισμού. Ευαίσθητες πληροφορίες μπορούν να σαρωθούν (scanned) και να αποθηκευτούν σε ένα αρχείο γραφικών ή ακόμα και να υπάρχουν πνευματικά δικαιώματα

στο αρχείο των γραφικών, όπως είναι τα έγγραφα που περιέχουν σχέδια, και τα οποία εκπίπτουν στην ίδια κατηγορία, των ευαίσθητων δηλαδή δεδομένων. Οι επιχειρήσεις, οι οργανισμοί ακόμα και οι ιδιώτες οι οποίοι διαθέτουν αρχεία γραφικών που το περιεχόμενό τους υπόκεινται σε πνευματικά δικαιώματα, θα πρέπει να αναπτύξουν ισχυρές πολιτικές που διέπουν τη χρήση και τη διάδοση τέτοιων πληροφοριών. Ενώ η εφαρμογή DLP δεν μπορεί να διαβάσει έξυπνα το περιεχόμενο από ένα αρχείο γραφικών, μπορεί όμως να εντοπίσει συγκεκριμένο είδος αρχείου, την πηγή του και τον προορισμό του. Αυτή η δυνατότητα, σε συνδυασμό με την καλή ανάλυση της κίνησης του δικτύου, μπορεί να σηκώσει σημαία (flag) σε ασυνήθιστη κίνηση αυτού του είδους της πληροφορίας και με αυτό τον τρόπο παρέχεται ένα επίπεδο ελέγχου.

γ. Πάροχοι – Υπηρεσίες τρίτων: Στην περίπτωση κατά την οποία ένας οργανισμός στέλνει ευαίσθητα δεδομένα σε ένα έμπιστο τρίτο μέλος, είναι έμφυτη και προφανής η εμπιστοσύνη ότι και ο πάροχος διαθέτει το ίδιο επίπεδο ελέγχου σε ότι αφορά την διαρροή πληροφοριών, μιας και σπάνια επεκτείνει ένας οργανισμός την λύση DLP στον πάροχο υπηρεσιών τηλεφωνίας και δικτύου. Στην περίπτωση αυτή ένα ισχυρό πρόγραμμα διαχείρισης τρίτων το οποίο θα ενσωματώνει μια αποτελεσματική γλώσσα επαφής και ένα πρόγραμμα υποστήριξης λογαριασμών θα βοηθούσε να περιοριστεί ο κίνδυνος αυτός.

δ. Κινητές Συσκευές: Με την έλευση των κινητών υπολογιστικών συσκευών, όπως είναι τα έξυπνα κινητά τηλέφωνα, αναπόφευκτα δημιουργήθηκαν κανάλια επικοινωνίας τα οποία δεν είναι εύκολο να παρακολουθηθούν ή να ελεγχθούν. Η υπηρεσία σύντομων μηνυμάτων (Short Message Service – SMS), ένα πρωτόκολλο επικοινωνίας το οποίο επιτρέπει την ανταλλαγή σύντομων μηνυμάτων κειμένου, είναι ένα βασικό παράδειγμα. Άλλο ένα ζήτημα είναι η δυνατότητα αυτών των συσκευών να συνδέονται και να χρησιμοποιούν το ασύρματο δίκτυο Wi-Fi ή ακόμα και να γίνουν οι ίδιες Wi-Fi Hot-Spot. Και οι δύο περιπτώσεις επιτρέπουν την επικοινωνία μέσω ενός εξωτερικού διαύλου ο οποίος δεν μπορεί να παρακολουθηθεί από τους περισσότερους οργανισμούς. Τέλος η δυνατότητα που έχουν πολλές από τις συσκευές αυτές να πραγματοποιούν λήψη και αποθήκευση φωτογραφιών ή ακόμα και αρχείων ήχου, μας παρουσιάζει ένα ακόμα πρόβλημα ασφαλείας. Παρόλο που έχει πραγματοποιηθεί πρόοδος στον τομέα αυτό, παραμένει μια πρόκληση για την διοίκηση ο περιορισμός της συγκεκριμένης δυνατότητας. Απέναντι σε αυτή την κατάσταση η καλύτερη αντιμετώπιση θα ήταν η σχεδίαση ισχυρής πολιτικής και η υποστήριξη εκπαίδευσης των χρηστών στην σωστή χρήση των συσκευών αυτών καθώς και η ευθιξία και ευαισθητοποίηση τους.

ε. Πολύγλωσση Υποστήριξη: Ορισμένες εφαρμογές DLP υποστηρίζουν πολλαπλές γλώσσες, αλλά σχεδόν όλες οι κονσόλες διαχείρισης υποστηρίζουν μόνο Αγγλικά. Είναι γεγονός ότι για κάθε γλώσσα και κάθε χαρακτήρα που προστίθεται στο σύστημα θα πρέπει να υποστηρίζεται από τις αντίστοιχες απαιτήσεις επεξεργασίας για την αύξηση της ανάλυσης. Μέχρι να αντιληφθούν οι εμπορικές εταιρίες την ανάγκη που υπάρχει στην αγορά για την κάλυψη αυτού του κενού, υπάρχει μια μικρή

διέξοδος ώστε να εφαρμοστούν άλλες μέθοδοι που θα ελέγχουν την διαρροή πληροφοριών σε άλλες γλώσσες πέρα από την Αγγλική. Οι πολυεθνικές επιχειρήσεις και οργανισμοί θα πρέπει να εξετάσουν πιο προσεκτικά το δυναμικό κενό όταν αξιολογούν και αναπτύσσουν μια λύση DLP.

Να επισημανθεί στο σημείο αυτό ότι τα σημεία που αναφέρθηκαν παραπάνω δεν έχουν σκοπό να αποθαρρύνουν τους οργανισμούς ή τους ιδιώτες από την υιοθέτηση μιας εφαρμογής DLP. Η μοναδική διέξοδος για πολλούς οργανισμούς είναι η εφαρμογή πολιτικής στην συμπεριφορά, όσο μπορεί να υλοποιηθεί αυτό, των χρηστών. Αυτό έχει σαν αποτέλεσμα η φυσική ασφάλεια να συμπληρώνει την σουίτα των ελέγχων που πραγματοποιείται με την βοήθεια της τεχνολογίας ακόμα και σήμερα. Αυτές που μπορούμε να αναφέρουμε είναι:

α. Λύση Κλειδώματος: Αυτή την στιγμή δεν υπάρχει δυνατότητα μεταφοράς κανόνων DLP μεταξύ διαφορετικών εφαρμογών DLP, το οποίο σημαίνει ότι η αλλαγή από μία εταιρία λογισμικού σε άλλη ή η ενσωμάτωση των διάφορων λειτουργιών σε διαφορετικές εφαρμογές είναι δυνατόν να απαιτήσει συγκεκριμένη εργασία για την αντικατάσταση ενός σύνθετου κανόνα σε μια διαφορετική εφαρμογή DLP.

β. Περιορισμένη υποστήριξη σε μη διαδεδομένα Λειτουργικά συστήματα: Πολλές εφαρμογές DLP δεν διαθέτουν πράκτορες (agent) σε end-point DLP για λειτουργικά συστήματα όπως είναι το Linux και Mac γιατί η χρησιμοποίησή τους από χρήστες σε έναν οργανισμό είναι πιο σπάνια. Επομένως αυτό το γεγονός αφήνει ένα σημαντικό κενό για τους οργανισμούς που χρησιμοποιούν τέτοια λειτουργικά. Ο κίνδυνος αυτός μπορεί να περιοριστεί με την εφαρμογή πολιτικής που έχει σχέση με την συμπεριφορά των χρηστών ή η απαίτηση για την χρησιμοποίηση προσαρμοσμένων εφαρμογών οι οποίες τυπικά δεν συμπεριλαμβάνονται μέσα στην πλατφόρμα της εφαρμογής DLP.

γ. Υποστήριξη διασταυρούμενων εφαρμογών: Οι λειτουργίες μιας εφαρμογής DLP μπορούν να περιοριστούν και από το είδος των εφαρμογών που χρησιμοποιούνται στον τελικό σταθμό εργασίας. Ένας πράκτορας DLP, ο οποίος είναι σε θέση να παρακολουθεί τους χειρισμούς των δεδομένων για μια εφαρμογή μπορεί να μην είναι σε θέση να το πραγματοποιήσει για μια άλλη εφαρμογή στο ίδιο σύστημα. Οι οργανισμοί θα πρέπει να διασφαλίσουν ότι όλες οι εφαρμογές που διαθέτουν ή χειρίζονται ευαίσθητα δεδομένα έχουν αναγνωριστεί ποιες είναι και έχει διαπιστωθεί ότι η εφαρμογή DLP τις υποστηρίζει. Σε περίπτωση που υπάρχουν εφαρμογές που δεν υποστηρίζονται, θα πρέπει να απαιτηθούν άλλες ενέργειες μέσω της πολιτικής, ή αν είναι εφικτό, ακόμα και αίτηση για την αφαίρεση της συγκεκριμένης εφαρμογής.

Κεφάλαιο 4 : Τυπική Δομή – Ανάπτυξη και Λειτουργία DLP

4.1 Εισαγωγή

Έχει ήδη αναφερθεί ότι ένα σύστημα δηλώνει έναν αριθμό αλληλοεπιδρώντων στοιχείων τα οποία έχουν οργανικά συναρμολογηθεί σε μια ολότητα, με τρόπο ώστε να εκτελούν μια ορισμένη λειτουργία. Επίσης μπορούμε να αναφέρουμε ότι αποτελείται από τα παρακάτω τρία υποσυστήματα:

1. Το Φυσικό σύστημα παραγωγής (physical production system) το οποίο όπως γίνεται αντιληπτό μετασχηματίζει την πρώτη ύλη που εισέρχεται στο σύστημα σε προϊόν, σύμφωνα με τις εντολές και οδηγίες που λαμβάνει από το σύστημα διοίκησης.
2. Το σύστημα διοίκησης/ λήψης αποφάσεων (management system, decision system) είναι το σύστημα το οποίο παραλαμβάνει πληροφορίες και δεδομένα από το πληροφοριακό υποσύστημα και παράγει εντολές και παραγγελίες προς το φυσικό σύστημα παραγωγής και οδηγίες για τις προσδοκίες και επιδιώξεις της διοίκησης, που επιθυμεί να επιτευχθούν.
3. Το πληροφοριακό σύστημα (information system) το οποίο συνδέει το φυσικό σύστημα παραγωγής με το σύστημα διοίκησης και λήψης αποφάσεων. Μετασχηματίζει δεδομένα, που υπάρχουν στο φυσικό σύστημα παραγωγής και σχετίζονται με την απόδοση της παραγωγικής διαδικασίας, σε πληροφορίες και δεδομένα που απαιτεί το σύστημα της διοίκησης για να πάρει αποφάσεις. Μετασχηματίζει τις εντολές του συστήματος σε κατάλληλες οδηγίες, πληροφορίες, δεδομένα για το φυσικό σύστημα παραγωγής.

Όλα αυτά είναι αναγκαία και απαραίτητα για την υλοποίηση και την δημιουργία μιας ενιαίας ενότητας που αποτελεί ο οργανισμός ή η επιχείρηση.

4.2 Αναγκαιότητα Προστασίας των Πληροφοριακών Συστημάτων.

Είναι γεγονός ότι ένα πληροφοριακό σύστημα σχετίζεται άμεσα με τρία βασικά στοιχεία που απαιτούν και ένα ξεχωριστό τρόπο αντιμετώπισης:

Σχετίζονται διπλά με τον άνθρωπο από την στιγμή που δημιουργούνται από αυτόν και λειτουργούν με την βοήθειά του ώστε να εξυπηρετούν πάλι αυτόν.

Σχετίζονται με τη πληροφορία ένα αγαθό με πάρα πολύ μεγάλη ζήτηση και αξία. Υπάρχει το θέμα της προστασίας ευαίσθητων πληροφοριών καθώς και της προστασίας των προσωπικών στοιχείων κάθε ατόμου.

Στηρίζονται στην πληροφορική, η οποία είναι τεχνολογία που χαρακτηρίζεται από τον μεγάλο ρυθμό εξέλιξής της. Επιπροσθέτως με την χρησιμοποίηση της πληροφορικής οι διαδικασίες επεξεργασίας πληροφοριών παρουσιάζουν μεγάλα περιθώρια προστιθέμενης αξίας. Τέλος το όλο πληροφοριακό σύστημα έχει ένα κύκλο ζωής μόλις 3-5 ετών, είναι ζωτικής σημασίας για μια επιχείρηση και αποτελεί σημαντική οικονομική επένδυση.

4.2.1 Τοποθέτηση των Μέτρων Ασφαλείας

Είναι γεγονός ότι ένα τυπικό Πληροφοριακό Σύστημα μπορεί να μοντελοποιηθεί χρησιμοποιώντας 5 διαφορετικά επίπεδα – στρώματα (layers) συστατικών. Αυτά μπορούμε να αναφέρουμε ότι είναι:

α. Τα προγράμματα εφαρμογών, που προσαρμόζονται κατά τέτοιο τρόπο ώστε να ικανοποιούνται οι απαιτήσεις των χειριστών.

β. Τις υπηρεσίες, οι οποίες χρησιμοποιούνται από τα προγράμματα εφαρμογών, όπως είναι για παράδειγμα αυτές που παρέχονται από ένα ΣΔΒΔ.

γ. Το λειτουργικό σύστημα, με βάση το οποίο παρέχονται οι υπηρεσίες και το οποίο παρέχει διαχείριση αρχείων, εκτυπωτών κλπ.

δ. Τον πυρήνα (το κεντρικό τμήμα του λειτουργικού συστήματος), που κανονίζει την προσπέλαση της μνήμης και του επεξεργαστή.

ε. Το υλικό, όπως είναι οι μνήμες, ο επεξεργαστής κλπ.

4.2.2 Προβλήματα κατά την Εισαγωγή Ασφάλειας

Αξίζει επιπλέον να αναφερθούμε ότι η εισαγωγή (προσθήκη μηχανισμών) ασφαλείας σε ένα πληροφοριακό σύστημα είναι ένα αρκετά δύσκολο και περίπλοκο έργο. Για να γίνει αντιληπτό το γεγονός αυτό θα επικεντρωθούμε στα παρακάτω:

α. τα σύγχρονα πληροφοριακά συστήματα περιέχουν συχνά ένα τεράστιο σε όγκο και πολυπλοκότητα λογισμικό, και τα μεγάλα έργα λογισμικού έχει αποδειχθεί από την εμπειρία ότι είναι σχεδόν αδύνατο να υλοποιηθούν χωρίς να πραγματοποιηθούν λάθη.

β. η ασφάλεια συνήθως δεν περιλαμβάνεται στο αρχικά σχεδιασμένο ή υλοποιημένο σύστημα αλλά προστίθεται κατόπιν.

γ. η ασφάλεια κοστίζει, συνήθως αρκετά.

δ. πολύ συχνά το πρόβλημα έγκειται στους ανθρώπους που χρησιμοποιούν το σύστημα και όχι στην τεχνολογία που χρησιμοποιείται.

Έχει γίνει παραδεκτό ότι οι χρήστες και οι υπάλληλοι ενός οργανισμού είναι επιβεβλημένο να αποκτήσουν «κουλτούρα» της ασφάλειας ώστε να είναι ευαισθητοποιημένοι σε ότι αφορά την προστασία των δεδομένων τους, την σωστή αποθήκευσή τους και την κατά νόμο ορθή χρησιμοποίησή τους.

4.3 Μοντέλο Ροής – Πληροφοριών

Σύμφωνα με τα μοντέλα ασφαλείας συμμορφώνονται οι μηχανισμοί που επιβάλλουν τις πολιτικές ασφαλείας.

Θα παρατηρήσουμε το Μοντέλο «Ροής – Πληροφοριών» (Information – Flow) σύμφωνα με το οποίο εξετάζεται οποιαδήποτε είδος ροής πληροφοριών και δεδομένων (όχι μόνο την άμεση πληροφοριακή ροή μέσω ενεργειών προσπέλασης που μοντελοποιείται στο BLP). Μια πληροφοριακή ροή προκαλείται από ένα αντικείμενο

x σε ένα αντικείμενο y όταν μπορούμε να μάθουμε περισσότερα για το x παρατηρώντας το y. Αν ήδη γνωρίζουμε το x τότε δεν μπορεί να υπάρξει πληροφοριακή ροή από το x. Μπορούμε να διαχωρίσουμε:

Σαφούς πληροφοριακής ροής: η παρατήρηση του y μετά την εκχώρηση y:=x μας λέει για την τιμή του x.

Υπονοούμενης πληροφοριακής ροής: η παρατήρηση του y μετά την εξαρτώμενη εντολή if x=0 then y:=1. Για παράδειγμα, αν y=2, τότε ξέρουμε ότι x=/0.

Τα συστατικά του μοντέλου ροής – πληροφοριών αποτελούνται από :

α. Ένα δικτυωτό από ετικέτες ασφαλείας

β. Ένα σύνολο αντικειμένων με ετικέτες

γ. Μιας πολιτική ασφάλειας, όπου η ροή πληροφοριών από ένα αντικείμενο με ετικέτα c1 σε ένα αντικείμενο με ετικέτα c2 επιτρέπεται μόνο αν c1<c2. Κάθε ροή πληροφοριών που παραβαίνει αυτόν τον κανόνα είναι παράνομη.

Σύμφωνα με αυτό το μοντέλο ένα σύστημα ονομάζεται ασφαλές αν δεν υπάρχει παράνομη πληροφοριακή ροή. Από τα πλεονεκτήματα που μπορούμε να αναφέρουμε είναι ότι το συγκεκριμένο μοντέλο καλύπτει όλα τα είδη πληροφοριακών ροών. Από την άλλη πλευρά μπορούμε να παρατηρήσουμε ότι με αυτόν τον τρόπο γίνεται όλο και πιο δύσκολος ο σχεδιασμός ασφαλών συστημάτων.

4.4 Μοντέλο Ασφαλείας Πληροφοριακών Συστημάτων

Είναι γεγονός ότι μέχρι τις μέρες μας έχουν προταθεί διάφορα μοντέλα ασφαλείας πληροφοριακών συστημάτων. Τα μοντέλα αυτά είναι αυτά που θα χρησιμοποιηθούν σαν αφετηρία για την δημιουργία των μηχανισμών και των μέτρων προστασίας. Τα κυριότερα είναι:

α. Μοντέλο Κιβωτισμού

β. Μοντέλο του Καταλόγου

γ. Μοντέλο του Πίνακα

δ. Μοντέλο του Φίλτρου

ε. Μοντέλο των Επάλληλων Στρωμάτων

Στην παρούσα φάση θα επικεντρωθούμε στο Μοντέλο του Πίνακα και να αναφερθούμε ότι το DLP βασίζεται πάνω σε αυτό το μοντέλο.

Το πλεονέκτημά του είναι ότι επιτρέπει την απεικόνιση διαφορετικών θεμάτων ταυτόχρονα. Το μοντέλο στηρίζεται σε ένα πίνακα τριών διαστάσεων:

α. Στην πρώτη διάσταση αντιπροσωπεύονται τα κρίσιμα πληροφορικά χαρακτηριστικά (critical information characteristics) για να θεωρείται ένα σύστημα ασφαλές, δηλαδή:

(1) η εμπιστευτικότητα

(2) η ακεραιότητα

(3) η διαθεσιμότητα

Συνεπώς γίνεται κατανοητό ότι εφαρμόζοντας τις πολιτικές ασφαλείας ενός προγράμματος DLP θα πρέπει τα δεδομένα να υπακούσουν στα παραπάνω χαρακτηριστικά. Δηλαδή δεν θεωρείται επιτυχημένο ένα πρόγραμμα DLP όταν απαγορεύει την χρησιμοποίηση μιας πληροφορίας γιατί δεν θα είναι διαθέσιμη.

β. Στη δεύτερη διάσταση απεικονίζονται οι τρεις καταστάσεις (information states) στις οποίες βρίσκεται η πληροφορία μέσα στο σύστημα, επομένως:

(1) η μετάβαση (transmission)
(2) η αποθήκευση (storage)
(3) η επεξεργασία

Η εφαρμογή DLP θεωρείται επιβεβλημένο για να θεωρηθεί επιτυχής να είναι σε θέση να ανιχνεύει, να παρακολουθεί, να εντοπίζει τα ευαίσθητα δεδομένα που έχουν προκαθοριστεί από τις αντίστοιχες πολιτικές, σε όλες τις μορφές στις οποίες δύναται να βρεθούν δεδομένα.

γ. Στη τρίτη διάσταση σχετίζεται με τα μέτρα προφύλαξης (security measures)

4.5 Πως Αναπτύσσεται ένα ΣΔΑΠ

Αναπτύσσοντας ένα ΣΔΑΠ για τις ανάγκες ενός οργανισμού εφαρμόζονται ορισμένες διαδικασίες μέσω ενός συστήματος διεργασιών, το οποίο μαζί με την καταγραφή τους, μαζί με τις αλληλεπιδράσεις αυτών των διεργασιών και τη διαχείρισή τους, καλούνται ως διεργασιοκεντρική προσέγγιση (process-based approach).

Μπορούμε να αναφέρουμε ότι ένα βασικό στοιχείο της διεργασιοκεντρικής προσέγγισης είναι η χρησιμοποίηση μεθόδων για τον έλεγχο και την συνεχή βελτίωση των διεργασιών. Μια τέτοια μέθοδος είναι η PDCA (Plan – Do – Check – Act). Η συγκεκριμένη μέθοδος χρησιμοποιείται έχοντας σαν φάρο το πρότυπο ISO/IEC 27001. Άλλη μέθοδος πλέον για την βελτίωση μιας διεργασίας είναι η DMAIC (Define – Measure – Analyze – Improve – Control). Η PDCA είναι μια επαναληπτική μέθοδος 4 βημάτων:

α. Σχεδιασμός (Plan): Αναλύεται η κατάσταση του οργανισμού, θέτονται οι στόχοι και καταστρώνονται τα σχέδια για να επιτευχθούν οι στόχοι αυτοί.

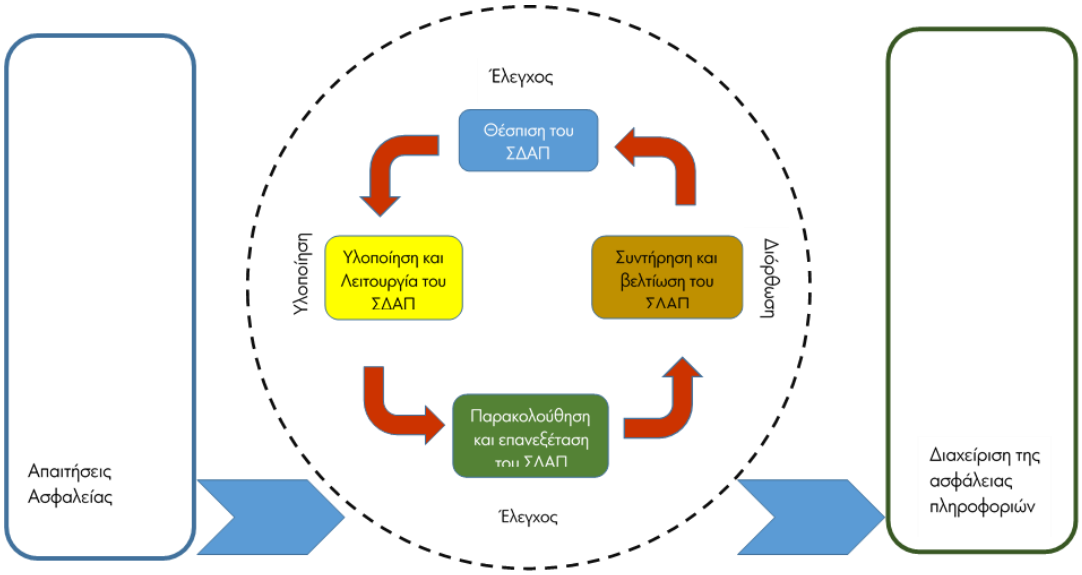
β. Υλοποίηση (Do): Πραγματοποιείται η υλοποίηση των σχεδίων.

γ. Έλεγχος (Check): Μετράμε τα αποτελέσματα σε σχέση πάντα με τους στόχους που έχουμε βάλει.

δ. Διόρθωση (Act): Πραγματοποιείται διόρθωση και βελτίωση των δραστηριοτήτων μαθαίνοντας από τα λάθη μας, ώστε να επιτύχουμε καλύτερα αποτελέσματα.

Στη φάση του σχεδιασμού σκεφτόμαστε και σχεδιάζουμε το ΣΔΑΠ εκτιμώντας τον κίνδυνο που διατρέχει η ασφάλεια πληροφοριών και επιλέγοντας κατάλληλα μέτρα ασφαλείας. Σε αυτή την φάση θεωρείται επιβεβλημένο να έχουν ολοκληρωθεί ο καθορισμός του πεδίου εφαρμογής του ΣΔΑΠ (κτήρια συστήματα δεδομένα), η θέσπιση πολιτικής ασφαλείας, ο ορισμός της μεθόδου ανάλυσης των κινδύνων που θα υλοποιηθεί, η λήψη έγκρισης από τη διοίκηση του οργανισμού και η διαμόρφωση της δήλωσης εφαρμογής.

Στη φάση υλοποίησης γίνεται πράξη και μπαίνουν σε λειτουργία οι δράσεις που σχεδιάστηκαν στην προηγούμενη φάση.



Εικόνα 8:Φάσεις Δημιουργίας ενός ΣΔΑΠ

Θα πρέπει στη φάση αυτή να έχει διαμορφωθεί το σχέδιο διαχείρισης κινδύνων, η κατανομή ρόλων και αρμοδιοτήτων, η υλοποίηση των μέτρων ασφαλείας για την επίτευξη συγκεκριμένων στόχων, ο καθορισμός του τρόπου αξιολόγησης της αποτελεσματικότητας των μέτρων ασφαλείας, ο σχεδιασμός και η υλοποίηση δράσεων ενημέρωσης και κατάρτισης για την ασφάλεια πληροφοριών, η λειτουργία του ΣΔΑΠ, η υλοποίηση των διαδικασιών ανίχνευσης περιστατικών ασφαλείας και η υλοποίηση των διαδικασιών αντιμετώπισης περιστατικών παραβίασης ασφαλείας.

Στη φάση αυτή ελέγχεται και αξιολογείται η απόδοση του ΣΔΑΠ και αναφέρονται τα αποτελέσματα στην διοίκηση του οργανισμού. Ελέγχεται η καλή λειτουργία των διαδικασιών που ακολουθούνται για την έγκαιρη ανίχνευση λαθών, για την έγκαιρη ανίχνευση περιστατικών παραβίασης ασφαλείας, για τον έλεγχο της τήρησης των αρμοδιοτήτων ασφαλείας, για την αποτελεσματικότητα των ενεργειών διαχείρισης περιστατικών ασφαλείας, τακτικοί έλεγχοι της αποτελεσματικότητας του ΣΔΑΠ, έλεγχος αποτελεσματικότητας των μέτρων ασφαλείας, έλεγχος στοιχείων της μελέτης ανάλυσης κινδύνων, τακτικοί εσωτερικοί έλεγχοι και τακτική επανεξέταση του ΣΔΑΠ ή τμημάτων του από τη διοίκηση του οργανισμού.

Στην επόμενη φάση, τη φάση της διόρθωσης πραγματοποιούνται οι απαραίτητες αλλαγές στο ΣΔΑΠ ώστε να βελτιώσουμε την απόδοσή του, σύμφωνα με τα αποτελέσματα των εσωτερικών ελέγχων και την επανεξέταση του ΣΔΑΠ που έγινε από την διοίκηση. Εκτελούνται στην φάση αυτή δραστηριότητες όπως η διόρθωση σημείων που εμφανίστηκαν στον έλεγχο ότι θέλουν διόρθωση, η υλοποίηση διορθωτικών ενεργειών, η υλοποίηση προληπτικών ενεργειών, η ενημέρωση των ιδιοκτητών για τις διορθώσεις και ο έλεγχος της αποτελεσματικότητας των διορθώσεων, η ενημέρωση των ιδιοκτητών για τις διορθώσεις και ο έλεγχος της αποτελεσματικότητας των διορθώσεων.

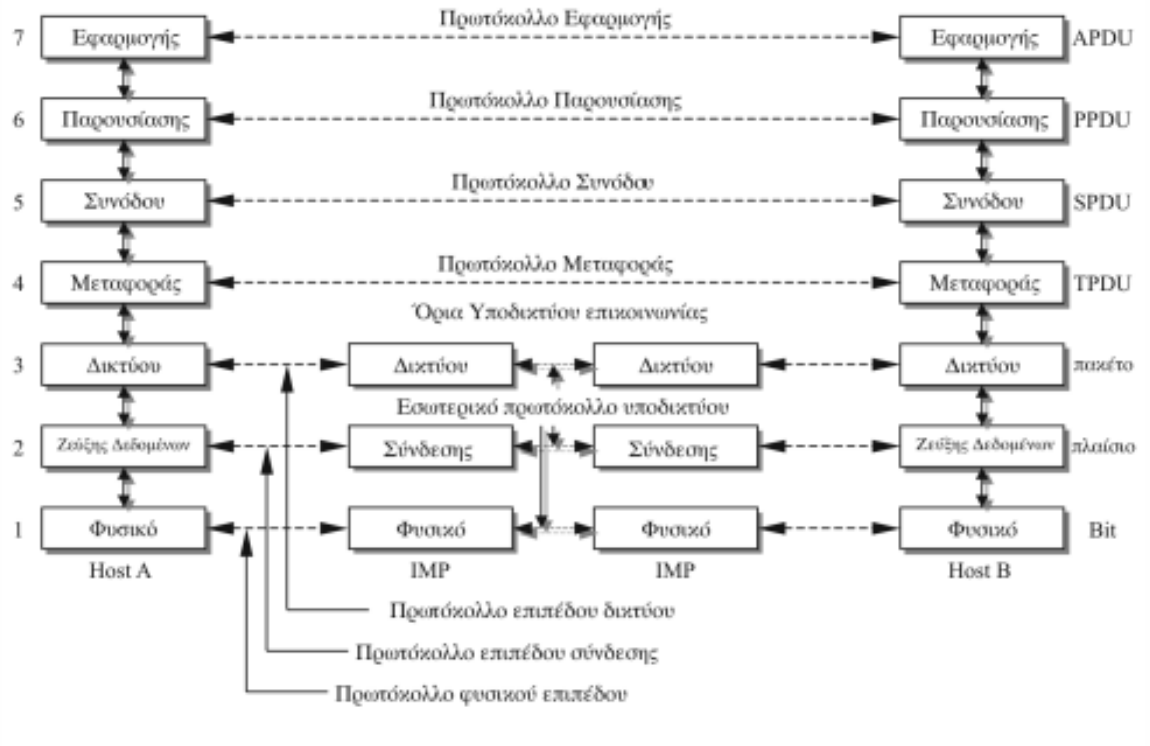
4.6 Πώς θα υλοποιηθεί ένα ΣΔΑΠ.

Από την στιγμή που θα έχει διαμορφωθεί το σχέδιο διαχείρισης κινδύνων το οποίο θα έχει εκπονηθεί και με βάση την σπουδαιότητα των μέτρων ασφαλείας που υλοποιούμε ώστε να δώσουμε την κατάλληλη προτεραιότητα σε καθεμία δραστηριότητα ασφαλείας. Η σπουδαιότητα εξαρτάται από τις συνέπειες που σχετίζονται με τον κίνδυνο από την πιθανότητα εμφάνισης του κινδύνου και από τις νομικές και κανονιστικές απαιτήσεις.

Ανάλογα το μέγεθος και το απαιτούμενο επίπεδο ασφαλείας η δραστηριότητα της υλοποίησης μπορεί να είναι και επίπονη και χρονοβόρα. Επίσης η υλοποίηση του ΣΔΑΠ περιλαμβάνει και τη διεξαγωγή δραστηριοτήτων επίγνωσης και κατάρτισης.

4.7 Μοντέλα Αναφοράς

Όταν αναφερόμαστε στα Μοντέλα Αναφοράς εννοούμε ένα μοντέλο που χρησιμοποιείται για να επεξηγήσει τον τρόπο με τον οποίο συνεργάζονται οι επιμέρους συνιστώσες ενός συστήματος και περιλαμβάνει τις προδιαγραφές των διεπαφών που υπάρχουν για τις διάφορες συνιστώσες. Μια συνήθης πρακτική την οποία θα ακολουθήσουμε και για την εφαρμογή DLP είναι η διαίρεση της συνολικής λειτουργικότητας σε επίπεδα (layers), με σκοπό την μείωση της πολυπλοκότητάς του, την καλύτερη κατανόηση και την ομαλότερη προσαρμογή στα συστήματα.



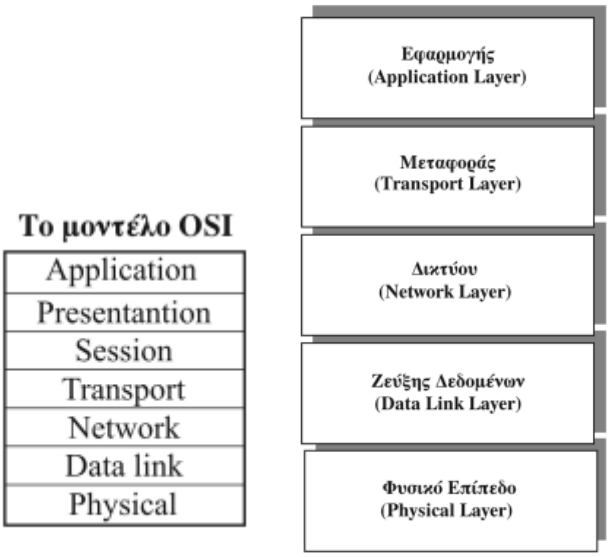
Εικόνα 9:Διάφορα επίπεδα (Layers)

4.7.1 Το μοντέλο OSI

Γνωρίζουμε ότι τα δίκτυα υπολογιστών για να μειώσουν την πολυπλοκότητα κατά την σχεδίαση και να γίνουν πιο κατανοητά, έχουν οργανωθεί σε σειρές στρωμάτων – επιπέδων (layers) και το καθένα χτίζεται πάνω στο προηγούμενό του. Δημιουργείται με αυτόν τον τρόπο η δομή στον σχεδιασμό δικτυακών πρωτοκόλλων. Το κάθε επίπεδο προσφέρει συγκεκριμένες υπηρεσίες στο αμέσως ανώτερο επίπεδο. Οι κανόνες που διέπουν την επικοινωνία των ομότιμων επιπέδων αποτελούν και τα πρωτόκολλα του επιπέδου. Επίσης το πρωτόκολλο καθορίζει και την μορφή και την σημασία που έχουν τα δεδομένα, τα οποία ανταλλάσσονται από τις ομότιμες οντότητες. Ένα επίπεδο πρωτοκόλλου μπορεί να υλοποιηθεί με λογισμικό, με υλικό ή με ένα συνδυασμό των δύο. Τα πρωτόκολλα επιπέδου εφαρμογής, όπως είναι για παράδειγμα τα HTTP και SMTP, υλοποιούνται πάντα με λογισμικό στα τερματικά συστήματα εργασίας. Κάτι αντίστοιχο συμβαίνει και με τα πρωτόκολλα επιπέδου μεταφοράς. Στη συνέχεια το φυσικό επίπεδο και το επίπεδο ζεύξης δεδομένων είναι υπεύθυνα για τον χειρισμό των επικοινωνιών σε μια συγκεκριμένη ζεύξη, συνήθως υλοποιούνται σε μια κάρτα διεπαφής δικτύου (π.χ. κάρτες Ethernet και κάρτες wi-fi), που σχετίζεται με μια δεδομένη ζεύξη. Το επίπεδο δικτύου υλοποιείται με ένα μείγμα υλικού – λογισμικού. Τέλος το πρωτόκολλο επιπέδου κατανέμεται ανάμεσα σε τερματικά συστήματα, σε μεταγωγείς πακέτων και σε άλλα συστατικά, τα οποία απαρτίζουν το δίκτυο.

Όταν ληφθούν όλα μαζί τα πρωτόκολλα των διαφόρων επιπέδων ονομάζονται στοίβα πρωτοκόλλων (protocol stack). Μπορούμε στο σημείο αυτό να επισημάνουμε τα δύο επίπεδα αναφοράς το στοίβα πρωτοκόλλων Διαδικτύου και το επίπεδο αναφοράς OSI.

Η στοίβα πρωτοκόλλων Διαδικτύου αποτελείται από 5 επίπεδα. Το φυσικό επίπεδο, το επίπεδο ζεύξης, το επίπεδο δικτύου, το επίπεδο μεταφοράς και το επίπεδο εφαρμογής όπως φαίνεται στον παρακάτω πίνακα. Δίπλα υπάρχει και ο πίνακας που εμφανίζει το μοντέλο αναφοράς OSI το οποίο αποτελείται από 7 επίπεδα.



Εικόνα 10:Μοντέλο OSI και Πρωτόκολλο Διαδικτύου

Το μοντέλο OSI είναι το πλαίσιο μέσα στο οποίο κινούνται οι λεπτομερείς τυποποιήσεις, για την επίλυση των προβλημάτων που εμφανίζονται στις επικοινωνίες των υπολογιστών. Το μοντέλο OSI παρέχει την δυνατότητα σε διαφορετικά υπολογιστικά συστήματα να επικοινωνούν μεταξύ τους. Η φιλοσοφία του στηρίζεται στην επιπεδοποίηση και όπως λέει και το όνομά του έχει σκοπό την ανοικτή και ελεύθερη επικοινωνία μεταξύ συστημάτων. Κατόπιν όλες οι λειτουργίες που απαιτούνται για την επικοινωνία κατηγοριοποιούνται σε επτά επίπεδα. Επομένως στον παρακάτω πίνακα φαίνονται τα 7 επίπεδα του μοντέλου OSI:

Επίπεδο 1	Φυσικό (Physical Layer)
Επίπεδο 2	Σύνδεσης Δεδομένων (Data Link Layer)
Επίπεδο 3	Δικτύου (Network Layer)
Επίπεδο 4	Μεταφοράς (Transport Layer)
Επίπεδο 5	Συνόδου (Session Layer)
Επίπεδο 6	Παρουσίασης (Presentation Layer)
Επίπεδο 7	Εφαρμογής (Application Layer)

Πίνακας 4:Επίπεδα Μοντέλου OSI

Στο σημείο αυτό θα πρέπει να σημειώσουμε ότι κατά τον ορισμό των επιπέδων ακολουθούνται ορισμένες αρχές:

1. Ένα επίπεδο δημιουργείται εφόσον είναι απαραίτητο.
2. Κάθε επίπεδο εκτελεί μια σαφώς ορισμένη λειτουργία.
3. Η λειτουργία κάθε επιπέδου ακολουθεί κατά τον δυνατόν διεθνή πρότυπα πρωτοκόλλων.
4. Τα όρια κάθε επιπέδου ελαχιστοποιούν τη ροή των πληροφοριών διαμέσου διαφορετικών επιπέδων
5. Διαφορετικές λειτουργίες ορίζονται σε διαφορετικά επίπεδα.

Επίπεδο 1: Φυσικό Επίπεδο (physical layer)

Στο φυσικό επίπεδο πραγματοποιείται η εκπομπή των bits σε ένα μέσο μεταφοράς (κανάλι επικοινωνίας) και το αντίστροφο δηλαδή η λήψη των bits από ένα μέσο μεταφοράς.

Επίπεδο 2: Επίπεδο Ζεύξης Δεδομένων (data link layer)

Ο κυριότερος σκοπός του επιπέδου αυτού είναι να λαμβάνει τα δεδομένα από το φυσικό επίπεδο και να τα προωθεί στο ανώτερο επίπεδο.

Επίπεδο 3: Επίπεδο Δικτύου (network layer)

Στο επίπεδο αυτό παρέχονται τα στοιχεία για τη δημιουργία, υποστήριξη και τερματισμό συνδέσεων μεταξύ συνδρομητών ενός δικτύου. Η κυριότερη λειτουργία του επιπέδου είναι η δρομολόγηση των μηνυμάτων, η οργάνωσή τους σε πακέτα, η απαρίθμηση και η ταξινόμησή τους.

Επίπεδο 4: Επίπεδο Μεταφοράς (transport layer)

Το επίπεδο μεταφοράς βελτιώνει τις υπηρεσίες των επιπέδων δικτύου και μπορεί να παρέχει αξιόπιστη παράδοση δεδομένων. Το επίπεδο μεταφοράς βασίζεται

στους μηχανισμούς ελέγχου των λαθών των χαμηλότερων επιπέδων για αν εξασφαλίσει την ακεραιότητα των δεδομένων.

Επίπεδο 5: Επίπεδο Συνόδου (session layer)

Το επίπεδο συνόδου χρησιμοποιεί το επίπεδο μεταφοράς για να παρέχει βελτιωμένες υπηρεσίες συνόδου όπως είναι η σύνδεση ενός χρήστη σε ένα κεντρικό σταθμό.

Επίπεδο 6: Επίπεδο Παρουσίασης (presentation layer)

Το επίπεδο παρουσίασης έχει σαν κύριο σκοπό την παράσταση της πληροφορίας από εφαρμογή σε εφαρμογή, καθώς επίσης και με τη δομή των δεδομένων. Συνεπώς πραγματοποιούνται κυρίως οι διαδικασίες κρυπτογράφησης, συμπίεσης δεδομένων, μετασχηματισμούς κωδικών και των διαφόρων μορφών των αρχείων, καθώς και η μετατροπή και προσαρμογή των δεδομένων στα χαρακτηριστικά του συγκεκριμένου τερματικού, ώστε σε τελική ανάλυση αυτά να παρουσιάζονται όπως πρέπει στο χρήστη.

Επίπεδο 7: Επίπεδο Εφαρμογών (application layer)

Στο επίπεδο αυτό είναι το ανώτερο επίπεδο και το επίπεδο το οποίο βρίσκεται πλησιέστερα στο χρήστη. Η μία εφαρμογή είναι σε θέση να συνομιλεί με την άλλη. Επειδή είναι το ψηλότερο επίπεδο, αποτελεί το interface μεταξύ εφαρμογής και των λοιπών επιπέδων του προτύπου. Οι λειτουργίες του επιπέδου αυτού καθορίζονται σε μεγάλο βαθμό από το χρήστη του δικτύου. Επίσης στο επίπεδο αυτό πραγματοποιείται η εξακρίβωση της ταυτότητας των εφαρμογών που θέλουν να επικοινωνήσουν και την επιβεβαίωση της διαθεσιμότητας τους για συνομιλία. Ακόμα πραγματοποιείται η επιβεβαίωση ή ο έλεγχος στο δικαίωμα της συνομιλίας. Επίσης καθορίζει τις αρμοδιότητες. Τέλος καθορίζει τις διαδικασίες για τον έλεγχο της ροής των συνόδων και την αξιοπιστία της πληροφορίας.

4.7.2 Επίπεδα στοίβας Πρωτοκόλλων Διαδικτύου.

Επίπεδο 1: Φυσικό Επίπεδο

Η εργασία του φυσικού επιπέδου είναι να μεταφέρει τα ξεχωριστά bit μέσα στο πλαίσιο, από έναν κόμβο στον επόμενο. Σε αυτό το επίπεδο τα πρωτόκολλα εξαρτώνται από τη ζεύξη καθώς επίσης και από το μέσο μετάδοσης της ζεύξης.

Επίπεδο 2: Επίπεδο Ζεύξης

Για να μετακινηθεί ένα πακέτο, από έναν κόμβο (υπολογιστή η δρομολογητή) στον επόμενο κόμβο μέσα στη διαδρομή, βασίζονται στο επίπεδο ζεύξης. Οι υπηρεσίες που παρέχονται από το επίπεδο ζεύξης εξαρτώνται από τα συγκεκριμένα πρωτόκολλα.

Επίπεδο 3: Επίπεδο Δικτύου

Το συγκεκριμένο επίπεδο είναι υπεύθυνο για την μετακίνηση πακέτων επιπέδου δικτύου, τα οποία τα ονομάζουμε δεδομενογράμματα (datagrams) από έναν υπολογιστή σε έναν άλλο. Το επίπεδο μεταφοράς σε έναν υπολογιστή προέλευσης μεταβιβάζει ένα τμήμα επιπέδου μεταφοράς και μια διεύθυνση προορισμού στο επίπεδο του δικτύου. Στη συνέχεια το επίπεδο δικτύου παρέχει την υπηρεσία παράδοσης του τμήματος στο επίπεδο μεταφοράς του υπολογιστή προορισμού. Στο σημείο αυτό

να αναφέρουμε ότι το επίπεδο αυτό περιλαμβάνει το πρωτόκολλο IP (internet protocol), το οποίο ορίζει τα πεδία μέσα στο δεδομενόγραμμα, καθώς και το πώς τα τερματικά συστήματα και οι δρομολογητές ενεργούν σε αυτά τα πεδία. Υπάρχει μόνο ένα πρωτόκολλο IP και όλα τα συστατικά του δικτύου που υλοποιούν επίπεδο δικτύου πρέπει να εκτελούν το πρωτόκολλο IP. Επίσης παρέχονται στο επίπεδο αυτό και πρωτόκολλα δρομολόγησης, τα οποία καθορίζουν τις διαδρομές που ακολουθούν τα δεδομενογράμματα ανάμεσα στις προελεύσεις και τους προορισμούς.

Επίπεδο 4: Μεταφοράς

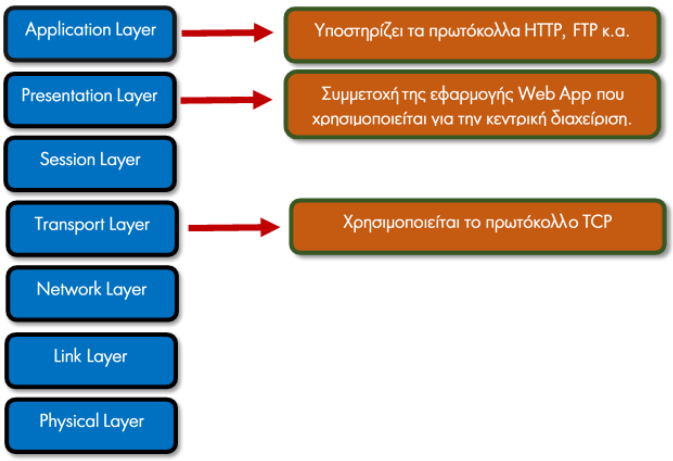
Το επίπεδο αυτό μεταφέρει τα μηνύματα του επιπέδου εφαρμογής ανάμεσα στα άκρα της εφαρμογής. Υπάρχουν δύο πρωτόκολλα μεταφοράς, το TCP και το UDP. Τα δύο αυτά πρωτόκολλα είναι σε θέση να μεταφέρουν μηνύματα επιπέδου εφαρμογής. Το TCP παρέχει μια συνδεσμική υπηρεσία στις εφαρμογές του. Περιλαμβάνει την εγγυημένη παράδοση των μηνυμάτων επιπέδου εφαρμογής στον προορισμό καθώς και τον έλεγχο της ροής, δηλαδή ταίριασμα ταχυτήτων αποστολέα – παραλήπτη. Επίσης το TCP τεμαχίζει τα μεγάλα μηνύματα σε μικρότερα και παρέχει έναν μηχανισμό ελέγχου συμφόρησης, έτσι ώστε μια προέλευση να ρυθμίζει τον ρυθμό μετάδοσης όταν το δίκτυο είναι σε συμφόρηση. Το πρωτόκολλο UDP παρέχει στις εφαρμογές του μια ασυνδεσμική υπηρεσία. Είναι μια απλή υπηρεσία η οποία δεν παρέχει αξιοπιστία, έλεγχο ροής και έλεγχο συμφόρησης.

Επίπεδο 5: Εφαρμογής

Το επίπεδο εφαρμογής είναι το μέρος αυτό όπου βρίσκονται οι δικτυακές εφαρμογές και τα πρωτόκολλα του επιπέδου εφαρμογής. Περιλαμβάνει πολλά πρωτόκολλα, όπως το πρωτόκολλο HTTP (για την υποστήριξη της αίτησης και της μεταφοράς εγγράφων στο Web), το SMTP (για την υποστήριξη μεταφοράς μηνυμάτων ηλεκτρονικού ταχυδρομείου) και το FTP (για υποστήριξη μεταφοράς αρχείων ανάμεσα σε δύο τερματικά συστήματα).

4.7.3 Μοντέλο Αναφοράς DLP

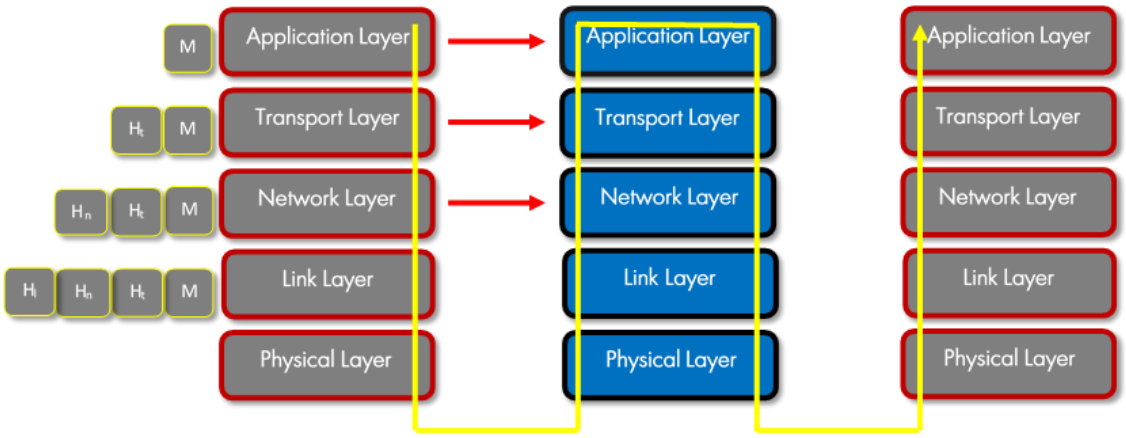
Ένα ενδεικτικό μοντέλο αναφοράς που θα μπορούσαμε να αναφέρουμε ότι δύναται να χρησιμοποιηθεί το DLP, παρουσιάζεται στο παρακάτω σχήμα:



Καθορίζουμε να επιλέξουμε το συγκεκριμένο Μοντέλο Αναφοράς DLP διότι παρατηρώντας τη λειτουργία της εφαρμογής είμαστε σε θέση να διαπιστώσουμε την χρησιμοποίηση ορισμένων πρωτοκόλλων τα οποία ανήκουν στα αντίστοιχα επίπεδα. Συνεπώς το Μοντέλο DLP συμμετέχει με αυτόν τον τρόπο στα συγκεκριμένα επίπεδα.

Εικόνα 11:Μοντέλο Αναφοράς DLP

Από το παραπάνω μοντέλο γίνεται κατανοητό ότι προσαρμόζοντας μια εφαρμογή DLP σε ένα πληροφοριακό σύστημα έχουμε χρησιμοποίηση και αναφορά στα συγκεκριμένα επίπεδα.



Εικόνα 12:Μοντέλο Αναφοράς DLP (2)

4.8 Δομή DLP

Ένα δίκτυο του οργανισμού μπορεί να είναι είτε μεγάλο σε μέγεθος και να περιλαμβάνει πάρα πολλά πληροφοριακά συστήματα είτε μικρό και να περιλαμβάνει λιγότερα σε αριθμό πληροφοριακά συστήματα αλλά της ίδιας αξίας σε λειτουργικό επίπεδο. Ανεξάρτητα του μεγέθους του δικτύου, περιλαμβάνονται ορισμένες υποδομές που απαιτούνται για να λειτουργήσει σωστά. Οι υποδομές του αναφορικά είναι:

α. Σύστημα διαχείρισης δικτύων ή το λειτουργικό σύστημα και
β. Στοιχεία δικτύων τα οποία θέλουμε να διαχειριζόμαστε.

Συγκεκριμένα στα στοιχεία δικτύου αναφερόμαστε στα μηχανήματα αποθήκευσης ή επεξεργασίας πληροφοριών και δεδομένων (H/Y, servers κ.α.) καθώς και τα μηχανήματα διασύνδεσης δικτύων (routers κ.α.). Τα στοιχεία δικτύου θα εκτελέσουν τις διαδικασίες διαχείρισης που ονομάζονται αντιπρόσωποι – agent. Συνεπώς στην συγκεκριμένη περίπτωση τα στοιχεία δικτύου θα εκτελέσουν τις διαδικασίες που απαιτούνται από έναν αντιπρόσωπο – agent της εφαρμογής DLP και συγκεκριμένα της διαδικασίες που ορίζονται από την διαχείρισης της εφαρμογής διαμέσου των αντιπροσώπων και καθορίζονται από τις πολιτικές ασφαλείας.

Αναλύοντας τη δομή λειτουργίας μιας εφαρμογής DLP και σε συνδυασμό και με ότι αναφέρθηκε παραπάνω, είμαστε σε θέση να διακρίνουμε τη συμμετοχή του στα διάφορα επίπεδα μοντέλου αναφοράς OSI ή του μοντέλου TCP/IP. Επίσης ανάλογα των δεδομένων και της κατάστασης της οποίας βρίσκονται υλοποιεί όλη ή μέρος της στοίβας πρωτοκόλλων.

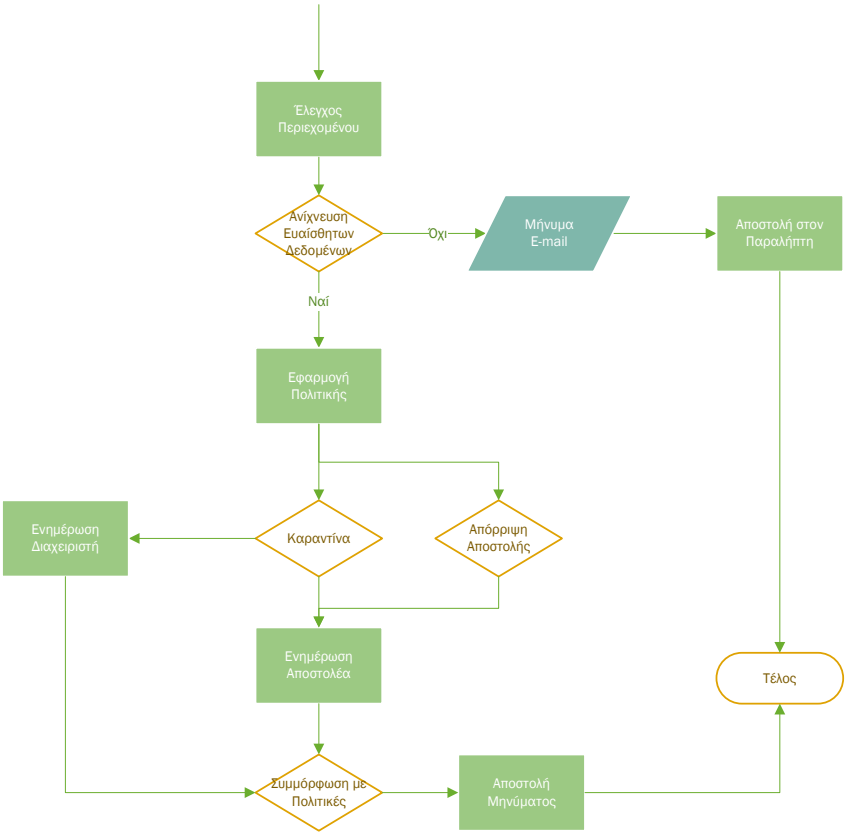
Γνωρίζουμε ότι τα δεδομένα μπορούν να βρίσκονται :

α. Σε κίνηση,
β. Σε αποθήκευση ή
γ. Στους τερματικούς σταθμούς εργασίας.

Κατά συνέπεια εξετάζεται ξεχωριστά κάθε περίπτωση.

4.8.1 Δεδομένα σε Χρήση

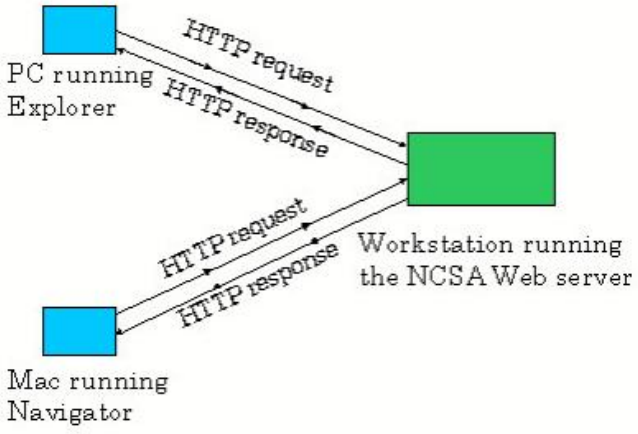
Πραγματοποιώντας την διαδικασία εφαρμογής DLP όταν τα δεδομένα κινούνται διαμέσου δικτύου και προς οποιαδήποτε κατεύθυνση, είτε εντός οργανισμού, είτε εκτός, παρατηρούμε και είμαστε σε θέση να αναλύσουμε την δομή της εφαρμογής ανάλογα με την στρατηγική και τις διαδικασίες που έχουμε αποφασίσει να υλοποιήσουμε. Για την παρακολούθηση της κίνησης των δεδομένων χρησιμοποιούνται συγκεκριμένες συσκευές (hardware) ή ενσωματωμένη τεχνολογία λογισμικού. Τα δεδομένα που βρίσκονται σε κίνηση, υποστηρίζονται από διάφορα πρωτόκολλα όπως είναι για παράδειγμα τα HTTP και FTP. Κατά κύριο λόγο θα εφαρμοστούν στο επίπεδο – στρώμα του λειτουργικού συστήματος. Οπότε χρησιμοποιούνται εξειδικευμένα λογισμικά όπως είναι οι agent και οι crawlers. Επίσης υπάρχει η δυνατότητα να χρησιμοποιηθεί και υλικό hardware το οποίο τοποθετείται κατάλληλα στο δίκτυο και το οποίο βέβαια έχει και αυτό το αντίστοιχο λογισμικό για τη σύλληψη των πακέτων και την ανάλυση του περιεχομένου. Στη συνέχεια αφού συλλάβει τα πακέτα που κινούνται και ανιχνευτεί το περιεχόμενό τους εφαρμόζεται η πολιτική ασφαλείας που έχει επιλεγεί. Στην περίπτωση που υπάρχουν δεδομένα τα οποία εκπίπτουν στις περιπτώσεις τις οποίες έχει επιλέξει η πολιτική εφαρμογής DLP να θεωρήσει ως ευαίσθητα, ενεργοποιείται η εφαρμογή για παράδειγμα της αναμονής, καραντίνας των δεδομένων, της μη αποστολής τους καθώς επίσης και της τελειωτικής απόρριψης της διεργασία, όπως για παράδειγμα η αποστολή e-mail ή η αποθήκευσή τους σε μία συσκευή αποθήκευσης USB Stick.



Εικόνα 13:Ροή DLP-Δεδομένα σε Χρήση

Γνωρίζουμε ότι το Πρωτόκολλο Μεταφοράς Υπερκειμένου HTTP (Hyper Text Transfer Protocol) είναι η καρδιά του Ιστού. Το HTTP ανήκει στο στρώμα εφαρμογών του διαδικτύου και υλοποιείτε ως δύο προγράμματα: ένα πρόγραμμα πελάτη (client program) και ένα πρόγραμμα εξυπηρετητή (server program). Τα δύο αυτά προγράμματα εκτελούνται σε διαφορετικά μηχανήματα επικοινωνώντας μεταξύ τους ανταλλάσσοντας HTTP μηνύματα. Συγκεκριμένα το HTTP ορίζει τη δομή των μηνυμάτων αυτών καθώς και τον τρόπο ανταλλαγής τους ανάμεσα στον πελάτη και στον εξυπηρετητή. Στην συνέχεια πριν την περιγραφή του πρωτόκολλου HTTP πρέπει να αναφερθούμε σε κάποιες βασικές ορολογίες. Γνωρίζουμε ότι μία Ιστοσελίδα (Web page) αποτελείται από αντικείμενα. Με τον όρο αντικείμενο (object) εννοούμε ένα απλό αρχείο, όπως ένα αρχείο HTML, ένα αρχείο εικόνας ή ένα αρχείο βίντεο, το οποίο μπορεί να προσπελαστεί μέσω ενός URL. Τα αντικείμενα αυτά μπορεί να περιέχουν πληροφορίες και δεδομένα τα οποία έχουν θεωρηθεί από τις πολιτικές ασφαλείας ως ευαίσθητα. Οι περισσότερες Ιστοσελίδες αποτελούνται από ένα βασικό αρχείο HTML και διάφορα σχετικά αντικείμενα. Αν υποθέσουμε ότι έχουμε μια Ιστοσελίδα που περιέχει ένα αρχείο HTML και 3 αρχεία εικόνων τότε λέμε ότι η Ιστοσελίδα έχει 4 αντικείμενα. Το βασικό αρχείο HTML αναφέρεται στα άλλα αντικείμενα της σελίδας μέσω των URL των αντικειμένων. Κάθε URL αποτελείται από δύο τμήματα: το όνομα του υπολογιστή – host στον οποίον είναι αποθηκευμένο το αρχείο και το όνομα του μονοπατιού (path) του αντικειμένου.

Π.χ. το URL www.google.gr/index.htm έχει ως όνομα host το www.google.gr και ως όνομα μονοπατιού το index.htm. Ο browser είναι ο αντιπρόσωπος του Ιστού: απεικονίζει στον χρήστη τη ζητούμενη Ιστοσελίδα και παρέχει πληθώρα χαρακτηριστικών πλοήγησης και παραμετροποίησης. Επίσης, στους browser υλοποιείτε και η πλευρά του πελάτη του πρωτοκόλλου HTTP. Ένας εξυπηρετητής Ιστού (Web server) αποθηκεύει τα αντικείμενα της Ιστοσελίδας, το καθένα από τα οποία έχει ως διεύθυνση ένα URL. Στους εξυπηρετητές Ιστού υλοποιείτε και η πλευρά του εξυπηρετητή του πρωτοκόλλου HTTP. Το HTTP ορίζει τον τρόπο με τον οποίο οι πελάτες του Ιστού (π.χ. οι browsers) ζητούν (request) Ιστοσελίδες από τους εξυπηρετητές του Ιστού (π.χ. τους Web servers) και πως οι εξυπηρετητές μεταφέρουν τις Ιστοσελίδες στους πελάτες. Η βασική ιδέα της του πρωτοκόλλου αυτού φαίνεται στο παρακάτω σχήμα.



Όταν ο χρήστης ζητά μια Ιστοσελίδα, ο browser στέλνει ένα μήνυμα HTTP αίτησης (HTTP request), για τα διάφορα αντικείμενα της σελίδας, στον εξυπηρετητή. Ο εξυπηρετητής όταν λάβει το μήνυμα αυτό ανταποκρίνεται με μηνύματα HTTP απόκρισης (HTTP response) στα οποία περιέχονται τα αιτούμενα αντικείμενα.

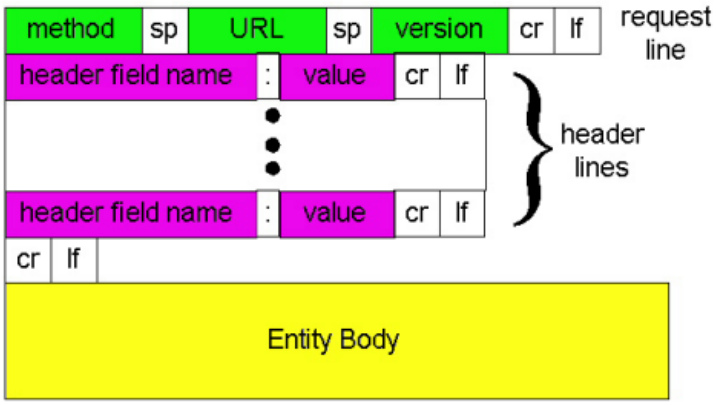
Εικόνα 14:Πρωτόκολλο HTTP

Τόσο το HTTP/1.0 όσο και το HTTP/1.1 χρησιμοποιούν το TCP ως πρωτόκολλο μεταφοράς. Αφού ο πελάτης εγκαταστήσει μια σύνδεση TCP με τον εξυπηρετητή αρχίζει την αποστολή μηνυμάτων – αιτήσεων προς αυτόν και τη λήψη μηνυμάτων– αποκρίσεων από αυτόν. Λόγω της χρήσης του TCP το HTTP δεν χρειάζεται να ασχοληθεί καθόλου με τη μεταφορά των δεδομένων. Το μόνο που πρέπει να κάνει είναι να στείλει τις αιτήσεις μέσω της TCP σύνδεσης και να περιμένει τις αποκρίσεις. Το TCP εγγυάται την αξιόπιστη μεταφορά των δεδομένων καθώς και τον έλεγχο της συμφόρησης. Οι εξυπηρετητές του HTTP δεν κρατάνε καθόλου στοιχεία για την κατάσταση του πελάτη. Επομένως, αν ένας πελάτης στείλει μια αίτηση για ένα αρχείο δύο φορές, ο εξυπηρετητής θα του στείλει το αρχείο αυτό δύο φορές. Τα πρωτόκολλα που δεν κρατάνε καθόλου πληροφορία για την κατάσταση του πελάτη ονομάζονται stateless. Το HTTP ορίζει μόνο δύο τύπους μηνυμάτων: τις HTTP αιτήσεις (requests) και τις HTTP αποκρίσεις (responses).

```
     GET /lessons/index.htm HTTP/1.1
Connection: close
User-agent: Mozilla/15.0
Accept: text/html, image/gif, image/jpeg
Accept-language:gr
```

Όπως φαίνεται και από το παραπάνω παράδειγμα οι HTTP αιτήσεις γράφονται με χαρακτήρες ASCII και μπορούν να διαβαστούν από τους ανθρώπους. Οι περισσότερες HTTP αιτήσεις αποτελούνται από 5 γραμμές κειμένου ακολουθούμενες από μια κενή γραμμή. Οι HTTP αιτήσεις περιέχουν τουλάχιστον μια γραμμή κειμένου, ενώ υπάρχουν και περιπτώσεις που αποτελούνται και από περισσότερες από 5 γραμμές κειμένου. Η πρώτη γραμμή κειμένου ονομάζεται γραμμή αίτησης (request line), ενώ οι επόμενες γραμμές επικεφαλίδας (header lines).
Η γραμμή αίτησης περιέχει τρία πεδία: το πεδίο μεθόδου, το πεδίο URL και το πεδίο HTTP έκδοσης. Το πεδίο μεθόδου μπορεί να έχει μια από τις ακόλουθες τιμές: GET, POST και HEAD. Η πιο συνηθισμένη μέθοδος στις HTTP αιτήσεις είναι η GET, με την οποία ζητείται από τον εξυπηρετητή η αποστολή του αρχείου που εμφανίζεται στο πεδίο URL. Στο URL δεν είναι απαραίτητο να υπάρχει και το όνομα του host, αφού ήδη έχει εγκατασταθεί μια σύνδεση με τον host αυτό (δηλαδή τον HTTP εξυπηρετητή). Τέλος, στο πεδίο έκδοσης HTTP περιγράφεται η έκδοση του HTTP που χρησιμοποιεί ο αιτών host. Στο παραπάνω παράδειγμα χρησιμοποιείται το HTTP/1.1. Στη συνέχεια θα εξετάσουμε τις γραμμές επικεφαλίδας του παραπάνω παραδείγματος. Η γραμμή Connection: close λέει στον εξυπηρετητή να τερματιστεί η σύνδεση μετά την αποστολή του αρχείου, δηλαδή να μην γίνει χρήση μόνιμης σύνδεσης. Η επόμενη γραμμή που αρχίζει με User-agent: δηλώνει τον τύπο του browser του χρήστη. Στο παραπάνω παράδειγμα δηλώνεται ότι ο χρήστης χρησιμοποιεί τον browser Mozilla/4.0. Η γραμμή αυτή χρησιμοποιείται από τον εξυπηρετητή για την αποστολή διαφορετικών αντικειμένων ανάλογα με τον browser του χρήστη (τα οποία όμως έχουν το ίδιο URL). Η Accept: γραμμή δηλώνει τον τύπο των αντικειμένων που υποστηρίζει ο browser. Στο παραπάνω παράδειγμα δηλώνεται ότι ο browser υποστηρίζει αρχεία HTML και αρχεία εικόνων τύπου GIF και JPEG. Τέλος, η Accept-language: γραμμή

δηλώνει την γλώσσα έκδοσης του αντικειμένου που επιθυμεί να λάβει ο browser. Αν ο εξυπηρετητής δεν έχει έκδοση του αντικειμένου για την γλώσσα αυτή τότε στέλνει την προκαθορισμένη έκδοση του αντικειμένου. Στο παραπάνω παράδειγμα αν ο εξυπηρετητής διαθέτει μια ελληνική έκδοση του αρχείου lessons/index.htm τότε πρέπει να τη στείλει, αλλιώς να στείλει την προκαθορισμένη έκδοση του αρχείου. Η δομή του μηνύματος HTTP αίτησης φαίνεται στο παρακάτω σχήμα.



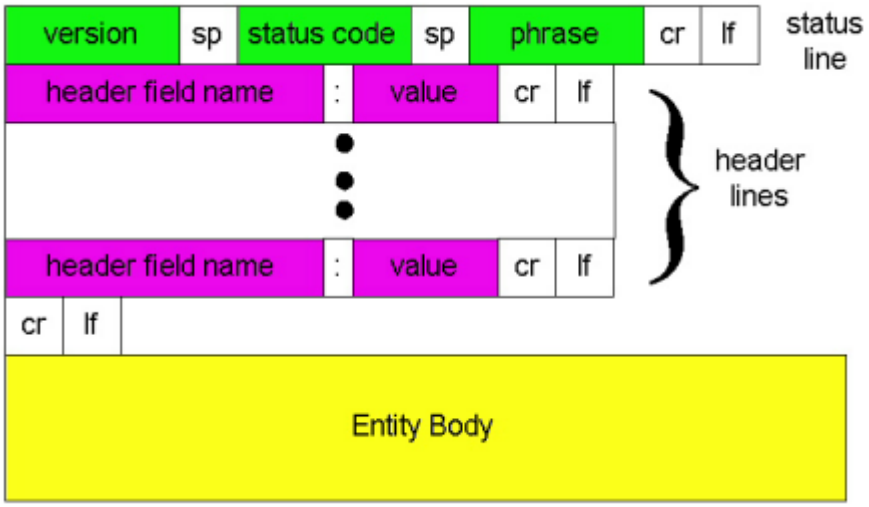
Εικόνα 15:Μήνυμα HTTP αίτησης

Από το παραπάνω σχήμα βλέπουμε ότι η γενική μορφή του μηνύματος ακολουθεί τη δομή του παραπάνω παραδείγματος. Το πεδίο Entity Body δεν χρησιμοποιείται για τη μέθοδο GET, χρησιμοποιείται όμως όταν γίνεται χρήση της μεθόδου POST. Ένα παράδειγμα χρήσης της μεθόδου POST είναι η αποστολή των δεδομένων που συμπλήρωσε ο χρήστης σε διάφορες φόρμες μιας Ιστοσελίδας. Στην περίπτωση αυτή τα δεδομένα αποστέλλονται στο πεδίο Entity Body και ανάλογα με τα δεδομένα αυτά ο χρήστης λαμβάνει μια κατάλληλη έκδοση της Ιστοσελίδας. Παρόμοια χρήση του πεδίου Entity Body γίνεται και στην περίπτωση χρήσης της μεθόδου HEAD. Η μέθοδος αυτή είναι χρήσιμη στον εντοπισμό σφαλμάτων (debugging) από τους developers των εξυπηρετητών Ιστού: όταν ο εξυπηρετητής λάβει αίτηση με χρήση της μεθόδου HEAD αποκρίνεται με ένα HTTP μήνυμα στο οποίο δεν περιλαμβάνεται το αρχείο. Παρακάτω φαίνεται ένα παράδειγμα μηνύματος HTTP απόκρισης.

```
     HTTP/1.1 200 OK
Connection: close
Date: Fri, 18 Nov 2016 23:00:12 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 7 Nov 2016 12:14:22 GMT
Content-Length: 6821
Content-Type: text/html
     data data data data
```

Το HTTP μήνυμα απόκρισης αποτελείται από τρία μέρη: την γραμμή κατάστασης (status line), τις γραμμές επικεφαλίδας (header lines) και το τμήμα περιεχομένου (entity body). Το τμήμα περιεχομένου περιέχει τα δεδομένα του αιτούμενου αρχείου, τα οποία στο παραπάνω παράδειγμα φαίνονται ως data data data data data data ... Η γραμμή κατάστασης περιέχει τρία πεδία: το πεδίο HTTP έκδοσης, το πεδίο κω-

δικού κατάστασης και το πεδίο του αντίστοιχου μηνύματος κατάστασης. Στο παραπάνω παράδειγμα δηλώνεται ότι γίνεται χρήση του HTTP/1.1 και ότι δεν παρουσιάστηκε κάποιο σφάλμα (κωδικός κατάστασης 200 και αντίστοιχο μήνυμα κατάστασης OK). Στο παραπάνω παράδειγμα περιλαμβάνονται έξι γραμμές επικεφαλίδας. Η γραμμή Connection: close δηλώνει ότι μετά την αποστολή του μηνύματος αυτού η TCP σύνδεση θα τερματιστεί. Η Date: γραμμή δηλώνει την ημερομηνία και την ώρα κατά την οποία δημιουργήθηκε και στάλθηκε η απόκριση, η Server: γραμμή δηλώνει τον τύπο του εξυπηρετητή Ιστού, η Last-Modified: δηλώνει την ημερομηνία και την ώρα κατά την οποία το αντικείμενο δημιουργήθηκε ή τροποποιήθηκε για τελευταία φορά, η γραμμή Content-Length: δηλώνει το μήκος των δεδομένων που αποστέλλονται (σε bytes), ενώ η γραμμή Content-Type: δηλώνει τον τύπο του αντικειμένου που περιέχεται στο τμήμα περιεχομένου του μηνύματος. Στο παραπάνω παράδειγμα δηλώνεται ότι χρησιμοποιείται ο Apache/1.3.0 (Unix) εξυπηρετητής Ιστού και ότι αποστέλλεται ένα αρχείο HTML μήκους 6821 bytes. Σε περίπτωση που ο browser χρησιμοποιεί το HTTP/1.0 ακόμη και αν ο εξυπηρετητής Ιστού υποστηρίζει το HTTP/1.1, ο εξυπηρετητής Ιστού πρέπει να χρησιμοποιήσει μη μόνιμες συνδέσεις (δηλαδή στην απόκριση πρέπει να στείλει τη γραμμή Connection: close).
Η δομή των HTTP μηνυμάτων απόκρισης φαίνεται στο παρακάτω σχήμα.



Εικόνα 16:Δομή HTTP μηνύματος απόκρισης

4.8.2 Δεδομένα σε Αποθήκευση

Για να ανιχνευθούν δεδομένα σε βάσεις δεδομένων ή σε χώρους αποθήκευσης πραγματοποιείται σάρωση με την χρησιμοποίηση ιχνηλατών (crawlers) το οποίο υλοποιεί το πρωτόκολλο επιπέδου εφαρμογής. Ο ιχνηλάτης στέλνεται μαζί με τον πράκτορα και πραγματοποιεί την συγκέντρωση των στοιχείων που έχουμε ορίζει ως ευαίσθητα δεδομένα. Ο πράκτορας εφοδιάζεται με τις πολιτικές δεδομένων που καθορίζουν ποια είναι τα ευαίσθητα δεδομένα. Διαβάζει τα πρώτα δεδομένα και στην συνέχεια τα εμφανίζει μέσω της εφαρμογής στον χειριστή. Μετά τις ενέργειες του χειριστή είτε θα τερματίσει είτε θα συνεχίσει την διεργασία της αναζήτησης.

4.8.3 Στοιχεία που απαιτούνται

Τα στοιχεία που απαιτούνται να έχει μία εφαρμογή DLP για να είναι σωστή η διαχείρισή της είναι:

α. Μία κονσόλα μέσω της οποίας θα χειριζόμαστε την εφαρμογή διαχείρισης DLP. Δηλαδή ένας σταθμός εργασίας όπου θα βρίσκεται ο διαχειριστής και υπεύθυνος για την DLP και θα πραγματοποιεί τις απαραίτητες εργασίες.

β. Διάφορα πρωτόκολλα διαχείρισης DLP. Συμμετοχή της εφαρμογής στα διάφορα επίπεδα των μοντέλων αναφοράς OSI και TCP. Επίσης αναφερόμαστε στον τρόπο με τον οποίο τα πραγματοποιείται η επικοινωνία με τις συσκευές που θα διαχειρίζεται.

γ. Πράκτορας διαχείρισης της εφαρμογής DLP. Αναφερόμαστε στο λογισμικό το οποίο εγκαθίσταται στις συσκευές που υπάρχουν στο δίκτυο του οργανισμού και πραγματοποιούν την χρήση των πρωτοκόλλων της διαχείρισης της εφαρμογής DLP.

δ. Δικτυακές συσκευές. Εννοούμε τις συσκευές router, switches, servers κ.α.

4.8.4 Ενδεικτικό Μοντέλο Διαχείρισης DLP

Θα μπορούμε να αναφέρουμε στο συγκεκριμένο σημείο μια ενδεικτική διαχείριση που πραγματοποιείται κατά την λειτουργία της εφαρμογής DLP, το οποίο αυτοματοποιεί την προστασία από την ακούσια ή εκούσια διαρροή δεομένων και πληροφοριών. Επομένως το σύνολο των λειτουργιών, των ενεργειών και των διαδικασιών καθώς και της εφαρμογής DLP θα αποτελέσει το μοντέλο ώστε να λειτουργεί το δίκτυο με σωστό τρόπο, καθώς και να πραγματοποιείται η διακίνηση των πληροφοριών και η αποθήκευσή τους με τον κατάλληλο τρόπο.

α. Διαχείριση της εφαρμογής DLP. Θα πραγματοποιηθεί η εγκατάσταση του προγράμματος σε κάποιον υπολογιστή του οργανισμού ο οποίος έχει πρόσβαση στο δίκτυο. Αυτόν τον υπολογιστή είναι προφανές ότι θα τη-ον χρησιμοποιεί ο διαχειριστής του δικτύου ή αν υπάρχει η δυνατότητα αναλόγως του μεγέθους του οργανισμού ο διαχειριστής της εφαρμογής DLP.

β. Τα στοιχεία δικτύου που θα διαχειριζόμαστε. Αναφερόμαστε στις δικτυακές συσκευές.

γ. Τους αντιπροσώπου – agent. Όπως αναφέρθηκε είναι τα προγράμματα σε κάθε στοιχείο που υπάρχει στο δίκτυο και καθιστά εφικτή την επικοινωνία με τον διαχειριστή της εφαρμογής.

4.8.5 Ενδεικτική Διαδικασία εφαρμογής DLP

α. Ο Διαχειριστής είναι σε θέση και στέλνει τις κατάλληλες εντολές εφαρμόζοντας τις πολιτικές ασφαλείας καθώς και ελέγχου με την βοήθεια των πρωτοκόλλων επικοινωνίας.

β. Οι αντιπρόσωποι λαμβάνουν τις εντολές αυτές.

γ. Οι αντιπρόσωποι στην συνέχεια θα εκτελέσουν τις εντολές αυτές στα διαχειριζόμενα στοιχεία δικτύου που ελέγχουν.

Κεφάλαιο 5 : Εφαρμογές DLP – OpenDLP και MyDLP

5.1 Εισαγωγή

Ιδιαίτερα σημαντικό θεωρείται στο σημείο αυτό να αναφερθούμε ενδεικτικά σε δύο εφαρμογές – εργαλεία που έχουν δημιουργηθεί και κυκλοφορούν στο διαδίκτυο. Το OpenDLP το οποίο είναι ελεύθερο και ανοικτό λογισμικό και το MyDLP. Η έκδοση MyDLP Enterprise δεν διατίθεται δωρεάν αλλά σε δοκιμαστική έκδοση 30 ημερών, πέρα των οποίων πρέπει να πραγματοποιηθεί η ανάλογη αγορά.

5.2 Το OpenDLP

Αρχικά θα αναφερθούμε στο OpenDLP. Αναπτύχθηκε το 2009 από το Andrew Gavin σαν ελεύθερο και ανοικτό λογισμικό προστασίας απώλειας δεδομένων, το οποίο ακολουθεί τις προδιαγραφές GPLv3 (GNU General Public License, version 3). Η συγκεκριμένη εφαρμογή αναπτύχθηκε να έχει τη δυνατότητα να ανιχνεύει τα δεδομένα σε αποθήκευση (Data at Rest) και είναι σε θέση να λειτουργήσει με ή χωρίς πράκτορα. Παρατηρώντας την εφαρμογή είμαστε σε θέση να διαπιστώσουμε ότι αποτελείται από έναν πράκτορα, το οποίο έχει σχεδιαστεί για λειτουργικό λογισμικό Windows και μια δικτυακή εφαρμογή, η οποία στηρίζεται σε LAMP (Linux, Apache, MySQL, PHP/Perl/Python). Επίσης αξίζει να αναφερθεί ότι είναι πολύ χρήσιμη η δυνατότητα που δίνεται για εγκατάσταση του προγράμματος σε εικονική μηχανή (VM – Virtual Machine).

Ένας από τους λόγους για τους οποίους γράφτηκε είναι ότι μέχρι εκείνη τη στιγμή δεν υπήρχαν προγράμματα και εφαρμογές τα οποία θα πραγματοποιούσαν αυτόματα τη σάρωση. Αν και υπήρχαν εφαρμογές ελεύθερου και ανοικτού λογισμικού όπως ήταν το Cornell Spider, το FindSSN (Sourceforge), το Grep (Global Regular Expression Print), μπορούσαν να παραβιαστούν μέσω network shares από την στιγμή που δεν χρησιμοποιούσαν πράκτορα, αλλά ήταν χειροκίνητη η σάρωση. Τέλος δεν ήταν επαρκές για μεγάλες επιχειρήσεις, καθώς μπορούσαν να αναπτυχθούν μόνο σε έναν μεμονωμένο σταθμό εργασίας. Το συγκεκριμένο λογισμικό μπορεί να χρησιμοποιηθεί από το προσωπικό του οργανισμού που είναι επιφορτισμένο με τον έλεγχο της τήρησης των εντολών της διοίκησης, τους διαχειριστές δικτύου, και τους penetration testers.

5.2.1 Πώς Λειτουργεί το OpenDLP

Για να γίνει αντιληπτό πώς λειτουργεί θα απαιτηθεί να δημιουργήσουμε μία πολιτική ασφαλείας. Στη συνέχεια πραγματοποιείται η αυθεντικοποίηση των διαπιστευτηρίων του διαχειριστή. Στο σημείο αυτό μπορούμε να αναφέρουμε ότι είναι δυνατόν να χρησιμοποιηθεί αντί για τον κωδικό (password) και η τεχνική pass-the-hash στην περίπτωση που δεν είναι γνωστός ο κωδικός στο σύστημα που θέλουμε να εισέλθουμε. Επίσης βάση της πολιτικής η οποία είναι επαναχρησιμοποιούμενη γίνεται η καθοδήγηση του πράκτορα. Στη συνέχεια είμαστε σε θέση να επιλέξουμε πόσο επί

της εκατό της μνήμης RAM θα χρησιμοποιήσει ο πράκτορας – agent, καθώς επίσης και το είδος των αρχείων που θέλουμε να προστατεύσουμε. Στην περίπτωση που δεν μας καλύπτουν οι πολιτικές που ήδη υπάρχουν στην εφαρμογή μας δίνεται η δυνατότητα να δημιουργήσουμε δικές μας μέσω κανονιστικών εκφράσεων (PCREs). Όπου θα ορίσουμε συγκεκριμένο περιεχόμενο αρχείων όπως είναι οι αριθμοί πιστωτικών καρτών ή μορφές αρχείων όπως είναι για παράδειγμα .jpeg. Τέλος προγραμματίζουμε πόσο συχνά θα μας αναφέρονται τα αποτελέσματα και θα πραγματοποιούνται οι σαρώσεις.

5.2.2 Ξεκινώντας την λειτουργία

Ξεκινώντας μια σάρωση με αντιπρόσωπο – agent, αναπτύσσεται πάνω στο πρωτόκολλο SMB (Server Message Block). Συνεπώς δημιουργείται μια σχέση ανάμεσα στις συσκευές πελάτη – εξυπηρετητή. Μπορεί να αναπτυχθεί από την λειτουργία μέσω φυλλομετρητή (web application) δίνοντας την δυνατότητα για την παρακολούθηση 1000 συστημάτων συνολικά, ενώ μπορεί ταυτόχρονα να σαρώνει 30 συστήματα. Καταλήγουμε με αυτόν τον τρόπο στο συμπέρασμα ότι μπορούν να διατεθούν μέχρι 1000 πράκτορες και μέχρι 30 πράκτορες ταυτόχρονα.

5.2.3 Πράκτορας σε λειτουργικό σύστημα Windows.

Την στιγμή που εκτελείται η σάρωση σε ένα τερματικό σύστημα που έχει επιλεγεί, δημιουργείται ένας φάκελος αρχείου και στη συνέχεια εκτελείται η ενέργεια σαν υπηρεσία με χαμηλή προτεραιότητα για την CPU και η οποία καταναλώνει όση μνήμη έχει επιλεγεί από την πολιτική. Αυτό έχει σαν αποτέλεσμα να μην ανιχνεύεται από τα anti-virus που ενδεχομένως υπάρχουν εγκατεστημένα στον υπολογιστή. Επιπρόσθετα είμαστε σε θέση να επιλέξουμε διαφορετικό όνομα στην υπηρεσία που θα εκτελεστεί το οποίο ο χειριστής του τερματικού δεν θα είναι σε θέση να αντιληφθεί ακόμα και στην περίπτωση που πραγματοποιήσει έλεγχο με την βοήθεια της διαχείρισης εργασιών.

Κατά την διάρκεια της σάρωσης πραγματοποιεί έρευνα σε «λευκές/μαύρες» λίστες στους φακέλους – αρχεία καθώς και στους καταλόγους. Ανιχνεύει και ψάχνει για να εντοπίσει φακέλους – αρχεία τα οποία βάση της πολιτικής εκπίπτουν στις κανονιστικές εκφράσεις. Δηλαδή αρχεία τα οποία μπορεί για παράδειγμα να περιέχουν αριθμούς πιστωτικών καρτών ή ακόμα και ορισμένους τύπους αρχείων. Κατόπιν προωθούνται τυχόν ευρέσεις δια μέσου της web εφαρμογής ανά τακτά χρονικά διαστήματα τα οποία τα έχουμε ορίσει εμείς. Όταν πραγματοποιείται η σάρωση ο αντιπρόσωπος στην συνέχεια ζητάει μέσω της web εφαρμογής να εκτελέσει την απεγκατάστασή του και να διαγραφεί. Αυτό σημαίνει ότι θα διαγραφεί αυτόματα και ο κατάλογος που είχε δημιουργηθεί έτσι ώστε να μην παραμείνουν ίχνη. Όπως γίνεται αντιληπτό ιδιαίτερα σημαντικό είναι ο χειριστής της εφαρμογής να μην πραγματοποιήσει εγκατάσταση σε ήδη υπάρχοντα φάκελο, αλλά σε κάποιον καινούργιο γιατί με την αίτηση της απεγκατάστασης θα διαγραφεί όλος ο φάκελος και ότι άλλο περιέχει

μέσα. Εύκολα γίνεται αντιληπτό ότι το σημείο όπου βρίσκεται ο φάκελος είναι η μοναδική απόδειξη ότι υπάρχει αντιπρόσωπος – agent στο τερματικό σύστημα. Στο σημείο αυτό να αναφερθεί ότι ο πράκτορας έχει συγγραφή σε γλώσσα προγραμματισμού C χωρίς να απαιτείται .NET.

5.2.4. Παρακολούθηση πράκτορα μέσω της εφαρμογής web.

Η εφαρμογή web λαμβάνει με ασφαλή τρόπο σε χρονικά διαστήματα που έχουμε επιλέξει τα αποτελέσματα της σάρωσης από τους αντιπροσώπου – agents τα οποία αφορούν:

α. την τρέχουσα κατάσταση του αντιπροσώπου. Δηλαδή εάν βρίσκεται σε σάρωση καταλόγου, παρακολούθηση κλπ.

β. το πλήθος των αρχείων καθώς και των bites που έχει σαρώσει.

γ. ο χρόνος που απομένει για να ολοκληρώσει την εργασία του.

Στο σημείο αυτό να αναφέρουμε ότι οι μεταφορές που πραγματοποιούνται από τους αντιπροσώπους – agent είναι βασισμένες στο πρωτόκολλο SSL (Secure Sockets Layer) το οποίο εξασφαλίζει την ασφάλεια των δεδομένων. Κατά συνέπεια ακόμα και αν εφαρμοστεί η επίθεση από κάποιον man – in – the middle δεν θα έχει επιτυχή έκβαση.

5.2.5. Εμφάνιση αποτελεσμάτων μέσω της Web εφαρμογής.

Η εφαρμογή μας δίνει την δυνατότητα να εμφανίσουμε τα συνολικά αποτελέσματα. Στη συνέχεια μας δίνεται η δυνατότητα να ελέγξουμε μέσω στης εφαρμογής το εκτιμώμενο χρόνο κάθε σάρωσης, να ανακαλύψουμε συγκεκριμένα δεδομένα χρησιμοποιώντας το όνομά τους ή το μέγεθός τους. Τέλος έχουμε την δυνατότητα να διαγράψουμε δεδομένα ή να τα μετακινήσουμε σε διαφορετικό μέρος, τα οποίο πληρεί της απαιτήσεις ασφαλείας. Επίσης μπορούμε να σταματήσουμε την σάρωση ή να απεγκαταστήσουμε τον πράκτορα όποτε το επιθυμούμε. Στην περίπτωση που διακόψουμε για τον οποιοδήποτε λόγο την σάρωση μας δίνεται η δυνατότητα να την συνεχίσουμε από το σημείο που σταματήσαμε. Η διακοπή μπορεί να πραγματοποιηθεί είτε από εμάς είτε να πραγματοποιηθεί από τον χειριστή του τερματικού σταθμού. Όταν εισέλθει στον υπολογιστή του ξανά, ο πράκτορας θα συνεχίσει την σάρωση από το σημείο που σταμάτησε. Στην περίπτωση που έχει διακοπεί η εφαρμογή αλλά συνεχίσει ο αντιπρόσωπος – agent την λειτουργία του, θα αποστείλει τα δεδομένα μαζικά όταν εισέλθει ο χειριστής της εφαρμογής.

5.2.6. Λειτουργία χωρίς την χρησιμοποίηση Αντιπροσώπου – agent

Η εφαρμογή OpenDLP μπορεί να χρησιμοποιηθεί και χωρίς την παρουσία αντιπροσώπου – agent. Υπάρχει η δυνατότητα να εφαρμοστεί σε όλα τα λειτουργικά συστήματα είτε αυτά στηρίζονται σε UNIX είτε σε windows.

Η λειτουργία της Web εφαρμογής όταν δεν χρησιμοποιείται αντιπρόσωπος είναι η ίδια με την λειτουργία όταν χρησιμοποιείται αντιπρόσωπος. Συνεπώς απαιτείται η δημιουργία επαναχρησιμοποιούμενης πολιτικής σύμφωνα με την οποία θα επιλέξουμε τις ενέργειες που επιθυμούμε να πραγματοποιηθούν. Ακόμα ορίζονται οι «μαύρες/λευκές» λίστες καταλόγων καθώς και οι επεκτάσεις αρχείων που θέλουμε, επίσης το μέγιστο της μνήμης που θα χρησιμοποιηθεί καθώς και οι κανονιστικές εκφράσεις που θα χρησιμοποιήσουμε όπως είναι για παράδειγμα οι αριθμοί πιστωτικών καρτών. Στο σημείο αυτό να επισημάνουμε ότι θα ήταν χρήσιμο να διαθέτουμε τα διαπιστευτήρια για κάθε λειτουργικό σύστημα αλλά όχι και απαραίτητο. Επιπροσθέτως να αναφερθεί ότι σε συστήματα οποία βασίζονται σε UNIX αρκεί μόνο η διεύθυνση IP του τερματικού συστήματος που θέλουμε να σαρώσουμε, συνεπώς είναι της μορφής 192.168.1.20, ενώ για συστήματα τα οποία βασίζονται σε λειτουργικό windows χρειάζεται να δοθεί ολόκληρη η διαδρομή, δηλαδή \\192.168.1.20 \OpenDLP. Επιπλέον στην περίπτωση που χρειαζόμαστε να κατευθύνουμε την σάρωση σε πιο συγκεκριμένο σημείο, χρειάζεται να συμπληρώσουμε την ακριβή διαδρομή. Για παράδειγμα \\192.168.1.20\OpenDLP\Documents. Επίσης μπορεί να ρυθμιστεί το μέγιστο όριο της μνήμης που θα χρησιμοποιηθεί. Η συγκεκριμένη ρύθμιση όμως αφορά την μνήμη του υπολογιστή που χρησιμοποιείται από τον χειριστή της εφαρμογής OpenDLP. Αυτό οφείλεται στο γεγονός ότι κατά την λειτουργία σάρωσης με την απουσία πράκτορα – agent πραγματοποιείται μεταφόρτωση όλων των αρχείων στον τερματικό σταθμό στον οποίο θα πραγματοποιηθεί η σάρωση. Υπάρχει όμως και η περίπτωση κατά την διάρκεια της σάρωσης να απαιτηθεί η χρησιμοποίηση περισσότερης μνήμης από αυτή που έχουμε ήδη ορίσει, οπότε πραγματοποιείται τεμαχισμός των δεδομένων σε μικρότερα τμήματα και αποστολή τους στον χειριστή τμηματικά.

Από την στιγμή που δεν χρησιμοποιούμε πράκτορας – agent χρειάζεται ένα σενάριο φλοιού (shell script) για να εκτελεστούν όλα όσα έχουν προαναφερθεί. Το συγκεκριμένο είναι γραμμένο στην αντικειμενοστραφή προγραμματιστική γλώσσα Perl.

5.2.7 Ξεκινώντας την Σάρωση χωρίς Πράκτορα – agent.

Όταν θα ξεκινήσει να εκτελείται η σάρωση θεωρητικά ο αριθμός των συστημάτων που υπάρχει η δυνατότητα τα σαρωθεί είναι απεριόριστο. Παρόλα αυτά όμως εξαιτίας του γεγονότος ότι χρησιμοποιούνται οι πόροι και οι δυνατότητες του χρήστη για να ολοκληρωθεί η διαδικασία, η οποία είναι αρκετά χρονοβόρα καθώς επίσης μεταφέρεται μεγάλος όγκος δεδομένων στο υπάρχον δίκτυο, μπορεί να πραγματοποιηθεί σάρωση σε περίπου 23 συστήματα. Μας δίνεται επίσης η δυνατότητα να σταματήσουμε την σάρωση, να την συνεχίσουμε από το σημείο που σταματήσαμε ή να την σταματήσουμε ολοκληρωτικά.

Όταν χρησιμοποιούμε αυτή την επιλογή σάρωσης σε λειτουργικό σύστημα Windows, η διαδικασία βασίζεται και αυτή στο πρωτόκολλο SMB (Server Message Block). Επιπλέον όταν το λειτουργικό σύστημα είναι UNIX τότε η διαδικασία βασίζεται στο πρωτόκολλο SSH (Secure Shell) και συγκεκριμένα χρησιμοποιείται το SSHFS

(SSH Filesystem). Αυτό μας δίνει την δυνατότητα να κρυπτογραφούνται τα δεδομένα και οι πληροφορίες που μεταφέρονται, επομένως με αυτόν τον τρόπο διατίθεται ασφαλή πρόσβαση, μεταφορά και λειτουργικότητα της διαχείρισης της εφαρμογής. Συνεπώς, στην περίπτωση που το δίκτυο δεν είναι ασφαλές, δημιουργείται ένα ασφαλές κανάλι επικοινωνίας ανάμεσα στα δύο συστήματα, το οποίο κρυπτογραφεί τις πληροφορίες που μεταφέρονται.

5.2.8 Λειτουργία χωρίς την χρήση Πράκτορα σε Βάσεις Δεδομένων.

Στην περίπτωση που θέλουμε να σαρώσουμε βάσεις δεδομένων χρησιμοποιούμε την επιλογή χωρίς αντιπρόσωπο – agent. Μπορούμε να σαρώσουμε ώστε να ανακαλύψουμε δεδομένα με την εφαρμογή OpenDLP σε διακομιστές βάσεων δεδομένων. Αυτή την στιγμή οι Βάσεις Δεδομένων που μπορεί να υποστηρίξει το OpenDLP είναι οι MySQL και οι Microsoft SQL Server. Αργότερα ίσως συμπεριληφθούν και οι OracleDB και PostgresSQL. Στο σημείο αυτό θα ήταν χρήσιμο να αναφέρουμε ότι για τον Microsoft SQL Server απαιτείται ο χειριστής της εφαρμογής OpenDLP να διαθέτει πρόσβαση στον διακομιστή της βάσεως, είτε με δικαιώματα διαχειριστή της βάση, είτε με τον αντίστοιχο, λογαριασμό του χρήστη Windows με πρόσβαση όμως στο domain στο οποίο ανήκει ο διακομιστής.

Χρησιμοποιούμε και σε αυτή την περίπτωση την web εφαρμογή από την οποία δημιουργούμε την επαναχρησιμοποιούμενη πολιτική που χρειαζόμαστε στον συγκεκριμένο τομέα. Επιλέγουμε επομένως «λευκές/μαύρες» λίστες Βάσεων Δεδομένων, δίνοντας μας την δυνατότητα επιλογής τι αποτελέσματα επιθυμούμε να επιστρέψει η σάρωση. Για παράδειγμα μπορούμε να επιλέξουμε αριθμό πινάκων, στηλών και γραμμών που θέλουμε να μας επιστρέψει. Επίσης μέσω των κανονιστικών εκφράσεων, που μας δίνεται και σε αυτή την περίπτωση η δυνατότητα να χρησιμοποιήσουμε, μπορούμε να επιλέξουμε συγκεκριμένα ονόματα πινάκων, στηλών και γραμμών αλλά και των δεδομένων που περιέχουν αυτά.

5.2.9 Ξεκινώντας την σάρωση Βάσεων Δεδομένων χωρίς Πράκτορα.

Την στιγμή που θα ξεκινήσει η σάρωση για την ανεύρεση ευαίσθητων δεδομένων μας δίνεται η δυνατότητα ταυτόχρονης σάρωσης σε βάσεις δεδομένων. Οι τεχνικές που θα χρησιμοποιήσουμε είναι το SQL Injection, οπότε με αυτόν τον τρόπο εκτελεί εντολές SQL (Queries) σε απομακρυσμένα συστήματα. Σε γενικές γραμμές το συγκεκριμένο exploit βασίζεται σε κάποια φόρμα εισαγωγής δεδομένων η οποία δεν φιλτράρει την εισαγωγή στοιχείων έχοντας ως αποτέλεσμα την εκτέλεση κώδικα είτε με την μορφή SQL , είτε με την μορφή JavaScript. Τέλος μας παρέχει η εφαρμογή την δυνατότητα της παύσης της σάρωσης και στη συνέχεια την επανεκκίνησή της από το σημείο στο οποίο είχε σταματήσει καθώς και την οριστικό τερματισμό της πριν ακόμα ολοκληρώσει την σάρωση.

5.3. Το MyDLP

Το MyDLP είναι ένα πρόγραμμα ανοικτού λογισμικού κώδικα το οποίο χρησιμοποιείται για την πρόληψη απώλειας δεδομένων. Η ανάπτυξη του ξεκίνησε το 2010 και έχει πραγματοποιηθεί κάτω από την άδεια GNU. Είναι από τα πρώτα λογισμικά που αναπτύχθηκαν για το σκοπό αυτό. Η εφαρμογή δίνει την δυνατότητα να εγκατασταθεί σε εξυπηρετητές (server) καθώς και σε τερματικούς σταθμούς εργασίας. Υποστηρίζει διάφορα κανάλια και τρόπους επικοινωνίας συμπεριλαμβανομένου του διαδικτύου (Web), του ηλεκτρονικού ταχυδρομείου (e-mail), του im, του FTP, ενώ δίνει την δυνατότητα να ασφαλίσει αποσπώμενες συσκευές αποθήκευσης (USB Stick) και εκτυπωτές.

Το Μάϊο του 2014 η εταιρία ανάπτυξης λογισμικών ασφαλείας Comodo με έδρα τις Η.Π.Α., απέκτησε το λογισμικό MyDLP. Η συγκεκριμένη εταιρία έχει αναπτύξει και άλλα λογισμικά όπως είναι τα anti-virus, firewall κ.ά. Στη συνέχεια η Comodo ξεκίνησε την δημιουργία έκδοσης Enterprise, η οποία είναι επί πληρωμή και όχι δωρεάν όπως η αρχική. Τέλος η Comodo δεν έχει πραγματοποιήσει καμία ανακοίνωση σε ότι αφορά το project ανάπτυξης του ανοικτού κώδικα.

Η εφαρμογή MyDLP από την στιγμή που ξεκίνησε να αναπτύσσεται περιλάμβανε τα παρακάτω υποέργα:

DLP Network: Ο εξυπηρετητής του δικτύου της εφαρμογής, ο οποίος χρησιμοποιείται για δίκτυα με υψηλή λειτουργική δραστηριότητα και μεγάλο φορτίο μεταφοράς, όπως είναι οι συνδέσεις TCP και οι υπηρεσίες φιλοξενίας του δικτύου MyDLP. Έχει γραφτεί στο περισσότερο μέρος της σε γλώσσα Erlang λόγω της απόδοσης που παρέχει σε ταυτόχρονες λειτουργίες δικτύου. Επίσης σε ορισμένες εξαιρετικές περιπτώσεις χρησιμοποιείται και η γλώσσα Python. Θα μπορούσε συνεπώς να λειτουργήσει σε οποιαδήποτε πλατφόρμα χρησιμοποιεί Erlang ή Python.

DLP Endpoint: Ο απομακρυσμένος πράκτορας – agent του προγράμματος ο οποίος εκτελείται στους τερματικούς σταθμούς με σκοπό να επιθεωρήσει τις λειτουργίες ενός τερματικού χειριστή όπως είναι η αντιγραφή αρχείων σε μία εξωτερική συσκευή, η εκτύπωση ενός εγγράφου καθώς και λήψη ενός στιγμιότυπου οθόνης (screen shots). Έχει γραφτεί για windows λογισμικό και είναι γραμμένο σε γλώσσα C++, C#.

DLP Web UI: Είναι η διεπαφή της διαχείριση του συστήματος για να διαμορφώσει το MyDLP. Προωθεί συγκεκριμένα τμήματα της διαμόρφωσης του συστήματος και στα δύο τμήματα, στο Network και στο Endpoint. Είναι γραμμένη σε γλώσσα PHP και Adobe Flex. Επίσης χρησιμοποιεί τη MySQL για την αποθήκευση των ρυθμίσεων των διαχειριστών και χρηστών.

Η έκδοση MyDLP Enterprise είναι μια έκδοση η οποία διαθέτει πολλά χαρακτηριστικά. Θεωρείται επεκτάσιμη και προσιτή, είναι μια λύση όλα-σε-ένα σε ότι αφορά την πρόληψη διαρροής δεδομένων με απίστευτα γρήγορη απόδοση.

Έχοντας αντιληφθεί το γεγονός ότι σχεδόν όλες οι απαραίτητες εφαρμογές γραφείου και συσκευών είναι πιθανές πηγές διαρροής δεδομένων, έχει καταβληθεί

προσπάθεια έτσι ώστε να επιτευχθεί η ασφάλεια των πληροφοριών χωρίς να παρεμποδίζουν την απόδοση. Από τη μία πλευρά οι περιοριστικές πολιτικές στο web, e-mail, στις αφαιρούμενες συσκευές αποθήκευσης (USB), στα έξυπνα τηλέφωνα (smartphones), στους εκτυπωτές, στους φορητούς υπολογιστές αφαιρεί σχεδόν όλα τα πλεονεκτήματα του σημερινού ενοποιημένου περιβάλλοντος γραφείου. Από την άλλη πλευρά, οι απαιτήσεις συμμόρφωσης, οι κίνδυνοι που υπάρχουν, τα πραγματικά περιστατικά που έχουν συμβεί, δημιουργούν καθημερινά πίεση στους IT διαχειριστές.

Η εφαρμογή MyDLP επιτρέπει την παρακολούθηση, την επιθεώρηση και την αποτροπή όλων των εξερχόμενων εμπιστευτικών δεδομένων χωρίς ιδιαίτερη ταλαιπωρία. Με εύκολη ανάπτυξη και διαμόρφωση, εύκολη στη χρήση διεπαφή (interface) πολιτικών και μεγάλη απόδοση οι IT διαχειριστές και οι υπεύθυνοι της ασφάλειας είναι σε θέση να αποτρέψουν τη διαρροή δεδομένων.

Η εφαρμογή έχει την δυνατότητα να εντοπίζει, να παρακολουθεί και να προστατεύει ευαίσθητες πληροφορίες και δεδομένα τα οποία βρίσκονται σε χρήση Data in use" (πχ., σε τερματικούς σταθμούς εργασίας), σε "Data in motion" (πχ, κατά την μεταφορά τους μέσω δικτύου) καθώς και "Data at rest" (πχ, αποθήκευση δεδομένων). Αυτό πραγματοποιείται μέσω της ανάλυσης του περιεχομένου, στα συμφραζόμενα ανάλυσης της ασφαλείας των συναλλαγών (πχ χαρακτηριστικά του εντολέα, αντικείμενο δεδομένων, μέσο επικοινωνίας, χρονοδιάγραμμα, αποδέκτης ή προορισμός κλπ). Έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να ανιχνεύει και να αποτρέπει την μη εξουσιοδοτημένη χρήση και διαβίβαση των εμπιστευτικών πληροφοριών.

Δεν χρειάζονται πολλαπλές άδειες για να χρησιμοποιηθούν τα διάφορα χαρακτηριστικά. Αρκεί μόνο μία αρχική για να χρησιμοποιηθεί η έκδοση DLP Enterprice. Αναπτύσσεται χωρίς ιδιαίτερη προσπάθεια και είναι αρκετά εύκολη στην εφαρμογή της. Από την στιγμή που θα αναπτυχθεί η εφαρμογή και καθοριστούν οι πολιτικές ασφαλείας, μπορεί να προστατεύσει τα δεδομένα μέσα σε λίγα λεπτά.

Η δημιουργία πολιτικών ασφαλείας των ευαίσθητων δεδομένων είναι απλή υπόθεση. Αρκεί ένας απλός εξυπηρετητής για να χρησιμοποιηθούν όλες οι δυνατότητες και τα χαρακτηριστικά. Δεν απαιτεί είτε εικονικά είτε φυσικά μηχανήματα τα οποία θα εκτελούν την εφαρμογή. Μπορεί και από έναν απλό εξυπηρετητή.

5.3.1. Συχνές περιπτώσεις χρήσεων

α. Αποκλεισμός ή απομόνωσης εξερχόμενων εμπιστευτικών δεδομένων από το δίκτυο του οργανισμού μέσω mail και web. Δημιουργία αρχείου καταγραφής με ύποπτα αρχεία.

β. Παρακολούθηση της χρήσης αφαιρούμενων συσκευών αποθήκευσης στον οργανισμό καθώς και μπλοκάρισμα ή απομόνωση εμπιστευτικών αρχείων που ενδεχομένων αντιγραφούν σε αυτές τις συσκευές, όπως είναι οι αφαιρούμενες συσκευές αποθήκευσης (USB sticks) ή τηλεφώνων (smart phones).

γ. Αποκλεισμός ή απομόνωση εκτύπωσης, από θέσεις εργασίας, εγγράφων που περιέχουν εμπιστευτικές πληροφορίες.

δ. Ανακάλυψη εμπιστευτικών δεδομένων τα οποία βρίσκονται αποθηκευμένα στο δίκτυο, σε βάσεις δεδομένων, σε σταθμούς εργασίας και σε φορητούς υπολογιστές στον οργανισμό.

5.3.2. Κεντρική Διαχείριση

α. Υπάρχει κεντρική διαχείριση από για όλα τα τμήματα MyDLP με φιλικό προς το χρήστη interface.

β. Μπορεί να οριστεί ένας ενιαίος κανόνας για όλα ή μπορούν να οριστούν διαφορετικούς κανόνες για τις διαφορετικές πηγές (AD Ομάδα, Rage TCP δικτύου κ.λπ.) καθώς και διαφορετικούς προορισμούς (ιστοσελίδες, πεδία Email κ.λπ.).

γ. Μπορεί να διαχειριστεί αποτελεσματικά πολιτικές DLP σε χιλιάδες πράκτορες (agent) καθώς και όλη τη κυκλοφορία του δικτύου με μερικά μόνο κλικ.

δ. Παρακολούθηση όλων των συμβάντων σε αρχεία καταγραφής, και εμφάνιση τους στο ταμπλό καθώς και συλλογής αναφορών.

ε. Μπορεί να πραγματοποιηθεί αναζήτηση, όπως γίνεται με την μηχανή αναζήτησης Google σε αρχεία που είναι σε καραντίνα ή αρχειοθετούνται ως ύποπτα, και να δούμε σχετικές λεπτομέρειες του περιστατικού καθώς και τους χρήστες.

στ. Μπορεί να περιορίσει διαφορετικούς ρόλους διαχείρισης για τη διαμόρφωση και τις λειτουργίες ελέγχου για τους χρήστες και τις ομάδες με την ενσωμάτωση του Microsoft Active Directory.

ζ. Επιτρέπει σε στελέχη και άλλο μη τεχνικό προσωπικό με διαπίστευση ρόλου διαχειριστή να σηματοδοτήσει τα έγγραφα ως εμπιστευτικά, χωρίς συναγερμό του IT προσωπικού ή της παραβίασης της πολιτικής DLP.

5.3.3. MyDLP Network Protecrion

Η προστασία του δικτύου εφαρμόζεται σε όλο το δίκτυο του οργανισμού. Ανεξάρτητα το χώρο και το γεωγραφικό μέρος στο οποίο βρίσκονται τα τμήματα. Πραγματοποιείται σχεδόν γραμμική κλιμάκωση κατά την εφαρμογή. Υπάρχει ελευθερία και δυνατότητα να εκτελεστεί σε εικονική μηχανή ή οποιοδήποτε υπολογιστή διαθέτει τις ελάχιστες απαιτήσεις. Μπορεί να αναλύσει μεγάλα αρχεία σε λίγα μόλις λεπτά. Τα κανάλια επικοινωνίας τα οποία υποστηρίζει είναι και το διαδίκτυο καθώς και το ηλεκτρονικό ταχυδρομείο. Μπορεί να ενσωματωθεί η εφαρμογή MyDLP με οποιοδήποτε proxy server ή στις πύλες παράδοσης χρησιμοποιώντας το πρωτόκολλο ICAP. Επίσης μπορεί να χρησιμοποιηθεί η κλασσική μέθοδο proxy. Ακόμα η εφαρμογή λειτουργεί με οποιοδήποτε είδος MTA (Massage Transfer Agent) συμπεριλαμβανομένου και του Microsoft Exchange χρησιμοποιώντας ενσωμάτωση σε μια πύλη SMTP. Υπάρχει η δυνατότητα να πραγματοποιηθεί απρόσκοπτη ενσωμάτωση σε οποιοδήποτε ICAP το οποίο υποστηρίζει Proxy ή οποιαδήποτε λύση για φιλτράρισμα του περιεχομένου. Ακόμα μπορεί να ενσωματωθεί με την Microsoft.

Μπορεί να φιλτράρει τον exchange server ή οποιοδήποτε άλλο e-mail. Έχει την επιλογή να πραγματοποιηθεί ανίχνευση και ανακάλυψη των ευαίσθητων δεδομένων είτε με πράκτορα ή χωρίς αυτόν. Τέλος μπορεί να παρακολουθεί ή να μπλοκάρει μηνύματα ηλεκτρονικού ταχυδρομείου με εξωτερική διεύθυνση BCC.

5.3.4. MyDLP Endpoint

Μας δίνεται η δυνατότητα κατά την εφαρμογή της συγκεκριμένης λύσης να γίνεται έλεγχος στις αφαιρούμενες συσκευές και στους εκτυπωτές που συνδέονται με φορητούς υπολογιστές και με τους σταθμούς εργασίας. Μπορεί να αναπτυχθεί εύκολα με τις ήδη υπάρχουσες υποδομές ανάπτυξης όπως είναι για παράδειγμα το Microsoft Active Directory. Εφαρμόζοντας σε έναν φορητό υπολογιστή μπορεί να προστατέψει τα δεδομένα και εκτός δικτύου του οργανισμού. Ανακαλύπτει δεδομένα που έχουν χαρακτηριστεί ως ευαίσθητες και ειδικού χειρισμού. Έχει τη δυνατότητα υποστήριξης όλων των τύπων των εκτυπωτών χωρίς καμία εξαίρεση. Χρησιμοποιεί ελάχιστους πόρους από το σύστημα και δεν ενοχλεί τους χειριστές με μηνύματα ή άλλες ενοχλητικές ειδοποιήσεις. Τέλος κρυπτογραφείται ο τομέας σε αφαιρούμενες συσκευές αποθήκευσης.

5.3.5. Διαχείριση Πολιτικών

Είναι αρκετά απλή και λειτουργική η διαδικασία δημιουργίας πολιτικών ασφαλείας. Οποιοσδήποτε είναι εξοικειωμένος με την διαδικασία της ασφάλειας πληροφοριών μπορεί εύκολα να τη χρησιμοποιήσει, δεν χρειάζεται να είναι κάποιος ειδικός πάνω στην συγκεκριμένη εφαρμογή.

α. Είναι εύκαμπτη. Μπορεί να χρησιμοποιηθεί οποιοδήποτε αντικείμενο σε οποιοδήποτε κανάλι μεταφοράς δεδομένων.

β. Κεντρικός έλεγχος. Μπορεί να διαχειριστεί ολόκληρη η εφαρμογή DLP χρησιμοποιώντας μόνο ένα απλό web interface.

γ. Είναι ενοποιημένα. Όλα τα είδη ανάλυσης των περιεχομένων είναι διαθέσιμα και για όλα τα είδη των καναλιών επικοινωνίας. Από τους προκαθορισμένους τύπους δεδομένων, όπως είναι για παράδειγμα οι αριθμοί πιστωτικών καρτών έως την μερική αντιστοίχιση ενός κειμένου με κάποιο παρεμφερές κείμενο, μπορεί να χρησιμοποιηθούν όλων των ειδών ορισμοί περιεχομένου, για το διαδίκτυο, για το ηλεκτρονικό ταχυδρομείο, για τις αφαιρούμενες συσκευές αποθήκευσης για τους εκτυπωτές κλπ. Επίσης όπως είναι εύλογο όλα αυτά είναι διαθέσιμα και κατά την διάρκεια της εξερεύνησης (discovery) σε δεδομένα σε αποθήκευση (data at rest).

δ. Δημιουργία πολλαπλών ρόλων. Υπάρχει η δυνατότητα να καθοριστούν πολλαπλοί χρήστες με διαφορετικούς πολλαπλούς ρόλους, όπως είναι Superadmin, Admin, Auditor, κλπ.

ε. Έλεγχος τερματικών. Μας δίνεται η δυνατότητα να παρακολουθούμε τις τερματικές συσκευές χρησιμοποιώντας την κονσόλα διαχείρισης του MyDLP. Για παράδειγμα είμαστε σε θέση να γνωρίζουμε πότε είναι οι υπολογιστές εκτός δικτύου, πότε δεν έχουν τις τελευταίες πολιτικές, η έκδοση του πράκτορα.

Κεφάλαιο 6: Συμπεράσματα - Προτάσεις

6.1 Εισαγωγή

Σε ένα περιβάλλον ιδιαίτερα απαιτητικό και επιβαρυμένο με πληροφορίες, θεωρείται επιβεβλημένη η ανάγκη της μέγιστης και προσεκτικής διαφύλαξης της ασφάλειας των πληροφοριών και των δεδομένων. Οι πληροφορίες και τα δεδομένα που υπάρχουν, που έχουν δημιουργηθεί ή που έχουν συλλεχθεί, κατατάσσονται στα περιουσιακά αγαθά ενός οργανισμού. Κατ' επέκταση χρήζουν και τις αντίστοιχης προστασίας, καθώς επίσης και της αντίστοιχης επιλογής των ατόμων που θα τα διαχειρίζονται. Ένας οργανισμός δεν μπορεί να ρισκάρει στην απώλεια πληροφοριών και δεδομένων, διότι πέρα από την οικονομική απώλεια, δημιουργείται απώλεια και στην ομαλή λειτουργία του, χάνει το ανταγωνιστικό πλεονέκτημα, επιφέροντας αρνητικές επιπτώσεις στους συνεργάτες, στους πελάτες και τελικά στα οικονομικά μεγέθη του οργανισμού. Απαιτείται κατά συνέπεια να προστατέψει τους πόρους που χρησιμοποιεί για να επιτύχει τους στόχους του. Δεδομένα, τα πληροφοριακά του συστήματα, τα δίκτυα και οι άνθρωποι που χειρίζονται όλα αυτά χρειάζονται ένα κανονιστικό πλαίσιο, βάση του οποίου θα λειτουργούν και θα κατευθύνονται. Γίνεται επιβεβλημένη η ανάγκη για την εφαρμογή και λειτουργία συστημάτων προστασίας τα οποία να εστιάζουν πέρα από το δίκτυο. Να εστιάζουν στον άνθρωπο, στο υλικό και στις διαδικασίες.

Επομένως πρώτη ενέργεια είναι η ευαισθητοποίηση της διοίκησης του οργανισμού και στην συνέχεια του αντίστοιχου προσωπικού το οποίο χειρίζεται δεδομένα. Κατόπιν η εφαρμογή της τεχνικής, της στρατηγικής και γενικότερα της πολιτικής ασφαλείας που θα εφαρμοστεί, ανάλογα με το επίπεδο και τον τομέα ενασχόλησής του.

6.2 Συμπεράσματα

Έχοντας αντιληφθεί τις δυνατότητες των εργαλείων DLP, χρησιμοποιώντας μια συγκεκριμένη διαδικασία μπορεί ο κάθε οργανισμός να επιλέξει τα κατάλληλα εργαλεία για τις απαιτήσεις του. Συγκεντρώνοντας αρχικά τις απαιτήσεις και τους πόρους που διαθέτει.

Πρέπει να τεθούν σωστά οι απαιτήσεις. Το DLP είναι ένα πολύ αποτελεσματικό εργαλείο για την αποτροπή ατυχής έκθεσης δεδομένων και της εσφαλμένης διαδικασίας που ακολουθεί ένας οργανισμός γύρω από την διαχείριση των ευαίσθητων πληροφοριών και δεδομένων. Στην περίπτωση όπου ένας οργανισμός αποφασίσει να θωρακιστεί με μια εφαρμογή DLP θα πρέπει να έχει αποφασίσει ποια τμήματα θα εμπλακούν καθώς και πώς θα πραγματοποιηθεί η σχεδίαση. Μετά την ανάπτυξη είναι αργά πλέον να διαπιστώσουμε ότι λάθος άτομα είδαν τις πολιτικές ασφαλείας ή οι νέες εφαρμογές είναι ακατάλληλες για την προστασία των ευαίσθητων δεδομένων, ή κάποιο τμήμα του οργανισμού δεν συμπεριλαμβάνεται στη σχεδίαση.

Θεωρείται ότι αν και η εφαρμογές καθώς και τα εργαλεία DLP είναι σε αρχικό στάδιο μπορούν να παρέχουν υψηλής ποιότητας προστασίας για όσους οργανισμούς μπορούν να σχεδιάσουν σωστά και καταλαβαίνουν πώς να εκμεταλλεύονται τις πλήρεις δυνατότητες τους. Επικεντρωνόμαστε σε εκείνα τα χαρακτηριστικά τα οποία είναι πιο σημαντικά για τον οργανισμό, παρέχοντας συγκεκριμένη προσοχή στην δημιουργία πολιτικών και στην διαδικασία διαχείρισης. Τέλος απαιτείται να έχουμε δημιουργήσει ομάδες εργασίας από τμήματα του οργανισμού πριν ξεκινήσει η εφαρμογή των εργαλείων DLP.

Προσεκτικός και λεπτομερείς σχεδιασμός, καθώς και προετοιμασία, συνεργασία όπως επίσης και επίγνωση της σωστής και καταρτισμένης εκπαίδευσης, κυριαρχούν στην ανάπτυξη μιας επιτυχημένης εφαρμογής προγράμματος DLP.

6.3 Προτάσεις

Έχοντας κατανοήσει η διοίκηση και τα στελέχη ενός οργανισμού την αναγκαιότητα της σωστής δομής και σχεδίασης μιας λειτουργικής διεξαγωγής διακίνησης και αποθήκευσης των δεδομένων.

Τα πληροφοριακά συστήματα να χρησιμοποιηθούν για τον σκοπό που προορίζονται και όχι για κάποιον διαφορετικό.

Επιλογή του κατάλληλου προσωπικού για την σχεδίαση. Στη συγκεκριμένη διαδικασία θεωρείται επιβεβλημένο να συμμετέχουν τα τμήματα του οργανισμού που θα δημιουργούν, θα διαχειρίζονται, θα μεταφέρουν και θα αποθηκεύουν ευαίσθητα δεδομένα. Όλοι πρέπει να θέσουν τις απαιτήσεις τους καθώς και τον βαθμό ασφαλείας των πληροφοριών. Με αυτόν τον τρόπο προσδιορίζονται οι πολιτικές ασφαλείας των συγκεκριμένων δεδομένων, καθορίζοντας τον τρόπο διακίνησης, χρήσης και τέλος τον τρόπο και τον χώρο αποθήκευσης. Στη συνέχεια καταλήγουμε στην χρυσή τομή έτσι ώστε και ασφάλεια να υπάρχει και να μην παρεμποδίζεται η ομαλή λειτουργία του οργανισμού. Έπειτα καθορίζονται οι διαδικασίες και τα στελέχη που θα στελεχώσουν το τμήμα το οποίο θα είναι επιφορτισμένο να αντιμετωπίσει μια ενδεχόμενη κρίση ή καταστροφή. Αυτές μπορεί να είναι είτε εκούσιες, είτε ακούσιες. Ακόμα χρειάζεται να καθοριστούν ακριβώς οι ενέργειες που απαιτούνται μετά από μία ενδεχόμενη κρίση. Τέλος απαιτείται να καθοριστεί ο τρόπος λειτουργίας τους για περιπτώσεις εκτός ωραρίου. Σχεδιάζεται η εφαρμογή για το σύστημα και πραγματοποιούνται οι δοκιμές οι οποίες θα φανερώσουν τυχόν αδυναμίες ή δυσλειτουργίες. Από την στιγμή που όλα βαδίζουν βάση του προγραμματισμού και έχουν ικανοποιηθεί όλες οι απαιτήσεις τίθεται σε λειτουργία η εφαρμογή. Ο διαχειριστής της εφαρμογής παρακολουθεί την λειτουργία της εφαρμογής και είναι έτοιμος να επέμβει για την επίλυση δυσλειτουργίων. Οι επικεφαλής των τμημάτων επίσης έχουν την υποχρέωση να μεταδώσουν τους κανονισμούς και τις πολιτικές ασφαλείας που ισχύουν στα τμήματά τους.

Θωρακίζοντας κατ' αυτό τον τρόπο τις διαδικασίες μεταφοράς των δεδομένων μέσω των γνωστών διαύλων επικοινωνίας όπως το ηλεκτρονικό ταχυδρομείο, τα έγγραφα κειμενογράφου, τις βάσεις δεδομένων κ.ά. είμαστε σε θέση να μειωθεί σημαντικά ο κίνδυνος απώλειας δεδομένων.

Κεφάλαιο 7: Βιβλιογραφία

Βιβλιογραφικές Αναφορές

Ηλεκτρονικές Πηγές

1. Adrew Gavin, n.d. *Google Code.* [Ηλεκτρονικό]
Available at: https://code.google.com/archive/p/opendlp/
[Πρόσβαση 4 Ιουλίου 2014].

2. COMODO, 2015. *COMODO.* [Ηλεκτρονικό]
Available at: www.mydlp.com
[Πρόσβαση 15 Δεκεμβριος 2016].

Ξενόγλωσση Βιβλιογραφία

1. J. Kurose – K.Ross, 2013. *Computer Networking.* Sixth Edition επιμ. New Jersey, USA: Pearson Education, Inc.

2. P. kanagasingham – SANS Institute, 2008. *Data loss Prevention,* USA: SANS Institute.

3. Power Hamilton, n.d. *Data Loss Prevention Program,* USA: Foundstone.

4. R.Mogull, n.d. *Understanding and Selecting a Data Loss Prevention Solution,* USA: SANS Institute.

5. W.Stallings, 2006. *Cryptography and Network Security.* 4th Edition επιμ. New Jersey: Pearson Education.

6. COMODO, 2013. *MyDLP Installation Guide,* USA: Comodo.

Ελληνική Βιβλιογραφία

1. Γ.Πάγκαλου – Ι. Μαυρίδη, 2002. *Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων.* Θεσσαλονίκη: Αννικούλα.

2. Σ. Γκρίτζαλη, Σ. Κάτσικα, Δ.Γκρίτζαλη, 2004. *Ασφάλεια Δικτύων Υπολογιστών.* Αθήνα: Παπασωτηρίου.

3. Σ. Κάτσικας, 2014. *Διαχείριση της Ασφάλειας Πληροφοριών.* Αθήνα: Πεδίο.