ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ.

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ.

Πρόγραμμα Μεταπτυχιακών Σπουδών:

«Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών»

(Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων).

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ.

“Μηχανισμοί Ανίχνευσης Υποκλοπής και Διαρροής Πληροφοριών από Εσωτερικά Επιτιθέμενους”

(Detection Mechanisms for Interception and Data Leakage by Insiders).

ΑΠΟΣΤΟΛΟΣ Σ. ΚΑΜΑΡΙΩΤΗΣ
A.M: mcse19035

Εισηγήτρια: Ιωάννα Καντζάβελου.

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ.

"Μηχανισμοί Ανίχνευσης Υποκλοπής και Διαρροής Πληροφοριών από Εσωτερικά Επιτιθέμενους"

ΑΠΟΣΤΟΛΟΣ Σ. ΚΑΜΑΡΙΩΤΗΣ.
Α.Μ. mcse19035.

Εισηγήτρια:

Ιωάννα Καντζάβελου, Επ. Καθηγήτρια.

Ioanna Kantzavelou
Digitally signed by Ioanna Kantzavelou
Date: 2022.02.07 13:41:32 +02'00'

Εξεταστική Επιτροπή:

Αντώνιος Μπόγρης, Καθηγητής.

Antonios Bogris
Digitally signed by Antonios Bogris
Date: 2022.02.08 16:39:56 +02'00'

Βασίλειος Μάμαλης, Καθηγητής.

Vasileios Mamalis
Digitally signed by Vasileios Mamalis
Date: 2022.02.08 12:13:32 +02'00'

Ημερομηνία εξέτασης: 26/01/2022.

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ.

Ο κάτωθι υπογεγραμμένος **Απόστολος Καμαριώτης** του Στέργιου, με αριθμό μητρώου **mcse19035** φοιτητής του **Προγράμματος Μεταπτυχιακών Σπουδών: Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών** *(Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων)* του **Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών** της **Σχολής Μηχανικών** του **Πανεπιστημίου Δυτικής Αττικής**, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών.

Digitally signed by APOSTOLOS KAMARIOTIS
Date: 2022.02.07 12:18:22 EET

Απόστολος Καμαριώτης.

ΕΥΧΑΡΙΣΤΙΕΣ.

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο. Την προσπάθειά μου αυτή υποστήριξε η επιβλέπουσα Καθηγήτριά μου **Ιωάννα Καντζάβελου**, την οποία θα ήθελα να ευχαριστήσω.

Ακόμα θα ήθελα να ευχαριστήσω την οικογένειά μου για την Υπομονή της με **(Υ)** – Κ Ε Φ Α Λ Α Ι Ο….

ΠΕΡΙΛΗΨΗ.

Η προστασία εμπιστευτικών δεδομένων και πληροφοριών από διαρροή, αποτελεί μια από τις μεγαλύτερες ανησυχίες παγκοσμίως. Παραδοσιακά, η εμπιστευτικότητα των δεδομένων διατηρείται χρησιμοποιώντας διάφορες διαδικασίες, μαζί με συμβατικούς μηχανισμούς όπως πολιτικές ασφάλειας, firewalls, εικονικά ιδιωτικά δίκτυα VPN, Proxy Servers, συστήματα ανίχνευσης εισβολών IDSs κ.τ.λ. Δυστυχώς, όμως αυτοί οι μηχανισμοί στερούνται προληπτικότητας και προβλεψιμότητας όσον αναφορά την διαρροή αλλά και την προστασία των εμπιστευτικών δεδομένων, τα οποία εμφανίζονται σε διάφορες μορφές, ψηφιακές και μη, αλλά και χωροταξικά σε διαφορετικά σημεία αποθήκευσης και επεξεργασίας. Τα πράγματα γίνονται ακόμη πιο σύνθετα, όταν αυτοί οι μηχανισμοί καλούνται να αντιμετωπίσουν επιπλέον κινδύνους διαρροών που προέρχονται από εσωτερικές απειλές. Οι “εσωτερικά επιτιθέμενοι” (Insiders) είναι πολύ σημαντική απειλή, γιατί δύναται να μην εντοπιστούν οι παραβιάσεις τους ποτέ. Περιπτώσεις, όπως υποκλοπή και διαρροή δεδομένων σε τρίτους, συχνά αποτελούν ανεξιχνίαστα περιστατικά ή πολλές φορές δεν διαπιστώνεται ότι συνέβησαν. Κλασικοί μηχανισμοί προστασίας αποδεικνύονται ανεπαρκείς με ιδιαίτερα δυσμενή αποτελέσματα, όταν τα δεδομένα είναι ευαίσθητα. Σχετικά πρόσφατα, έχουν εισαχθεί ειδικοί μηχανισμοί για τον ***Εντοπισμό*** και κυρίως τη ***Πρόληψη Διαρροής*** εμπιστευτικών ***Δεδομένων και Πληροφοριών (Data & Information Leakage Prevention Systems – DLPS, ILPS).*** Χρησιμοποιώντας διάφορες τεχνικές, οι μηχανισμοί αυτοί, σχεδιάζονται και αναπτύσσονται από ερευνητές ασφάλειας πληροφορικής, αλλά και εμπορικούς προμηθευτές, κυρίως ως αυτόνομα προϊόντα.

Το θέμα της εργασίας αυτής αποτελεί τη μελέτη των μηχανισμών που υπάρχουν για την ανίχνευση ***α) υποκλοπών*** και ***β) διαρροής δεδομένων*** προς τρίτους, αλλά και την αναγνώριση των αδυναμιών τους.

Λέξεις Κλειδιά:

DLP, ILP, Διαρροή Δεδομένων, Απώλεια Δεδομένων, Διαρροή Πληροφοριών, Δεδομένα σε αποθήκευση, Δεδομένα σε χρήση, Δεδομένα σε κίνηση.

ABSTRACT.

Protection of confidential data and information from being leaked is one of the biggest concerns worldwide. Traditionally, data confidentiality is preserved using various procedures, such as information security policies along with conventional security mechanisms, firewalls, virtual private VPN networks, Proxy Servers, IDSs intrution detection systems etc. Unfortunately, these mechanisms lack preventiveness and predictability regarding leakage and protection of confidential data which appear in various forms, digital and non-digital, but also spatially at different storage and processing points. Things get even more complicated when these mechanisms need to deal with the additional risk of leakings which stem from internal threats. Internal attackers (Insiders) are a grave threatening because their violations may never be detected. Cases, such as incidents of data interception and leakage to third parties are often unsolved cases or are not confirmed to have occurred. Conventional protection mechanisms prove to be inadequate, accompanied by particularly adverse effects when data is sensitive. Quite recently, special mechanisms have been introduced to detect and in particular prevent the leakage of confidential data and **Data & Information Leakage Prevention Systems (DLPS) (ILPS)** material. Using various techniques, these mechanisms are designed and developed mainly as standalone products by IT security researchers as well as by commercial suppliers. The subject of this project is the study of the mechanisms that exist for the detection of

a) interceptions and ***b) data leakage*** to third parties, as well as for the acknowledgement of their weakness.

Keywords:

DLP, ILP, Data Leakage, Data Loss, Information Leakage, Date in Rest (DIR), Data in Use (DIU), Data in Motion (DIM).

ΠΕΡΙΕΧΟΜΕΝΑ.

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ.

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ.

DAR: Data At Rest.

DIM: Data In Motion.

DIU: Data In Use.

DLPS: Data Leakage Prevention Systems.

DLPS: Data Loss Prevention Systems.

DoS: Denial of Service.

IDS: Intrusion Detection Systems.

ILPS: Information Leak Prevention.

ILPS: Information Loss Prevention.

IM: Instant Message.

IPS: Intrusion Prevention Systems.

IS: Information Security.

LSBS: Least Significant Bit Steganography.

NFC: Near Field Communication.

SSL: Secure Sockets Layer.

VPN: Virtual Private Network.

1. ΕΙΣΑΓΩΓΗ.

Η πρόληψη της αποκάλυψης δεδομένων σε μη εξουσιοδοτημένες οντότητες είναι ένας από τους κύριους στόχους της ασφάλειας των πληροφοριών (Information Security - IS). Συνεπώς, οδηγεί τόσο τον ακαδημαϊκό όσο και τον εμπορικό τομέα να ερευνήσει, να σχεδιάσει και να αναπτύξει λύσεις ασφαλείας για την μείωση του κινδύνου διαρροής δεδομένων. Η αποφυγή της διαρροής δεν είναι πάντα δυνατή λόγω της ανάγκης πρόσβασης, κοινοποίησης και χρήσης της πληροφορίας, όπου η κυκλοφορία εμπιστευτικών δεδομένων είναι αναπόφευκτη. Η διαρροή ή η απώλεια πληροφοριών μπορεί να είναι αποτέλεσμα εσκεμμένης δράσης ή κάποιου λάθους. Πρόσφατες αναφορές προερχόμενες από το *Datalossdb* έδειξαν [1], ότι περίπου το 50% της καταγεγραμμένης διαρροής δεδομένων σημειώθηκε σε επιχειρήσεις διαφόρων κλάδων, περίπου 20% σημειώθηκε σε κυβερνητικούς τομείς και περίπου 30% σε τομείς υγείας και εκπαίδευσης. Επίσης, μικρού μεγέθους επιχειρήσεις ιδιωτικού ενδιαφέροντος, ελεύθεροι επαγγελματίες, ιδιώτες κ.τ.λ. επηρεάζονται από τη διαρροή δεδομένων, αλλά είναι δύσκολο να γνωρίσουμε την βαρύτητα, το μέγεθος και τις πιθανές συνέπειες των περιστατικών αυτών. Μερικές αναφερθείσες διαρροές δεν ήταν επιζήμιες για τους οργανισμούς στους οποίους προκλήθηκαν, αλλά στις περισσότερες των περιπτώσεων έχουν προκληθεί τεράστιες ζημιές αρκετών μάλιστα εκατομμυρίων δολαρίων. Εκτός από τις οικονομικές συνέπειες, διακυβεύεται κυρίως η επιχειρηματική αξιοπιστία όταν ευαίσθητα δεδομένα και μυστικά π.χ. για επενδυτικά Projects, μελλοντικά σχέδια, εμπορικές συμφωνίες, μυστικά προγράμματα πελατών, διαρρέουν σε οικονομικούς αντιπάλους και ανταγωνιστές. Οι διαρροές κυβερνητικών δεδομένων ενδέχεται να περιλαμβάνουν ευαίσθητες πληροφορίες σχετικά με την πολιτική και μυστικές παρεμβάσεις, αλλά κυρίως θέματα εσωτερικής ασφάλειας. Ένα δημοφιλές περιστατικό, που αφορούσε διαρροή ευαίσθητων κυβερνητικών πληροφοριών, ήταν η δημοσιοποίηση

διπλωματικών εγγράφων των Ηνωμένων Πολιτειών από το WikiLeaks[1]. Η διαρροή αποτελούνταν από περίπου 250.000 έγγραφα των Ηνωμένων Πολιτειών και 400.000 στρατιωτικές αναφορές, που αναφέρονται ως «war logs». Αυτή η αποκάλυψη πραγματοποιήθηκε από μια εσωτερική οντότητα (insider) χρησιμοποιώντας εξωτερικό σκληρό δίσκο με περίπου 100.000 “Εμπιστευτικά” διπλωματικά έγγραφα και άλλα 15.000 διαβαθμισμένα ως “Μυστικά”. Με αυτό το περιστατικό οι εμπλεκόμενοι κυβερνητικοί φορείς, αντιμετώπισαν μεγάλη κριτική από άλλες κυβερνήσεις και πολιτικές οργανώσεις παγκοσμίως.

Απειλές προερχόμενες από “τα έσω” (insiders) αντιπροσωπεύουν μία από τις πιο δύσκολες κατηγορίες απειλών που πρέπει να λάβει υπόψιν του ένας οργανισμός για τη μείωση του κινδύνου διαρροών. Η πλειοψηφία των περιστατικών απώλειας δεδομένων αποδίδονται σε τωρινούς ή παλαιότερους υπαλλήλους ή σε άλλες περιπτώσεις σε κακόβουλα άτομα, που απέκτησαν πρόσβαση στον εξοπλισμό ενός οργανισμού ή σε αρχεία του προσωπικού, υποκλέπτοντας και διαρρέοντας εμπιστευτικές πληροφορίες δημόσια ή π.χ. σε ανταγωνιστές. Επίσης, υπάρχει και η περίπτωση απώλειας δεδομένων από κάποιο ατυχές γεγονός ή ακόμη και από λάθος χειρισμό. Οι insiders εξ ορισμού διαθέτουν αυξημένα προνόμια και τις περισσότερες των περιπτώσεων έχουν εξιδεικευμένες γνώσεις σχετικά με τα μέτρα ελέγχου και εντοπισμού και ενδέχεται να είναι σε θέση να τα παρακάμψουν. Ο συνδυασμός λογισμικού πρόληψης απώλειας δεδομένων και η τακτική εκπαίδευση των εργαζομένων, μειώνουν τις πιθανότητες ένας υπάλληλος να βγάλει ευαίσθητες πληροφορίες εκτός οργανισμού χωρίς άδεια ή από κάποιο λάθος.

Η ανάγκη αντιμετώπισης τόσο σοβαρών ζητημάτων ασφάλειας, ωθούν τους ειδικούς να αντιμετωπίσουν μια από τις μεγαλύτερες προκλήσεις, ώστε να αναπτύξουν διάφορους μηχανισμούς ασφαλείας. *Συστήματα Εντοπισμού Εισβολών (Intrusion detection Systems - IDS)* ή *Συστήματα Πρόληψης*

[1] Το ***WikiLeaks*** είναι διεθνής μη κερδοσκοπικός οργανισμός ΜΜΕ ο οποίος δημοσιεύει έγγραφα από ανώνυμες πηγές και διαρροές, που υπό άλλες συνθήκες δεν θα έβλεπαν το φως της δημοσιότητας. Τον ιστότοπο του οργανισμού, ο οποίος και ξεκίνησε τη λειτουργία του το 2006, διαχειρίζεται η «The Sunshine Press».

Εισβολών (Intrusion Prevention Systems - IPS) και *Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Network - VPN)* έχουν εισαχθεί τις τελευταίες δεκαετίες. Αυτά τα συστήματα αποδεδειγμένα μπορούν να αποδώσουν ικανοποιητικά αποτελέσματα, εάν τα δεδομένα που προστατεύονται είναι καλά ορισμένα, δομημένα και σταθερά. Η χρησιμοποίηση μόνο τέτοιου είδους μέτρων για την προστασία εμπιστευτικών δεδομένων σίγουρα δεν είναι επαρκής, γιατί π.χ. ένα firewall μπορεί να αποκλείσει με επιτυχία τη πρόσβαση σε ένα εμπιστευτικό τμήμα δεδομένων χρησιμοποιώντας απλούς κανόνες, ωστόσο το ίδιο τμήμα δεδομένων μπορεί να είναι προσβάσιμο μέσω άλλων μέσων όπως ένα συνημμένο email για παράδειγμα ή ανταλλαγής άμεσων μηνυμάτων (IM) κ.τ.λ. Έτσι τα συμβατικά μέτρα ασφαλείας (firewalls, IDSs, VPNs) δεν έχουν την ικανότητα για τέτοιου είδους περιπτώσεις.

Για να ξεπεραστεί αυτή η αδυναμία, μια νέα κατεύθυνση για την προστασία των ευαίσθητων δεδομένων θεωρήθηκε απαραίτητη. Νέα σχεδιασμένα συστήματα *Πρόληψης και Απώλειας Διαρροών* **(Data Leakage *I* Loss Prevention Systems - DLPSs)** έχουν τη δυνατότητα αναγνώρισης, παρακολούθησης και προστασίας δεδομένων, εντοπίζοντας με μεγαλύτερη επιτυχία κακή χρήση βάσει προκαθορισμένων κανόνων. Τα DLPs θεωρούνται σχετικά νέα σε σύγκριση με τις συμβατικές λύσεις ασφαλείας και αποτελούν αντικείμενο συνεχούς έρευνας από ακαδημαϊκούς αλλά και μεγάλους επαγγελματίες συστημάτων ασφαλείας.

Ένας διαχωρισμός που είναι απαραίτητος να γίνει, είναι να αναδειχθεί η διαφορά μεταξύ των DLPS ως ολοκληρωμένη λύση και των DLPS ως χαρακτηριστικό γνώρισμα. Ορισμένα προϊόντα για παράδειγμα, προσφέρουν λύσεις ασφάλειας ηλεκτρονικού ταχυδρομείου ή αποκλεισμού μεταφοράς δεδομένων μέσω φορητών μέσων, παρέχοντας βασικές λειτουργίες DLP, αλλά δεν αποτελούν ολοκληρωμένες DLP λύσεις. Η διαφορά μεταξύ τους είναι ότι:

- Ένα προϊόν DLP ως ολοκληρωμένη λύση, περιλαμβάνει πλατφόρμα κεντρικής διαχείρισης, δυνατότητα δημιουργίας πολιτικών και κανόνων προστασίας, ειδικά χαρακτηριστικά ανίχνευσης απειλών και αποτελούν μια ολοκληρωμένη σουίτα λογισμικού ή μια αυτόνομη συσκευή DLP.

- Οι λύσεις με χαρακτηριστικά DLP, περιλαμβάνουν ορισμένες από τις δυνατότητες ανίχνευσης των ολοκληρωμένων προϊόντων DLP. Πολλές φορές αποκαλούνται “DLP Light” και αποτελούν ένα επιπλέον χαρακτηριστικό κάποιων εργαλείων ή μηχανισμών ασφαλείας.

Αυτή η διάκριση είναι σημαντική, κυρίως για τους διαχειριστές ασφαλείας ενός οργανισμού, προκειμένου να επιλέξουν τη βέλτιστη λύση, για να διασφαλιστεί με τον καλύτερο δυνατό τρόπο η προστασία των δεδομένων τους.

Καθώς οι μεγάλοι προμηθευτές εισέρχονται στο χώρο των DLPS, νέα προϊόντα καθώς και ερευνητικές προτάσεις εμφανίζονται σε ένα διαρκώς μεταβαλλόμενο περιβάλλον, που ορίζεται δυστυχώς από όλο πιο έμπειρους και κακόβουλους εισβολείς.

Η εργασία αυτή είναι δομημένη ως εξής:

Στο ***κεφάλαιο 2*** περιγράφεται η αξία της πληροφορίας και αναλύεται η διαφοροποίησή της με τα δεδομένα. Επίσης, ενδεικτικά αναφέρονται κάποια από τα πιο χρήσιμα πρότυπα και νομικές ρυθμίσεις που έχουν εκδοθεί για την ασφάλεια πληροφοριών.

Στο ***κεφάλαιο 3*** ορίζονται η εσωτερική απειλή και οι εσωτερικά επιτιθέμενοι, τα κίνητρά τους, οι επιδράσεις μιας επίθεσης, οι τρόποι ελέγχου και παρακολούθησης και οι κοινωνικοτεχνικές προσεγγίσεις τους.

Στο ***κεφάλαιο 4*** περιγράφεται ο εντοπισμός επιθέσεων, η ανίχνευση εισβολών και η ταξινόμησή τους.

Στο ***κεφάλαιο 5*** αναλύονται τα συστήματα πρόληψης διαρροών δεδομένων (DLPS) και οι τρεις καταστάσεις τους, σε ηρεμία, σε κίνηση και σε χρήση (DAR - DIM - DIU). Επίσης, περιγράφεται η διαφορά ανάλυσης περιεχομένου και ανάλυσης πλαισίου, καθώς και οι επτά προκλήσεις που καλούνται να αντιμετωπίσουν τα συστήματα DLP. Επιπροσθέτως, αναφέρονται οι διαφορές των ολοκληρωμένων εφαρμογών DLPS, των λύσεων με χαρακτηριστικά DLPS και περιγράφονται οι εμπορικές και ακαδημαϊκές προσεγγίσεις των μηχανισμών αυτών με τα προτερήματα και τις αδυναμίες τους.

Τέλος, η παρούσα εργασία στο ***κεφάλαιο 6*** καταλήγει σε κάποια συμπεράσματα για την σωστή εφαρμογή των DLPS και προτείνει μελλοντικά ερωτήματα και διαδικασίες, που πιθανόν να βοηθήσουν αποτελεσματικά στην

αντιμετώπιση των εσωτερικών απειλών και την αποτροπή διαρροής εμπιστευτικών δεδομένων.

2. Αξία της Πληροφορίας.

Διαρροή / απώλεια δεδομένων είναι ένας όρος που χρησιμοποιείται στον χώρο της ασφαλείας για να περιγράψει ανεπιθύμητες αποκαλύψεις και διαρροές πληροφοριών. Επίσης, η διαφοροποίηση ανάμεσα στις πληροφορίες και στα δεδομένα είναι πολύ λεπτή και η έλλειψη κατανόησής της είναι μια από τις αιτίες παρεξηγήσεων. Τα *Δεδομένα* δεν είναι τίποτε άλλο παρά ένα σύνολο καταγραμμένων συμβόλων. *Πληροφορία* είναι τα δεδομένα μαζί με την υποκειμενική ερμηνεία τους. Πιο αναλυτικά [2]:

- **Δεδομένα (Data):** Αποτελούνται από αριθμούς, κείμενο ή σήμα όπως εικόνες, ήχος και βίντεο, που μπορούν να καταγραφούν σε ένα σύστημα. Τα δεδομένα είναι οτιδήποτε μπορεί να καταγραφεί στον πραγματικό κόσμο και να εισαχθεί σε έναν Η/Υ με τη μορφή bits, για αποθήκευση και επεξεργασία, χωρίς απαραίτητα να είναι ξεκάθαρη η σημασία τους, ενώ με κατάλληλη επεξεργασία από τον άνθρωπο ή από αυτόματα μέσα βοηθάνε στη λήψη σωστών αποφάσεων.

Εικόνα 2.1: *Data vs Information.*

- **Πληροφορία (Information):** Η επεξεργασία των δεδομένων μας δίνουν την πληροφορία. Οι πληροφορίες μας βοηθούν να λαμβάνουμε αποφάσεις, να λύνουμε προβλήματα, προσφέρουν επιπρόσθετη γνώση και έχουν νόημα και συγκεκριμένη χρησιμότητα.

Οι πληροφορίες λοιπόν αποτελούνται από δεδομένα μαζί με την ερμηνεία τους που αποδίδει νόημα σε αυτά.

Λαμβάνοντας υπόψη τον ορισμό του ISO/IEC 27002:2013 [3], η πληροφορία είναι ουσιαστικά ένα αγαθό, το οποίο όπως όλα τα επιχειρηματικά αγαθά έχει ορισμένη αξία σε αυτόν που την κατέχει και συνεπώς χρειάζεται να διασφαλιστεί με τον κατάλληλο τρόπο. Η πληροφορία μπορεί επίσης, να αποτελέσει αντικείμενο οικονομικής συναλλαγής, επομένως έχει και κόστος και αξία, ωστόσο δεν καταναλώνεται, σε αντίθεση με τα υλικά αγαθά ή τον χρόνο. Μπορεί δηλαδή να πουληθεί περισσότερο από μια φορά από τον ίδιο ιδιοκτήτη και η αξία της διαμορφώνεται με βάση παράγοντες, οι οποίοι μπορούν να την κάνουν μεγαλύτερη από το αναγνωρίσιμο κόστος, όπως [4]:

1. Η αποκλειστική κατοχή.
2. Η χρησιμότητά της.
3. Το κόστος δημιουργίας ή αναδημιουργίας της.
4. Η αστική ή νομική ευθύνη.
5. Η μετατρεψιμότητα και
6. Η επιχειρηματική σημασία της.

Υπάρχει μια αυξανόμενη εξάρτηση της οικονομίας από την πληροφορία, ενώ η ανάπτυξη και η λειτουργία μεγάλου μέρους του επιχειρηματικού κόσμου βασίζεται στην ύπαρξη, διαχείριση και επεξεργασία της. Έτσι πολλές φορές, η κατοχή της κατάλληλης πληροφορίας υπό προϋποθέσεις, μετατρέπεται σε περιουσιακό στοιχείο αυτού που την κατέχει, αποκτώντας πολλές φορές υπεραξία. Μια από τις μεθόδους καθορισμού της αξίας της πληροφορίας είναι το κόστος δημιουργίας ή η απόκτησής της. Σε κάποιες περιπτώσεις μπορεί να εκτιμηθεί η αξία της πληροφορίας βάσει των επιπτώσεων που έχει στην επιχείρηση η απουσία της. Είναι σημαντικό λοιπόν, μια εταιρία να μπορεί να εκτιμήσει την πραγματική αξία των δεδομένων και πληροφοριών που κατέχει, ώστε να είναι σε θέση να τα διασφαλίσει με τον καταλληλότερο τρόπο.

Τέλος, πέραν της οικονομικής σημασίας της πληροφορίας, πρέπει να τονιστεί και η κοινωνική της σημασία και αξία. Ανάλογα τη κάθε περίπτωση, η πληροφορία μπορεί δυστυχώς να χρησιμοποιηθεί για την άσκηση ελέγχου, την παρακολούθηση δραστηριοτήτων, ατόμων ή και κοινωνικών ομάδων. Για αυτόν το λόγο θα πρέπει να υπάρχουν κανόνες και ένα πλαίσιο θεσμικών, οργανωτικών και κοινωνικών δράσεων που να εξασφαλίζουν την κοινωνικά αποδεκτή και ορθή χρήση των πληροφοριών.

Παραδείγματα νομικών ρυθμίσεων σε ευρωπαϊκό επίπεδο [4], είναι η σύβαση 108 του Συμβουλίου της Ευρώπης και οι ευρωπαϊκές οδηγίες 95/46, 2002/58 και 2006/24.

Σε εθνικό επίπεδο, είναι τα άρθρα 9Α και 19 του Συντάγματος και οι νόμοι 2472/97 περί «Προστασίας δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών», όπως έχει τροποποιηθεί και ισχύει. Ακόμα, σε εθνικό επίπεδο κανονιστικές ρυθμίσεις έχουν εκδοθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ) και την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).

Σκόπιμα γίνεται ενδεικτική μόνο αναφορά σε κάποιες νομικές ρυθμίσεις, γιατί η περεταίρω ανάλυσή τους δεν αποτελεί αντικείμενο της παρούσας εργασίας. Όσον αφορά τις οργανωτικές δράσεις, δηλαδή τα μέτρα που πρέπει να λάβει κάθε οργανισμός για να διασφαλίσει την προστασία των πληροφοριών που διαχειρίζεται, αυτές μπορούν να είναι [5]:

- Η αναγνώριση των γενικών αρχών που διέπουν την προστασία των πληροφοριών στα πληροφοριακά συστήματα του οργανισμού.
- Η διαμόρφωση πολιτικών ασφαλείας με βάση τις οποίες θα πρέπει να λειτουργήσει ο οργανισμός.
- Η διαμόρφωση τεχνικών και διαδικαστικών μέτρων για τη συμμόρφωση με την πολιτική ασφαλείας (σχέδιο ασφαλείας).

Οι κοινωνικές δράσεις αφορούν κυρίως την εκπαιδευτική διαδικασία, την ενημέρωση και την ευαισθητοποίηση των πολιτών για την αναγκαιότητα της προστασίας των πληροφοριών.

Προκειμένου να διασφαλιστεί η ακεραιότητα των πληροφοριών έχουν γίνει πολλές προσπάθειες για τη δημιουργία προτύπων και πιστοποιήσεων. Ωστόσο, στις τεχνολογίες πληροφορικής και επικοινωνιών υπάρχουν πρότυπα που αναπτύσσονται από εταιρείες ή οργανώσεις κοινής αποδοχής χωρίς να υπάρχει κανονιστική ή νομική υποχρέωση συμμόρφωσης σε αυτά. Μέσω των προαναφερόμενων προτύπων [5]:

- Επιτυγχάνεται μια γενικά αποδεκτή ορολογία για την ασφάλεια.
- Καθορίζονται κοινές αποδοχές για τις προδιαγραφές ασφαλείας.

- Συμφωνούνται τα αποδεκτά επίπεδα ασφαλείας.
- Επιτυγχάνεται η ασφαλής λειτουργικότητα των συστημάτων.

Επιπρόσθετα, το Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (ISACA) και ο Διεθνής Οργανισμός Τυποποίησης (ISO) έχουν εκδώσει κατευθυντήριες γραμμές για όσους διαχειρίζονται θέματα ασφάλειας καθώς και πληθώρα χρήσιμων δημοσιεύσεων για την ασφάλεια πληροφοριών. Όλα αυτά τα πρότυπα χρησιμοποιούνται από οργανισμούς και εταιρίες ώστε εφαρμόζοντάς τα να βελτιωθούν και να μπορέσουν να πιστοποιηθούν καταλλήλως. Ενδεικτικά και πάλι θα αναφερθούν κάποια από τα πιο χρήσιμα πρότυπα για την ασφάλεια πληροφοριών όπως:

1. Η σειρά προτύπων ISO/IEC 27000, γνωστά και ως ISO 27k, που έχουν αναπτυχθεί από κοινού από τον Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization - ISO) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission - IEC)
2. Η σειρά προτύπων BSI-100 του Ομοσπονδιακού Γραφείου για την Ασφάλεια Πληροφοριών της Γερμανίας (Bundesamt für Sicherheit in der Informationstechnik – BSI).
3. Η σειρά προτύπων ISO/IEC 15408, η οποία έχει αναγνωριστεί ως σύστημα προσδιορισμού των απαιτήσεων ασφαλείας για τα προϊόντα υπολογιστών και δικτύων.
4. Το πρότυπο ασφάλειας δεδομένων για εφαρμογές πληρωμής (Payment Application Data Security Standard - PA-DSS) του συμβουλίου προτύπων ασφαλείας PCI. (PA- DSS, 2010)
5. Η σειρά προτύπων του αμερικάνικου εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology-NIST) καθώς και τα πρότυπα FIPS (Federal Information Processing Standards).
6. Το διεθνές πρότυπο ISO 20000-1:2011 «Information technology - Service management - Part 1: Service management system requirements», που έχει ως στόχο τη Διαχείριση Παροχής Υπηρεσιών.

3. Εσωτερικά Επιτιθέμενοι (Insiders).

Η γνωστή ρήση **«Τα κάστρα πέφτουν εκ των έσω»** δυστυχώς έχει επιβεβαιωθεί σε πολλές και άσχημες περιόδους της ιστορίας. Στην Κωνσταντινούπολη για παράδειγμα, η άλωσή της προήλθε μόνο όταν από εσωτερική προδοσία οι Τούρκοι μπόρεσαν και μπήκαν από την Κερκόπορτα περικυκλώνοντας τους αμυνόμενους, ενώ μέχρι εκείνη τη στιγμή δεν είχαν καταφέρει να σπάσουν τη γραμμή άμυνας των τειχών (1453 μ.Χ.).

Αντίστοιχα ο Εφιάλτης, αρχαίος Έλληνας, όπως αναφέρει ο Ηρόδοτος στις Θερμοπύλες, ανέλαβε να οδηγήσει από ένα στενό πέρασμα τους Πέρσες, για να χτυπήσουν από τα νώτα τους Σπαρτιάτες του Λεωνίδα (480 π.Χ.).

Η απειλή λοιπόν για διαρροή εμπιστευτικών πληροφοριών είναι τόσο παλιά όσο και οι δραστηριότητες του ανθρώπου σε αυτόν τον κόσμο. Ανά πάσα στιγμή μπορεί να εμφανιστεί κάποιος και επιδιώκοντας τα δικά του συμφέροντα μπορεί να γίνει προδότης. Υπό αυτές τις συνθήκες, ο οποιοσδήποτε αμυντικός μηχανισμός προστασίας μπορεί να αποδειχθεί ανεπαρκής.

3.1. Ορισμός της εσωτερικής απειλής (Internal attacker ή Insider).

Οι χρήστες ενός συστήματος, που μπορεί να έχουν προθέσεις αλλά και στόχους που εναντιώνονται με αυτούς του οργανισμού που κατέχει το σύστημα, αποτελούν απειλή. Ένας τέτοιος χρήστης είναι ένας πιθανός εσωτερικός εισβολέας του συστήματος που εμπίπτει σε μία από τις ακόλουθες κατηγορίες [6] [7]:

- ***Προδότης (Traitor).*** Εξουσιοδοτημένος χρήστης με συγκεκριμένα δικαιώματα χρήσης ενός συστήματος που εκμεταλλεύεται τα δικαιώματά του για την επίτευξη των στόχων του και παραβιάζει την ασφάλεια του συστήματος, επηρεάζοντας την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πόρων του.

- ***Μεταμφιεσμένος (Masquerader).*** Κλέβει την ταυτότητα κάποιου άλλου χρήστη και προσποιούμενος ότι κάποιος νόμιμος χρήστης ενεργεί, προκαλεί ζημιά.

Ποιος τελικά είναι *«εκ των έσω»;*

Ο ορισμός μιας εσωτερικής απειλής δεν είναι καλά εδραιωμένος, υπάρχουν διάφορες πιθανές χρήσεις του όρου [8] [9].

Ένας πληροφοριοδότης / προδότης μπορεί να είναι:

- Υπάλληλος, φοιτητής ή άλλο μέλος ιδρύματος, που διαχειρίζεται συστήματα υπολογιστών στα οποία έχει νόμιμη πρόσβαση.
- Συνεργάτης, εργολάβος, προμηθευτής, τεχνικός συντήρησης υπολογιστών, επισκέπτης ή κάποιος άλλος, που έχει επίσημη ή άτυπη επιχειρηματική σχέση με το ίδρυμα.
- Οποιοσδήποτε ταυτοποιήθηκε και πιστοποιήθηκε σωστά στο σύστημα, συμπεριλαμβανομένου, ίσως κάποιου που μεταμφιέζεται σε νόμιμο πληροφοριοδότη ή κάποιου στον οποίο έχει δώσει πρόσβαση ένας εκ των έσω (για παράδειγμα, με την κοινή χρήση λογαριασμού πρόσβασης).
- Κάποιος εξαπατήθηκε ή εξαναγκάστηκε από εξωτερική οντότητα να εκτελέσει ενέργειες για λογαριασμό του.
- Ένας πρώην υπάλληλος ο οποίος χρησιμοποιεί διαπιστευτήρια πρόσβασης που δεν ανακλήθηκαν με την λήξη της συνεργασίας του ή χρησιμοποιώντας διαπιστευτήρια πρόσβασης που δημιουργήθηκαν κρυφά, ενώ ένας εσωτερικός χρήστης έδωσε πρόσβαση αργότερα.

Αυτό το μάλλον ευρύ φάσμα ερμηνειών του όρου μιας εσωτερικής απειλής προσδιορίζει αλλά και επισημαίνει κάποιες από τις περιπτώσεις που κάποιος μπορεί να είναι εν δυνάμει πληροφοριοδότης / προδότης και χρήζει ιδιαίτερης προσοχής.

3.2. Κίνητρα.

Τα κίνητρα για μια εσωτερική επίθεση είναι διαφορετικά σε κάθε περίπτωση. Στην πραγματικότητα, ο όρος "επίθεση" μπορεί να είναι υπερβολικός για ορισμένους τύπους εσωτερικών απειλών / ενεργειών [8] [9]:

- Κάνοντας π.χ. ένα ακούσιο λάθος.
- Προσπαθώντας κάποιος χρήστης να επέμβει στο σύστημα, ώστε να κάνει κάτι για το οποίο δεν σχεδιάστηκε και να γίνει το σύστημα πιο χρήσιμο.
- Προσπαθώντας χωρίς δόλο ένας χρήστης να κάνει κάτι πέρα από το εξουσιοδοτημένο όριο, χωρίς να γνωρίζει ότι η ενέργεια αυτή είναι μη εξουσιοδοτημένη.
- Να γίνει έλεγχος του συστήματος για αδυναμίες, ευπάθειες ή σφάλματα, με σκοπό την αναφορά προβλημάτων και ενημέρωση του οργανισμού από κάποιο αναρμόδιο χρήστη.
- Δοκιμή των ορίων του συστήματος για αδυναμίες, προκαλώντας άθελα κάποια βλάβη στα πληροφοριακά συστήματα.
- Αντιμετωπίζοντας το σύστημα ως ένα παιχνίδι προσπαθώντας χωρίς ιδιαίτερο σκοπό, να ξεγελάσει τα συστήματα ασφαλείας.
- Άσκοπη περιήγηση και προβολή, ανάγνωση, επεξεργασία δεδομένων.

Προφανώς και πρέπει να αντιμετωπίζεται διαφορετικά κάθε περίπτωση ανάλογα τα κίνητρα και είναι λάθος να κατατάξουμε ως «κακόβουλο» ή «εσωτερικά επιτιθέμενο» κάποιον εργαζόμενο, που θέλει να κάνει καλύτερα και πιο γρήγορα τη δουλειά του από κάποιον που πραγματικά έχει κακόβουλη πρόθεση. Τα ακούσια σφάλματα θεωρούνται συνήθως ως ατυχή αλλά και πολλές φορές αναπόφευκτα, παρόλα αυτά δεν παύουν να αποτελούν σοβαρή απειλή για έναν οργανισμό και πρέπει να αντιμετωπίζονται με την ίδια σοβαρότητα και προσοχή όσο και μία κακόβουλη κίνηση. Η περιοχή μεταξύ αυτών των δύο άκρων δυστυχώς είναι δυσδιάκριτη και γκρίζα. Έτσι μια δεδομένη ενέργεια μπορεί να χαρακτηριστεί ως “επίθεση εκ των έσω” σε μια περίπτωση αλλά όχι σε μια άλλη, γεγονός που περιπλέκει την αξιολόγηση της σοβαρότητας και της συχνότητας των “εσωτερικών επιθέσεων”.

Οι περιπτώσεις που κάποιος είναι κακοπροαίρετος και αποτελεί πραγματική απειλή για ένα οργανισμό είναι για παράδειγμα, όταν ένας εργαζόμενος είναι δυσαρεστημένος, ή απογοητευμένος, ή μετά από μια σύγκρουση με τον εργοδότη ή είναι εκ φύσεως ανέντιμος. Άλλες περιπτώσεις περιλαμβάνουν έναν απολυθέντα υπάλληλο, όπου η απογοήτευση και η ανεργία μπορεί να τον στρέψουν εναντίων του οργανισμού, ή έναν συνταξιούχο, που θέλει να εκδικηθεί για αδικίες που είχε υποστεί. Ο κατάλογος επεκτείνεται ανάλογα με το μέγεθος, τη δομή και την κατάσταση του οργανισμού, όπου πιθανόν εμπλέκονται εξωτερικοί συνεργάτες, ελεγκτές, σύμβουλοι, πελάτες, προμηθευτές, τεχνικοί κ.τ.λ. που ενδέχεται να έχουν πρόσβαση στα συστήματα. Επίσης, όταν ένας οργανισμός προσλαμβάνει υπαλλήλους και συνεργάτες μερικής απασχόλησης για σύντομες περιόδους και πολλές φορές με αυξημένα δικαιώματα πρόσβασης, οι οποίοι αργότερα σαν εξωτερικές οντότητες συνεχίζουν να αλληλοεπιδρούν κακόβουλα με τον οργανισμό όπου ενδέχεται να έχουν αντικρουόμενα συμφέροντα με την εταιρία δίνοντας στοιχεία ή έχοντας προσληφθεί από ανταγωνιστές.

Μολονότι ο κατάλογος των εν λόγω εμπλεκόμενων μερών είναι μακρύς, υπάρχει ένας μικρός αριθμός κοινών χαρακτηριστικών μεταξύ τους. Για παράδειγμα η πρόθεση τους να βλάψουν το σύστημα προκαλώντας ζημία, να αυξήσουν το ατομικό τους κέρδος και σε ορισμένες περιπτώσεις μόνο να εκδικηθούν.

Επειδή η λέξη "απειλή" έχει αρνητικό αντίκτυπο, εύλογα δεν πρέπει να χρησιμοποιηθεί για να περιγράψει ακούσια ή μη κακόβουλη συμπεριφορά. Πρέπει να είμαστε ιδιαίτερα προσεκτικοί, όταν χρησιμοποιούμε τον όρο "εσωτερική απειλή" και να βεβαιωθούμε, ότι το νόημά της δεν παρερμηνεύεται.

3.3. Ψυχολογία και εσωτερικά επιτιθέμενοι.

Ορισμένοι ερευνητές αμφισβητούν την απόλυτη χρησιμότητα μόνο τεχνολογικών προσεγγίσεων του προβλήματος, λέγοντας ότι «το βασικό στοιχείο της εσωτερικής απειλής είναι ο άνθρωπος, ως δράστης, που έχει καταχραστεί μια θέση εμπιστοσύνης» [10].

Έρευνες που προέρχονται από τις κοινωνικές επιστήμες, κοινωνιολογία, ψυχολογία, εγκληματολογία, έχουν εξετάσει τα χαρακτηριστικά των προσώπων που κατέχουν εμπιστευτικές πληροφορίες, προσπαθώντας να κατανοήσουν τα κίνητρα μιας εν δυνάμει επίθεσης. Αναλύοντας ψυχολογικά προφίλ προσώπων που κατέχουν εμπιστευτικές πληροφορίες, σε συνδυασμό με μελέτες περιπτώσεων και συνεντεύξεις ατόμων που έχουν κατηγορηθεί για κατασκοπεία ή δολιοφθορά, συλλέγονται ευρήματα που αποκαλύπτουν συμπεριφορές, κίνητρα και διαταραχές προσωπικότητας που συνδέονται με εγκλήματα εσωτερικών επιθέσεων. Γίνονται επίσης προσπάθειες, για την ανάπτυξη προγνωστικών μοντέλων που συσχετίζουν ψυχολογικά προφίλ ή συμπεριφορές και προδιαθέσεις με ακατάλληλες αντιδράσεις. Επίσης, καταστάσεις άγχους, οικονομικές δυσκολίες, δυσαρέσκεια, μπορεί να οδηγήσουν σε προσωπικές συγκρούσεις, απόκρυψη παραβιάσεων κανόνων και ισχυρές αντιδράσεις σε χώρους εργασίας. Απαριθμούνται μεταξύ άλλων πέντε ψυχοκοινωνικοί δείκτες [9] [11], που θεωρούνται ενδείξεις ότι ένα άτομο είναι δυνητικά κακόβουλος πληροφοριοδότης:

- Δυσαρέσκεια.
- Αποδοχή / ανοχή αρνητικών σχολίων.
- Διαχείριση θυμού.
- Περιφρόνηση της εξουσίας.
- Ζητήματα επιδόσεων.

Μια σημαντική διαπίστωση είναι ότι κάποια περίπτωση αξίζει να εξεταστεί μόνο εάν ο εργαζόμενος παρουσιάζει σοβαρές ή εξαιρετικά σοβαρές εκδηλώσεις κάποιων εκ των δεικτών. Επιπλέον και στον χώρο της ποινικής δικαιοσύνης, ερευνώνται προφίλ προβληματικής οντότητας, ενώ στον εγκληματολογικό τομέα είναι δυσκολότερος ο εντοπισμός προφίλ κακόβουλων προθέσεων εκ των προτέρων. Φαίνεται ότι τα εγκληματολογικά προφίλ ποικίλλουν ως προς τα κίνητρα και την ψυχολογική τους σύνθεση. Μπορούν να αναγνωριστούν κάποιες πολύ αντικοινωνικές προσωπικότητες, αλλά άλλοι εγκληματίες διαφεύγουν της εκ των προτέρων ανίχνευσης, πιθανότατα λόγο ψευδώς θετικών στοιχείων που παρεμποδίζουν αυτές τις προσπάθειες [10].

Ένας ψυχολογικός έλεγχος θα ήταν ιδανικός πριν προσληφθεί κάποιος υπάλληλος. Μια τυπική συνέντευξη εργασίας όμως, δεν αρκεί για την αξιολόγηση τέτοιων διαταραχών προσωπικότητας και κινήτρων. Επιπροσθέτως, σε έναν οργανισμό το προσωπικό ανθρώπινου δυναμικού συνήθως δεν είναι σε θέση να διαχειριστεί τέτοιες καταστάσεις, επειδή σε έναν τυπικό οργανισμό δεν απαιτούνται ψυχολογικές εξετάσεις ή τεστ ανάλυσης προσωπικότητας πριν από μια πρόσληψη. Μια άλλη πρόκληση είναι ότι καμία μελέτη δεν αξιολογεί και δεν συγκρίνει την ανάλυση τέτοιων προδιαθέσεων "εσωτερικής απειλής" και τα ποσοστά εμφάνισης στο συνολικό πληθυσμό των εργαζομένων. Έτσι, απουσιάζει ένας μηχανισμός ή διαδικασία εντοπισμού ενός πιθανά εσωτερικού επιτιθέμενου πριν επιτεθεί και ιδανικά πριν προσληφθεί.

3.4. Κακόβουλες δράσεις και επιδράσεις των κακόβουλων ενεργειών.

Ένας υπάλληλος εάν είναι κακόβουλος εξετάζει τους τρόπους με τους οποίους μπορεί να δράσει και σχεδιάζει, πως μπορεί να επιτεθεί στο σύστημα για τους δικούς του σκοπούς. Αρχικά, δρα σύμφωνα με τις δεσμεύσεις των συστημάτων ασφαλείας και τα καθήκοντά του, ενεργεί επίσης συστηματικά για να προετοιμάσει τις επιθέσεις, οι οποίες μπορούν να χαρακτηριστούν ως ενέργειες πριν ή και κατά της φάσης επίθεσης. Κάποιος που θέλει να κλέψει πληροφορίες ή να βλάψει μια εταιρία δεν είναι απαραίτητα έμπειρος χρήστης ή γνώστης πληροφορικής. Αντίθετα, μπορεί να είναι π.χ. διοικητικός υπάλληλος, οικονομολόγος, αποθηκάριος, φύλακας, εργαζόμενος παραγωγής έως και διευθυντικό στέλεχος. Άλλωστε σήμερα, με την εξέλιξη της τεχνολογίας το έγκλημα εκ των έσω δεν απαιτεί καν εξιδεικευμένες γνώσεις και σχετικά εύκολα πληροφορίες μπορούν να μεταφερθούν χρησιμοποιώντας απλά μέσα, όπως εξωτερικές μονάδες αποθήκευσης, χρήση ηλεκτρονικού ταχυδρομείου και άλλα σύγχρονα εργαλεία τεχνολογίας πληροφοριών. Σε αντίθεση με παλαιότερες εποχές, όπου ο εκάστοτε πληροφοριοδότης έπρεπε να έχει την απαιτούμενη γνώση, άμεση πρόσβαση στις πληροφορίες που έπρεπε να διαρρεύσουν, φυσική πρόσβαση στον παραλήπτη των πληροφοριών και ένα φυσικό

αντίγραφο των πληροφοριών που έπρεπε να δοθεί. Σε σύγκριση π.χ. με τις υποθέσεις του WikiLeaks, ακόμη και πριν από είκοσι χρόνια θα ήταν απαραίτητο να χρησιμοποιηθεί ένα φορτηγό, για να μεταφερθούν τα εκατοντάδες χιλιάδες έγγραφα που εμπλέκονται σε κάθε υπόθεση.

Αναφέροντας το πόρισμα μιας μελέτης που διεξήχθη στον χρηματοπιστωτικό τομέα, σχετικά με τη δραστηριότητα των εσωτερικών απειλών αποκαλύφθηκε ότι [6] [12]:

- Τα περισσότερα περιστατικά απαιτούσαν μικρή τεχνική εξειδίκευση.
- Οι πληροφοριοδότες προγραμμάτισαν τις ενέργειές τους εκ των προτέρων.
- Τα κίνητρά τους είχαν κυρίως οικονομικό όφελος.
- Δεν είχαν κοινό προφίλ.
- Εντοπίστηκαν με διάφορες μεθόδους και από μια σειρά ανθρώπων, όχι μόνο από το προσωπικό ασφαλείας.
- Η απώλεια του οργανισμού ήταν κυρίως οικονομική.
- Οι πληροφοριοδότες έδρασαν κατά τη διάρκεια των κανονικών ωρών εργασίας.

Παρόλα αυτά, είναι δύσκολο να ανιχνευθούν οι κινήσεις των επιτιθέμενων κυρίως λόγω των προνομίων τους που τους προστατεύουν εν μέρει από το να αποκαλυφθούν. Μια τέτοια προσπάθεια δημιουργεί συνήθως ένα μεγάλο αριθμό ψευδώς θετικών αλλά και ένα σημαντικό αριθμό ψευδώς αρνητικών συναγερμών.

Ένας τρόπος για να αναλυθεί η εσωτερική απειλή είναι να εξεταστεί η επίδραση που είχαν οι ενέργειες τους, κάποιες από τις οποίες είναι [8]:

1. Η διάθεση δεδομένων ή αυξημένων υπηρεσιών υπολογιστή σε άτομα που διαφορετικά δεν θα τα είχαν, είτε επειδή τα άτομα δεν είχαν εξουσιοδοτηθεί είτε επειδή το σύστημα απέτυχε να τα αποδώσει όπως αναμενόταν.
2. Λήψη δεδομένων για τα οποία ο χρήστης δεν έχει εξουσιοδοτηθεί, επειδή τα δεδομένα αυτά δεν συμπεριλαμβάνονται στις απαιτήσεις εργασίας του χρήστη.
3. Απόκτηση δεδομένων ή υπηρεσιών για δόλιους σκοπούς.

Στην πρώτη περίπτωση θα μπορούσε μερικές φορές να θεωρηθεί ως μη επιβλαβής επίδραση, γιατί μπορεί να αξιολογηθεί ως τυχαίο γεγονός, ενώ η τελευταία περίπτωση έχει συνήθως αρνητικές επιπτώσεις. Η δεύτερη περίπτωση δεν είναι ξεκάθαρη, εξαρτάται από την επόμενη κίνηση του χρήστη και έτσι μπορεί να θεωρηθεί ανάλογα από θετικό έως και αρνητικό συμβάν. Έτσι αυξάνεται η πολυπλοκότητα και η δυσκολία σε ένα μηχανισμό ανίχνευσης, ώστε να ενεργοποιηθεί ή όχι σωστά και πρέπει να μπορεί να αξιολογεί περιπτώσεις όταν συμβαίνουν κακόβουλες ενέργειες, παρόλο που δεν γίνεται υπέρβαση των προνομίων του συστήματος. Ωστόσο, είναι καλή τακτική να παρακολουθούνται ύποπτες ενέργειες και κάθε φορά που παραβιάζεται μια πολιτική ασφαλείας, τα συστήματα άμυνας να μπορούν να αντιδράσουν και να απαγορεύσουν τέτοιες αποκλίσεις [7] [9]. Ένας εκ των έσω μπορεί να έχει νόμιμα δικαιώματα πρόσβασης σε αρκετές πληροφορίες του οργανισμού του ακόμα και διαβαθμισμένες, όπου θα μπορούσε να τις αποκαλύψει προκειμένου να λάβει άλλες πληροφορίες, που είναι απαραίτητες για να ολοκληρώσει μια επίθεση. Επιπλέον, οι επιθέσεις *κοινωνικής μηχανικής*[2] *(Social engineering)* θα μπορούσαν να συμπεριληφθούν σε αυτήν την κατηγορία, όταν παραδείγματος χάριν ένας υπάλληλος επιτυγχάνει να λάβει πολύτιμες πληροφορίες από έναν μη υποψιασμένο συνεργάτη του.

Οι επιδράσεις των κακόβουλων ενεργειών, εξαρτώνται από τις συνέπειες και την έκταση του προβλήματος που δημιουργείται από αυτές. Ως εκ τούτου, η ανίχνευση διαρροής εμπιστευτικών πληροφοριών γίνεται όλο και πιο απαιτητική, δυστυχώς όμως μερικές φορές χωρίς ικανοποιητικά ευρήματα.

[2] ***Κοινωνική μηχανική*** (Social engineering): είναι η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών. Αν και είναι παρόμοια με το τέχνασμα ή την απλή απάτη, ο όρος είναι κυρίως συνδεδεμένος με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα.

3.5. Έλεγχος, παρακολούθηση και εγκληματολογία.

Οι παρατηρήσεις σχετικά με την παρακολούθηση των συστημάτων ή ύποπτων συμπεριφορών μπορεί να είναι χρήσιμες, για παράδειγμα χρησιμοποιώντας την ανθρώπινη λογική για να προβλεφθούν νέες πιθανές επιθέσεις. Στις περισσότερες περιπτώσεις, κάποιος τρίτος γνώριζε για τις κακόβουλες ενέργειες εσωτερικής απειλής που συνέβησαν. Επομένως είναι σημαντικό να βρεθούν τρόποι ενθάρρυνσης αναφοράς οποιασδήποτε "ύποπτης δραστηριότητας" από τρίτους.

Η αναζήτηση ύποπτης συμπεριφοράς από εσωτερικούς συνεργάτες είναι χρήσιμη, αλλά είναι δύσκολο να εφαρμοστεί συστηματικά. Κάποια πρότυπα περίεργης συμπεριφοράς, που είναι ανησυχητικά και χρειάζονται ιδιαίτερη προσοχή, περιλαμβάνουν [9]:

- Ασυνήθιστα μεγάλη δραστηριότητα στον κυβερνοχώρο, μη φυσιολογικές αναζητήσεις, κινήσεις και εμφάνιση σε χώρους και τμήματα άλλων υπηρεσιών όπως αποθήκες, servers rooms κ.τ.λ.
- Υπερβολικός ζήλος ή υπέρμετρη προσφορά βοήθειας συναδέλφων σε θέματα υπολογιστών π.χ. για μεταφορά αρχείων, αποστολή emails κ.τ.λ. ενώ δεν είναι της αρμοδιότητάς τους, είναι ανησυχητικό και χρειάζεται ιδιαίτερη προσοχή και περαιτέρω ανάλυση.

Ένα σημαντικό ερώτημα που τέθηκε σχετικά με την παρακολούθηση [13] για τον εντοπισμό ακατάλληλης συμπεριφοράς είναι κατά πόσο η παρακολούθηση είναι αποτελεσματική και χρήσιμη για την επιβεβαίωση μιας πιθανής περίπτωσης εσωτερικής επίθεσης. Υπάρχει διαμάχη ως προς το κατά πόσον η παρακολούθηση λειτουργεί αποτρεπτικά, δηλαδή εάν οι υπάλληλοι γνωρίζουν ότι η δραστηριότητά τους παρακολουθείται πόσο πιθανό είναι να εμπλακούν σε ακατάλληλη δραστηριότητα. Η απάντηση σε αυτό είναι άγνωστη, γιατί η παρακολούθηση δείχνει να μην είναι αποτελεσματική για την αποτροπή κλοπής ούτε σε μικρά εμπορικά καταστήματα από τους ίδιους τους υπαλλήλους για παράδειγμα.

Επίσης, η παρακολούθηση μπορεί να βοηθήσει στην ανίχνευση παραβιάσεων πρόσβασης, όμως επιδεινώνει δυνητικά σχέσεις εμπιστοσύνης και συμπεριφοράς και σε πολλές περιπτώσεις το προσωπικό δυσανασχετεί.

Ο αποφασιστικός παράγοντας είναι μέσα σε ποια πλαίσια η παρακολούθηση είναι αποδεκτή, τόσο ηθικά όσο και νομικά. Το ερώτημα αυτό τίθεται σε όλα τα επίπεδα από μεμονωμένους χρήστες, ομάδες, εταιρείες, διάφορα κοινωνικά σύνολα και στις περισσότερες περιπτώσεις δεν υπάρχει συμφωνία ως προς το τι είναι "αποδεκτό".

Η ευαισθητοποίηση του προσωπικού σχετικά με την ασφάλεια θα πρέπει να θεωρείται βασική προϋπόθεση για μια σωστή εσωτερική στρατηγική. Ακολουθούν τρία σημεία ευαισθητοποίησης των χρηστών [14]:

1. ***Αντίληψη:*** Ο χρήστης να είναι σε θέση να ανιχνεύει πιθανές απειλές στο περιβάλλον.
2. ***Κατανόηση:*** Ο χρήστης πρέπει να είναι σε θέση να συνδυάζει πληροφορίες από διαφορετικούς παράγοντες, να τις ερμηνεύει και να χρησιμοποιήσει τα ευρήματα για να μειώσει τον κίνδυνο στο περιβάλλον.
3. ***Πρόβλεψη:*** Ο χρήστης πρέπει να είναι σε θέση να προβλέπει μελλοντικές επιθέσεις και να αλλάζει προληπτικά τη συμπεριφορά του για να μειώσει ή να αποφύγει τον κίνδυνο.

Ο τομέας της εγκληματολογίας επίσης μπορεί να βοηθήσει στην κατανόηση των εσωτερικών απειλών. Στην εγκληματολογία υπάρχουν διάφορες θεωρίες σχετιζόμενες με εσωτερικές απειλές. Προηγούμενες θεωρίες αποτροπής και κοινωνικής μάθησης έχουν ενσωματωθεί σε θεωρίες προβλέψιμης συμπεριφοράς. Για να διαπραχθεί ένα έγκλημα, πρέπει να υπάρχει ισχυρό κίνητρο και να δοθεί τουλάχιστον μία ευκαιρία στον επιτιθέμενο να το διαπράξει. Εάν η πιθανότητα τιμωρίας είναι υψηλή και οι κυρώσεις αυστηρές, πιθανοί εγκληματίες θα αποθαρρυνθούν να διαπράξουν κάτι παράνομο, ειδικά όταν τα κίνητρά τους είναι αδύναμα. Ο στόχος πρόληψης και αποτροπής ενός εγκλήματος πριν αυτό γίνει είναι να καταφέρει [9] [15]:

- Να κάνει την εγκληματική πράξη να φαίνεται πιο δύσκολη.
- Να καταστήσει την εγκληματική πράξη πιο επικίνδυνη.
- Να μειώσει το όφελος που αναμένει να ανακτήσει ένας εν δυνάμει εγκληματίας.
- Να ελαχιστοποιηθούν τυχόν δικαιολογίες και άλλοθι που μπορεί να είναι διαθέσιμα στον πιθανό κακοποιό.

Η απειλή διαρροής εμπιστευτικών πληροφοριών έχει αναγνωριστεί ως ένα από τα πιο δύσκολα προβλήματα. Η παρακολούθηση ύποπτων συμπεριφορών και κινήσεων μπορεί να αποδειχθεί πολύτιμη για την πρόληψη και την αποτροπή μιας κακόβουλης ενέργειας πριν αυτή συμβεί. Αντιθέτως, η αντιμετώπιση του προβλήματος μέσω εγκληματολογικής ανάλυσης πραγματοποιείται μόνο μετά τις ενέργειες επίθεσης.

3.6. Τεχνολογική και Κοινωνιολογική προσέγγιση.

Κάθε οργανισμός είναι διαφορετικός μόνο και μόνο επειδή το προσωπικό που τον αποτελεί είναι διαφορετικό. Έτσι και η εσωτερική απειλή δεν είναι ένα μεμονωμένο πρόβλημα, αλλά συνδυασμός πολλών παραγόντων. Οι διάφορες προσεγγίσεις που αναπτύχθηκαν απεικονίζουν το εύρος αλλά και τους τρόπους με τους οποίους οι εσωτερικές επιθέσεις και απειλές ποικίλλουν μεταξύ τους [9] [11].

Οι αμιγώς ***τεχνικές προσεγγίσεις*** επιδιώκουν να καθορίσουν τον έλεγχο πρόσβασης, να παρακολουθούν τις ακολουθίες εντολών και άλλα μετρήσιμα μεγέθη, ώστε να “σκληρύνουν” όσο γίνεται τα συστήματα ή τις δομές δικτύων, με στόχο να αποτρέψουν τυχαίες ή κακόβουλες δραστηριότητες.

Εργασίες στις ***κοινωνικές επιστήμες*** χρησιμοποιούν προσεγγίσεις από την ψυχολογία, την οργανωτική συμπεριφορά και την κοινωνιολογία για να οριοθετήσουν τα κίνητρα των εσωτερικών απειλών, ώστε να προσπαθήσουν να προβλέψουν εσωτερικές επιθέσεις. Οι κοινωνικοτεχνικές προσεγγίσεις συνδυάζουν στοιχεία και των δύο προοπτικών. Αυτός ο διαχωρισμός των τεχνολογικών και κοινωνιολογικών προσεγγίσεων είναι σημαντικός για την ασφάλεια γενικά και ειδικά για τις εσωτερικές απειλές, όπου επιτρέπει το διαχωρισμό των τεχνικών μέσων για την εκτέλεση ή και τον μετριασμό μιας επίθεσης από τα κοινωνιολογικά μέσα που προσπαθούν να εξηγήσουν τα κίνητρα των “εκ των έσω”.

Η μοντελοποίηση της ανθρώπινης συμπεριφοράς είναι σχεδόν αδύνατη, πόσο μάλλον η μοντελοποίηση του τρόπου επίθεσης, ο οποίος εξαρτάται από εξωτερικούς και εσωτερικούς παράγοντες [9] [11]

Κατά συνέπεια, καμία προσέγγιση δεν έχει προσφέρει μέχρι στιγμής ικανοποιητικά αποτελέσματα προς την εύρεση λύσης και αυτό που περιπλέκει ακόμη περισσότερο την κατάσταση είναι, ότι ο πληροφοριοδότης έχει ήδη πρόσβαση μέσα στο σύστημα με κάποιο τρόπο. Σε εποχές όπου οι περισσότερες επιθέσεις πραγματοποιούνται χρησιμοποιώντας υποδομή πληροφορικής και διαδικτύου η διάκριση, μεταξύ προσώπων που κατέχουν εμπιστευτικές πληροφορίες και εξωτερικών οντοτήτων γίνεται όλο και λιγότερο ορατή. Ακόμη χειρότερα όταν οι κακόβουλες δραστηριότητες γίνονται με συνεργασία εσωτερικών και εξωτερικών οντοτήτων.

4. Εντοπισμός Επιθέσεων.

Οι εσωτερικές επιθέσεις είναι δύσκολο να εντοπιστούν, είτε με ανθρώπινα είτε με τεχνικά μέσα. Έχει παρατηρηθεί, ότι οι περισσότερες εσωτερικές επιθέσεις εντοπίζονται γιατί ο δράστης μπορεί να μίλησε σε κάποιον και “υπερηφανεύτηκε” για την πράξη του. Επίσης, σε πολλά ήδη εγκλήματος οι ανακριτές της αστυνομίας μερικές φορές επωφελούνται από έναν τέτοιο δράστη που κάνει κάτι για να τραβήξει την προσοχή. Ένα εργαλείο αναγνώρισης επίθεσης εκ των έσω θα ήταν χρήσιμο για την επισήμανση επιθέσεων ή ύποπτης συμπεριφοράς εγκαίρως για τον περιορισμό συνεπειών. Είναι σαφές, ότι οι περισσότερες δραστηριότητες εκ των έσω δεν είναι απαραίτητα κακόβουλες. Έτσι, ο όγκος δεδομένων της φυσιολογικής δραστηριότητας εμπιστευτικών πληροφοριών υπερβαίνει κατά πολύ αυτόν της κακόβουλης δραστηριότητας και ένας τέτοιος όγκος δεδομένων είναι δύσκολο να αναλυθεί. Το ίδιο ισχύει για παράδειγμα σε ένα σύστημα ανίχνευσης που προστατεύει από κακόβουλη πρόσβαση ένα δίκτυο. Το μεγαλύτερο μέρος κυκλοφορίας ενός δικτύου είναι καλοήθης. Ωστόσο, για αυτού του είδους τις επιθέσεις, το σύστημα ανίχνευσης εισβολής πρέπει να συλλέγει και να συσχετίζει δεδομένα ελέγχοντας συνεχώς το δίκτυο αδιάληπτα. Οι εσωτερικά επιτιθέμενοι πιθανώς θα εκτελέσουν τόσο κανονικές όσο και κακόβουλες πράξεις, γεγονός που περιπλέκει την αναζήτηση ανώμαλης συμπεριφοράς.

Η υπεράσπιση από εσωτερικές επιθέσεις είναι και θα παραμείνει δύσκολη. Ως επί το πλείστων, οι παραδοσιακές άμυνες ασφαλείας υπολογιστών δεν επαρκούν. Θα χρειαστεί ένας συνδυασμός πραγμάτων, όπως τεχνικές άμυνας, συστήματα ανίχνευσης εισβολών, διαδικασίες και πολλά άλλα για την παροχή ουσιαστικής προστασίας.

4.1. Ανίχνευση εισβολών στην ασφάλεια της πληροφορίας.

Ανίχνευση εισβολής είναι η παρακολούθηση των συμβάντων ενός συστήματος και η απόφαση για το αν ένα συμβάν είναι φυσιολογικό (normal) ή μη [7] [16].

> Ως ***φυσιολογικό*** ορίζεται κάθε συμβάν που είναι συνεπές με τις πολιτικές ασφαλείας που εφαρμόζονται στο σύστημα.
>
> ***Μη φυσιολογικό*** ορίζεται οποιοδήποτε γεγονός απειλεί την κατάσταση ασφαλείας του συστήματος.

Υπάρχει ανάγκη για ένα σύστημα ανίχνευσης εισβολών, που να μπορεί να παρέχει προστασία σε ένα σύστημα υπολογιστή εντοπίζοντας παραβιάσεις ασφαλείας σε πραγματικό χρόνο. Οι μηχανισμοί για αυτοματοποιημένη ανάλυση συμβάντων ασφαλείας, δικτύων, δεδομένων, διατηρώντας και ελέγχοντας αρχεία καταγραφής ονομάζονται ***Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDSs)*** και πρέπει να καλύπτουν τους ακόλουθους στόχους [7] [17]:

- Να παρέχουν ίχνος συμβάντων του συστήματος υπολογιστών.
- Να προσδιορίζουν τον τρόπο παραβίασης του συστήματος.
- Να εντοπίζουν και να αποτρέπουν μια επίθεση πριν από την ολοκλήρωσή της σε πραγματικό χρόνο.
- Να καθορίζουν ποιος ευθύνεται για την παράβαση.
- Να λαμβάνουν μέτρα για την πρόληψη περαιτέρω παραβιάσεων.

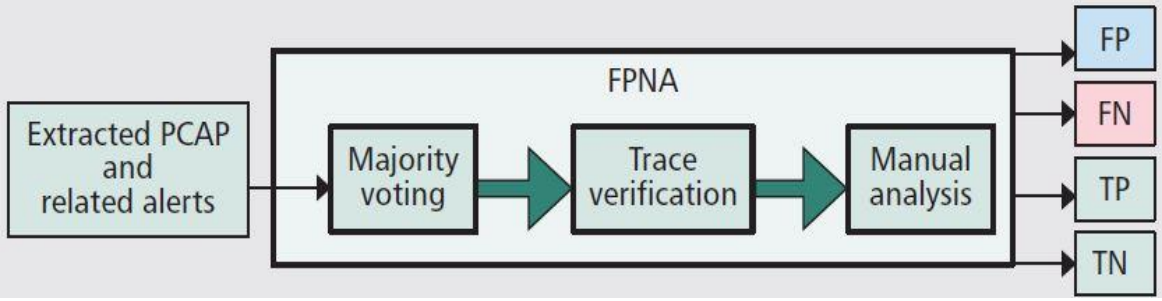
Σε ένα σύστημα IDS υπάρχουν τρεις τρόποι υλοποίησης της μεθόδου που χρησιμοποιείται για την ανίχνευση εισβολών [7]:

1. *Ανίχνευση ανωμαλιών (Anomaly detection – Behavior-based)*
2. *Ανίχνευση κακής χρήσης (Misuse detection ή Signature-based detection).*
3. *Ανίχνευση βάση προδιαγραφών (Specification-based detection).*

Η μεγάλη πλειοψηφία των προϊόντων είναι υβριδικά συστήματα που ενσωματώνουν τουλάχιστον δύο τεχνικές ανίχνευσης γιατί η κάλυψη μόνο από μία έχει αποδειχθεί ανεπαρκής.

4.2. Ταξινόμηση συμβάντων.

Τα γεγονότα που λαμβάνουν χώρα σε ένα σύστημα είναι επιθέσεις και φυσιολογικά συμβάντα αναμεμειγμένα. Ένα μέρος αυτών των επιθέσεων θα ανιχνευθεί σωστά από ένα IDS, ενώ τα υπόλοιπα όχι. Ομοίως, ένα IDS θα χαρακτηρίσει ορισμένα από τα φυσιολογικά γεγονότα ως επιθέσεις και θα τα απορρίψει προκαλώντας έτσι ψευδείς συναγερμούς. Το ακόλουθο σχήμα, απεικονίζει όλες τις διαδικασίες ελέγχου συμβάντων, μέχρι την τελική ταξινόμηση τους που επιτυγχάνει ένα IDS.



Εικόνα 4.2: *Έλεγχος και ταξινόμηση συμβάντων* [16].

Στις περιπτώσεις πραγματικών επιθέσεων το σύστημα είναι σε θέση να ανιχνεύσει μια σειρά από καταστάσεις [7] [16] [18]:

- Κάποιες επιθέσεις θα ανιχνευτούν σωστά. ***Αληθώς θετικοί συναγερμοί (True Positive Alarms).***
- Θα υπάρξουν επιθέσεις που δυστυχώς δεν θα ανιχνευτούν. ***Ψευδώς αρνητικοί συναγερμοί (False Negative Alarms).***

Ο αριθμός των πραγματικών επιθέσεων δεν είναι γνωστός για ένα σύστημα. Οι ψευδώς αρνητικοί συναγερμοί, είναι επίσης απροσδιόριστοι. Τα συμβάντα που ανιχνεύονται ως επιθέσεις απαιτούν περαιτέρω ταξινόμηση, ίσως με ανθρώπινη παρέμβαση [16], για να γίνει διάκριση μεταξύ των εντοπισμένων πραγματικών επιθέσεων και των ψευδώς θετικών συναγερμών.

Στις περιπτώσεις κανονικών συμβάντων ανιχνεύονται καταστάσεις όπως [7] [16] [18]:

- ***Ψευδώς θετικοί συναγερμοί (False Positive Alarms)*** για κανονικά συμβάντα που εντοπίστηκαν ως επιθέσεις.
- Και φυσιολογικά γεγονότα. ***Αληθώς αρνητικοί συναγερμοί (True Negative Alarms).***

Ο υπολογισμός του ποσοστού επιτυχούς ανίχνευσης σε ένα IDS είναι περίπλοκος, επειδή ο αριθμός των πραγματικών επιθέσεων δεν είναι γνωστός για ένα σύστημα. Αυτό σημαίνει ότι τα συστήματα και οι διαχειριστές συστημάτων γνωρίζουν ένα μέρος των επιθέσεων που λαμβάνουν χώρα και όχι όλες. Ως αποτέλεσμα, η αξιοπιστία και η ακρίβεια ανίχνευσης ενός IDS μπορεί να υπολογιστεί σε φάση δοκιμής χρησιμοποιώντας δεδομένα εκπαίδευσης και όχι πραγματικά γεγονότα.

Πιο αναλυτικά [7] [18]:

Αξιοπιστία: Ένα IDS είναι αξιόπιστο εάν ο αριθμός των εντοπισμένων πραγματικών επιθέσεων είναι ίσος με τον συνολικό αριθμό επιθέσεων που πραγματοποιούνται σε ένα σύστημα. Η αξιοπιστία ενός IDS ορίζεται ως ο λόγος του αριθμού των εντοπισμένων πραγματικών επιθέσεων προς το συνολικό αριθμό των επιθέσεων που σημειώθηκαν και εκφράζει το ρυθμό ανίχνευσης ενός IDS:

$$IDS_{Reliability} = \frac{number\ of\ detected\ true\ attacks}{total\ number\ of\ attacks}$$

Ο λόγος αυτός πρέπει να είναι όσο το δυνατόν πλησιέστερα στη μονάδα για να είναι αξιόπιστο ένα IDS. Σε αντίθετη περίπτωση το IDS γίνεται λιγότερο αξιόπιστο και αποτυγχάνει να ανιχνεύσει όλες τις επιθέσεις.

Ακρίβεια: Ένα IDS είναι ακριβές εάν εγείρει ελάχιστο αριθμό ψευδών συναγερμών, ιδανικά κανένα. Η ακρίβεια ενός IDS μπορεί να οριστεί ως

ο λόγος του αριθμού των εντοπισμένων πραγματικών επιθέσεων προς τον αριθμό των εντοπισμένων ως επιθέσεων:

$$IDS_{Accuracy} = \frac{number\ of\ detected\ true\ attacks}{number\ of\ detected\ as\ attacks}$$

Ο λόγος πρέπει πάλι να είναι όσο το δυνατόν πλησιέστερα στη μονάδα για να είναι πιο ακριβές ένα IDS. Αυτό σημαίνει ότι ο αριθμός των ψευδών θετικών συναγερμών πρέπει να είναι στο ελάχιστο επίπεδο ή ιδανικά μηδέν.

Η δυσκολία για τα IDS να διακρίνουν σωστά ένα ατυχές συμβάν από ένα που αποτελεί πραγματική επίθεση αξιολογώντας το σωστά είναι μεγάλη. Τα γεγονότα αυτά τις περισσότερες φορές είναι δυσδιάκριτα και αλληλοκαλύπτονται με αποτέλεσμα την επεξεργασία άσχετων δραστηριοτήτων ή τον εντοπισμό ψευδών επιθέσεων και την εξουδετέρωση φυσιολογικών γεγονότων ενεργοποιώντας λανθασμένους συναγερμούς. Αυτές οι λανθασμένες αποφάσεις, καθιστούν επίσης ένα IDS λιγότερο αποτελεσματικό. Δυστυχώς, τα συστήματα ανίχνευσης εισβολών αποτυγχάνουν να διαχειριστούν σε αποδεκτό επίπεδο τα γεγονότα που εντοπίζονται ως πραγματικές επιθέσεις, ψευδώς θετικούς και ψευδώς αρνητικούς συναγερμούς αντίστοιχα και να ξεπεράσουν όλες αυτές τις δυσκολίες και τους περιορισμούς.

Ως εκ τούτου, το ερευνητικό ερώτημα που δημιουργείται είναι πώς μπορεί να βελτιωθεί η ανίχνευση εισβολών στην ασφάλεια πληροφορικής βελτιστοποιώντας τα IDS και καθιστώντας τα λιγότερο προβληματικά. Κατά συνέπεια, υπάρχει ανάγκη για νέους τύπους προσεγγίσεων ανίχνευσης εισβολών, οι οποίοι θα χρησιμοποιούν εργαλεία και τεχνικές από άλλους καθιερωμένους τομείς, για μεγαλύτερη και καλύτερη αντιμετώπιση της προστασίας πληροφοριών.

5. Συστήματα Ανίχνευσης - Πρόληψης Διαρροής Δεδομένων και Πληροφοριών (DLPS - ILPS).

Ορισμένα πρόσφατα περιστατικά διαρροής δεδομένων, ανέδειξαν την δυσκολία παροχής μιας ολοκληρωμένης λύσης για την πρόληψη διαρροής πληροφοριών. Επιπλέον, έδειξαν ότι οι επιχειρήσεις πρέπει να διευρύνουν το

επίκεντρο των προσπαθειών τους πέρα από τους βασικούς τρόπους προστασίας και κλασικές απειλές (π.χ. ιούς, δούρειους ίππους, επιθέσεις DoS και απλές εισβολές). Οι οργανισμοί λοιπόν, κατανοούν την ανάγκη χρήσης νέων ***Συστημάτων Πρόληψης Διαρροής Δεδομένων (Data Leakage Prevention Systems – DLPS)*** και θα πρέπει να θεωρείται αυτονόητη η χρήση τους, ως μέρος ενός ολοκληρωμένου σχεδίου για τον χειρισμό και τη προστασία ευαίσθητων δεδομένων. Υποχρεούνται επίσης, να συμμορφώνονται με ομοσπονδιακούς και κρατικούς κανονισμούς που αποσκοπούν στην προστασία των επιστημονικών και άλλων ιδιωτικών δεδομένων. Τα τεχνολογικά μέσα, που χρησιμοποιούνται για την ενίσχυση της ασφάλειας, μπορούν να χωριστούν στις ακόλουθες κατηγορίες [19]:

- Συστήματα DLP.
- Έλεγχος πρόσβασης και κρυπτογράφηση.
- Προηγμένα /ευφυή μέτρα ασφαλείας.
- Βασικά μέτρα ασφάλειας.

Εικόνα 5.3: *Κατηγορίες τεχνολογικών προσεγγίσεων για ανίχνευση / πρόληψη διαρροής δεδομένων* [19].

Πιο αναλυτικά:

- Τα ***Συστήματα DLP*** αποσκοπούν στην ανίχνευση, τον εντοπισμό και την πρόληψη προσπαθειών αντιγραφής ή αποστολής ευαίσθητων δεδομένων σκόπιμα ή ακούσια, κυρίως από εξουσιοδοτημένο προσωπικό που έχει πρόσβαση σε ευαίσθητες πληροφορίες. Μια σημαντική δυνατότητα τέτοιων λύσεων είναι η ικανότητα ταξινόμησης του περιεχομένου των πληροφοριών ως ευαίσθητου. Η υλοποίηση αυτή γίνεται συνήθως με τη χρήση μηχανισμών, όπως είναι η ακριβής αντιστοίχιση δεδομένων, οι στατιστικές μέθοδοι, η μηχανική μάθηση, η αντιστοίχιση κανόνων και κανονικών εκφράσεων, οι εννοιολογικές έννοιες και λέξεις κλειδιά.
- Ο ***Έλεγχος συσκευής***, ο ***έλεγχος πρόσβασης*** και η ***κρυπτογράφηση*** χρησιμοποιούνται για την αποτροπή πρόσβασης από μη εξουσιοδοτημένους χρήστες. Αυτά είναι τα απλούστερα μέτρα που μπορούν να ληφθούν για την προστασία μεγάλων ποσοτήτων προσωπικών δεδομένων από κακόβουλες επιθέσεις ξένων και προσώπων που κατέχουν εμπιστευτικές πληροφορίες και έχουν σκοπό την υποκλοπή τους.
- Τα ***Προηγμένα /Ευφυή μέτρα ασφαλείας*** περιλαμβάνουν αλγόριθμους μηχανικής μάθησης για τον εντοπισμό μη φυσιολογικής πρόσβασης σε δεδομένα, όπως βάσεις δεδομένων ή συστήματα ανάκτησης πληροφοριών. Επίσης, περιλαμβάνουν επαλήθευση βάσει δραστηριότητας, δηλαδή με βάση τα πατήματα πλήκτρων και μοτίβα κίνησης ποντικιού, ανίχνευση μη φυσιολογικών προτύπων ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου, εφαρμογή δολωμάτων honeypot[3] για τον εντοπισμό κακόβουλων προσώπων που κατέχουν εμπιστευτικές πληροφορίες.

[3] **Honeypots**, ονομάζονται οι παγίδες που έχουν σαν στόχο να ανιχνεύσουν ή να εξουδετερώσουν κάθε μη εξουσιοδοτημένη πρόσβαση σε δίκτυα υπολογιστών. Στην πραγματικότητα είναι σχεδιασμένες για να παγιδεύουν ή και να παρακολουθήσουν τον εισβολέα.

- Τα ***Βασικά μέτρα ασφαλείας*** χρησιμοποιούνται από πολλούς οργανισμούς και περιλαμβάνουν κοινούς μηχανισμούς όπως firewalls, συστήματα ανίχνευσης εισβολών (IDSs) και λογισμικό προστασίας από ιούς που μπορεί να παρέχει προστασία από επιθέσεις. Ακόμα, μπορεί να χρησιμοποιείται συνδυασμός δύο ή περισσότερων λύσεων π.χ. ένα firewall που περιορίζει την πρόσβαση στο εσωτερικό δίκτυο και ένα σύστημα ανίχνευσης εισβολής που ανιχνεύει απόπειρες εισβολής από εξωτερικές επιθέσεις Ένα άλλο παράδειγμα, είναι η δημιουργία και η επιβολή πολιτικών και κανόνων διαχείρισης δεδομένων σε επίπεδο οργανισμού, ώστε να διασφαλίζεται για παράδειγμα η απόρριψη ή η πρόσβαση σε δεδομένα, μόνο από εξουσιοδοτημένους υπαλλήλους. Η δημιουργία πολιτικών θα πρέπει επίσης να συνοδεύεται από κατάλληλη κατάρτιση που θα ενημερώνει τους αντίστοιχους υπαλλήλους σχετικά για την εφαρμογή τους.

Οι ιδανικές λύσεις DLPs θα πρέπει να παρέχουν προστασία δεδομένων σε όλο τον κύκλο ζωής και χρήσης μιας πληροφορίας από την πηγή / καταχώριση έως και το τελικό σημείο αποθήκευσης ή επεξεργασίας της. Οι συμβατικοί έλεγχοι ασφαλείας έχουν λιγότερη σχέση με το περιεχόμενο ***(content)*** των δεδομένων και έτσι μπορεί εσφαλμένα να εμποδίσουν την πρόσβαση των χρηστών σε αυτά. Αυτό μπορεί να είναι σημαντικό μειονέκτημα όταν υπάρχει ένα ταχέως μεταβαλλόμενο περιβάλλον. Ωστόσο, ορισμένα μέτρα ασφαλείας, όπως τα IDS που βασίζονται σε ανωμαλίες, μπορεί να ενεργοποιηθούν προληπτικά όταν πληρούνται ορισμένα κριτήρια. Αυτά τα συστήματα επικεντρώνονται κυρίως στο πλαίσιο / περιβάλλον της πληροφορίας ***(context)*** όπως μέγεθος, χρονισμός, πηγή και προορισμός, παρά την ευαισθησία του περιεχομένου.

Τα DLPS εστιάζουν και στο περιβάλλον, που βρίσκονται τα εμπιστευτικά δεδομένα για ανίχνευση πιθανών διαρροών, αλλά κυρίως σε ανάλυση βάσει περιεχομένου, δεδομένου ότι είναι πιο λογικό να επικεντρωθούμε στην προστασία των ίδιων των δεδομένων παρά στο περιβάλλον που είναι καταχωρημένα.

Τα DLPS είναι πολύ νέα και δεν υπάρχει συγκεκριμένη συμφωνία για έναν κοινό ορισμό. Τόσο οι ακαδημαϊκοί όσο και οι επαγγελματίες του χώρου, χρησιμοποιούν διάφορα ονόματα, όπως ***Data Loss / Leak Prevention***, ***Information Loss / Leak Prevention***, ***Extrusion / Interception & Prevention Systems***, ***Content Monitoring*** & ***Filtering / Protection*** κ.τ.λ.

Επίσης, έχουν προταθεί διάφοροι ορισμοί για την περιγραφή λύσεων και μηχανισμών DLP όπως:

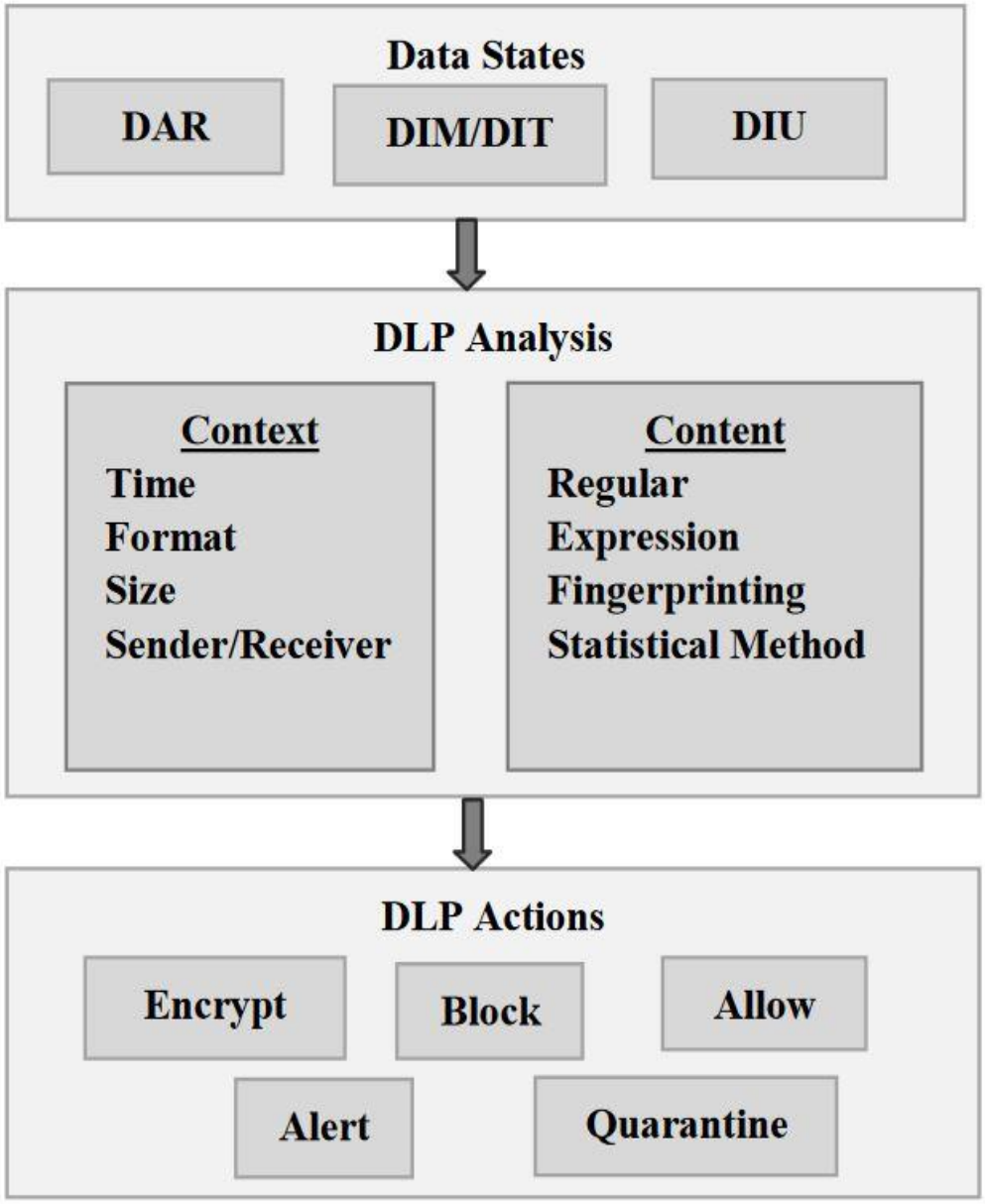
- "Σύστημα που παρακολουθεί και επιβάλλει πολιτικές σχετικά με δεδομένα που βρίσκονται σε κατάσταση ηρεμίας, σε κίνηση ή σε χρήση, σε δημόσιο ή ιδιωτικό υπολογιστή / δίκτυο" [20].
- "Συστήματα που εντοπίζουν, παρακολουθούν και προστατεύουν δεδομένα σε χρήση, σε κίνηση και τα δεδομένα σε λειτουργία μέσω βαθιάς επιθεώρησης περιεχομένου χρησιμοποιώντας ένα κεντρικό πλαίσιο διαχείρισης" [21].
- "Καθορισμένα συστήματα ανάλυσης που χρησιμοποιούνται για την προστασία δεδομένων από μη εξουσιοδοτημένη χρήση ή αποκάλυψη τους, με τεχνικές που χρησιμοποιούν διορθωτικές ενέργειες που ενεργοποιούνται από ένα σύνολο καλά ορισμένων κανόνων" [22].

Συμπεριλαμβανομένων τόσο διαχειριστικών όσο και τεχνικών προσεγγίσεων, η διαρροή δεδομένων είναι ένας όρος που χρησιμοποιείται στον χώρο της ασφαλείας για να περιγράψει ανεπιθύμητες αποκαλύψεις ή υποκλοπή πληροφοριών.

Τρία είναι τα κύρια χαρακτηριστικά που διακρίνουν τα DLPS από τους συμβατικούς μηχανισμούς ασφαλείας [22] [23]:

1. Τα DLPS μπορούν να αναπτυχθούν για να παρέχουν προστασία στα δεδομένα σε διαφορετικές καταστάσεις, δηλαδή κατά τη μεταφορά τους (DIM), σε χρήση (DIU) και σε κατάσταση ηρεμίας (DAR).
2. Τα DLPS έχουν την ικανότητα να αναλύουν το περιβάλλον, αλλά και το περιεχόμενο των εμπιστευτικών δεδομένων.
3. Το τρίτο χαρακτηριστικό είναι η ικανότητα προστασίας των δεδομένων μέσω ενεργειών, όπως ***κρυπτογράφηση, αποκλεισμός, ειδοποίηση, έλεγχος και καραντίνα***.

Το ακόλουθο σχήμα απεικονίζει τα τρία κύρια χαρακτηριστικά που διακρίνουν τα DLPS από τα συμβατικά μέτρα ασφαλείας.



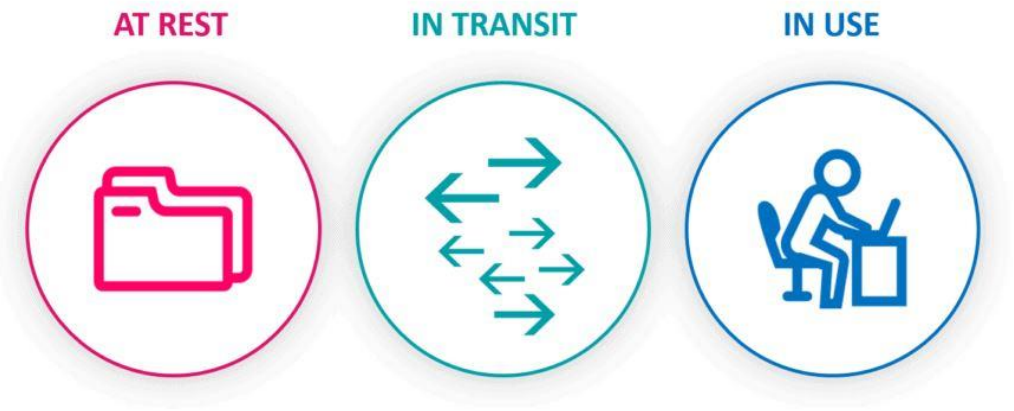
Εικόνα 5.4: *Τα τρία κύρια χαρακτηριστικά ενός τυπικού DLP* [23].

Η εφαρμογή ενός DLP πρέπει να σχεδιαστεί διεξοδικά και να μελετηθεί όσον αφορά την ανάγκη, το μέγεθος και το στόχο του κάθε οργανισμού που θα εφαρμοστεί.

Για παράδειγμα, εάν ένας οργανισμός εφαρμόζει λανθασμένα κάποιες από τις δυνατότητες ενός DLP η λειτουργία της επιχείρησης μπορεί να διαταραχθεί και να παρεμποδιστεί η ροής της εργασίας, πιθανώς από εκτεταμένη επιθεώρηση κυκλοφορίας ή αδυναμία ενσωμάτωσης με άλλους μηχανισμοί ασφαλείας. Έτσι, τα όποια προβλήματα πιθανόν προκύψουν πρέπει πρώτα να μελετηθούν για να αντιμετωπιστούν πριν από την εφαρμογή του DLP, ώστε να διασφαλιστεί ο οργανισμός ότι είναι έτοιμος να το χρησιμοποιήσει. Οι συγκεκριμένες προκλήσεις διαφέρουν μεταξύ των οργανισμών, ανάλογα με τη φύση της επιχείρησης και των όγκο των συναλλαγών της.

5.1. Καταστάσεις Δεδομένων.

Ο κύκλος ζωής των δεδομένων αποτελείται από διάφορες καταστάσεις οι οποίες δεν είναι σταθερές αλλά μεταβάλλονται ανάλογα τη χρήση και τη χρονική στιγμή που αναζητούνται. Τα DLPS καλούνται να παρέχουν προστασία στα δεδομένα σε όλες τις καταστάσεις που μπορεί να βρίσκονται κάθε στιγμή.



Εικόνα 5.5: *Καταστάσεις Δεδομένων* [24].

Στο πιο πάνω σχήμα φαίνονται οι τρεις καταστάσεις που μπορεί να περιλαμβάνουν δεδομένα όπως:

5.1.1. Δεδομένα σε κατάσταση ηρεμίας (Data at Rest - DAR).

Τα δεδομένα σε κατάσταση ***ηρεμίας*** [21] [25] είναι ο τύπος δεδομένων που βρίσκονται σε αποθηκευτικά μέσα, όπως π.χ. σκληροί δίσκοι, αποτελούμενα από βάσεις δεδομένων, εφαρμογές, backups, κ.α. Συνήθως για να εμποδιστεί η πρόσβαση, η κλοπή ή η αλλαγή τους από μη εξουσιοδοτημένα άτομα, προστατεύονται από κρυπτογράφηση και ισχυρούς ελέγχους πρόσβασης, συμπεριλαμβανομένων και φυσικών μηχανισμών. Τα DLPS που ασχολούνται με δεδομένα "σε ηρεμία" συνήθως επικεντρώνονται στην προστασία γνωστών δεδομένων. Η προστασία παρέχεται με τη μορφή πρόσβασης σε δεδομένα που βασίζονται σε πολιτικές ασφαλείας. Ένας τρόπος για να γίνει αυτό είναι με τη χρήση ανάλυσης περιεχομένου. Για παράδειγμα, μέσω μιας πολιτικής μπορούν όλοι οι αριθμοί πιστωτικών καρτών να αποθηκεύονται μόνο σε εγκεκριμένους εξυπηρετητές. Αν τα δεδομένα ανιχνευθούν σε μη εγκεκριμένο εξυπηρετητή, μπορούν να κρυπτογραφηθούν ή να απομακρυνθούν, ή να σταλεί μια προειδοποίηση στους διαχειριστές και στον ιδιοκτήτη των δεδομένων. Επίσης, αυτός ο τύπος DLP κατά τον έλεγχο αποφασίζει ποια κανάλια μεταφοράς πρέπει να παραμείνουν ανοικτά, απομονώνοντας τα κοινά κανάλια διαρροής. Ορισμένα από τα κανάλια είναι εύκολο να τα διαχειριστούν, ενώ άλλα απαιτούν σημαντική προσπάθεια για να ασφαλιστούν πλήρως.

5.1.2. Δεδομένα σε κίνηση (Data in Transit / Motion - DIM).

Δεδομένα ***εν κινήσει*** [21] [25] είναι αυτά που μετακινούνται από ένα κόμβο σε άλλο. Αυτός ο τύπος δεδομένων ταξιδεύει εσωτερικά εντός του ίδιου δικτύου ή εξωτερικά, μεταξύ κόμβων που ανήκουν σε διαφορετικά δίκτυα.

Μια λύση DLP μπορεί να αναπτυχθεί σε κάποια κομβικά σημεία αναλύοντας την κυκλοφορία του δικτύου και βάσει προκαθορισμένων πολιτικών, μπορούν να ενεργοποιούνται μηχανισμοί εμποδίζοντας ύποπτες μεταφορές δεδομένων. Ένα σύστημα DLP που έχει εφαρμοστεί στο δίκτυο πρέπει να έχει τη δυνατότητα να υποστηρίζει πολλαπλά σημεία ελέγχου, ενώ ένας κεντρικός εξυπηρετητής (server) να συλλέγει και να αναλύει όλα τα δεδομένα που λαμβάνονται από τα σημεία παρακολούθησης.

Αυτός ο τύπος DLPS πρέπει να διαθέτει ειδικές δυνατότητες επεξεργασίας για να μπορεί να διαχειριστεί μεγάλες ποσότητες δεδομένων και επίσης, είναι υπεύθυνος για την επιθεώρηση όλης της εξερχόμενης και εισερχόμενης κυκλοφορίας. Παράλληλα ενεργεί και ως διακομιστής μεσολάβησης κατά την πρόσβαση σε ορισμένες εφαρμογές με εμπιστευτικά δεδομένα. Επιπλέον, αναφέρει και ειδοποιεί προληπτικά τους διαχειριστές ασφαλείας και τους ανάλογους χρήστες σχετικά με πιθανές διαρροές δεδομένων. Τέλος, ιδανικά θα πρέπει να υπάρχει συνεργασία και με άλλους μηχανισμούς ασφαλείας, όπως secure sockets layer (SSL), firewalls κ.τ.λ. για την επίτευξη του βέλτιστου δυνατού αποτελέσματος.

5.1.3. Δεδομένα σε χρήση (Data in Use - DIU).

Τα δεδομένα ***σε χρήση*** [21] [25] είναι αυτά τα οποία είναι προσβάσιμα από χρήστες με τη μορφή εγγράφων, email, εφαρμογών κ.τ.λ. Αυτός ο τύπος δεδομένων στις περισσότερες των περιπτώσεων είναι απλό κείμενο που μπορεί εύκολα να επεξεργαστεί και να αναλυθεί. Τα δεδομένα σε χρήση είναι οποιαδήποτε δεδομένα με το οποία ένας χρήστης αλληλοεπιδρά. Για να προστατευτούν, χρησιμοποιούνται συστήματα *τελικού σημείου (endpoint)*, παρακολουθώντας την κίνηση και την αλληλεπίδραση που γίνεται με τους χρήστες. Συνήθως, ένα μέσο παρακολούθησης επιτηρεί τα δεδομένα κατά τη χρήση ή τη μεταφορά τους από τη συσκευή τελικού σημείου, μέσω των διαύλων επικοινωνίας ή εξόδων σε περιφερειακές συσκευές.

Ο στόχος είναι ότι, όταν γίνει μια προσπάθεια να αποσταλούν ευαίσθητα δεδομένα, να ανιχνευθεί αμέσως η πιθανή απώλεια, να εμποδιστεί προτού σταλθούν τα δεδομένα και να μπλοκαριστούν ή να κρυπτογραφηθούν. Τα εργαλεία των δεδομένων σε χρήση μπορούν να ελέγχουν τις ακόλουθες δραστηριότητες:

- Λειτουργίες αντιγραφής και επικόλλησης, λειτουργίες σύλληψης της οθόνης (screen capture).
- Μεταφορά ευαίσθητου περιεχομένου από ένα μέρος σε ένα άλλο με χρήση φορητών συσκευών, όπως USB, δίσκων CD/DVDs, έξυπνων

τηλεφώνων και PDAs ενώ περιορίζεται και η παραγωγή έντυπων αντιγράφων μέσω εκτυπωτών.

- Μεταφορά ευαίσθητων δεδομένων μέσω διαύλων επικοινωνίας, για παράδειγμα εσκεμμένη ή ακούσια αποστολή δεδομένων σε μορφή δακτυλογραφημένου περιεχομένου, συνημμένων αρχείων ή φωνητικών συνομιλιών, μέσω μιας εφαρμογής μηνυμάτων ή μίας ιστοσελίδας, ή αντιγραφή ευαίσθητου περιεχομένου από διαμοιρασμένους φακέλους σε ένα δίκτυο (LAN).
- Χρήση ευαίσθητων δεδομένων σε μη εγκεκριμένη εφαρμογή, όπως π.χ. προσπάθεια κρυπτογράφησης δεδομένων με σκοπό να ξεγελάσουν τους μηχανισμούς ελέγχου και να αποσταλούν.

Ανάλογα με τα δεδομένα που προορίζονται για προστασία, η ανάπτυξη DLPS μπορεί να λάβει πολλές μορφές. Για παράδειγμα, η προστασία των δεδομένων σε χρήση απαιτεί ενσωματωμένο λογισμικό που λειτουργεί ως πράκτορας DLP σε τελικά σημεία. Αυτός ο πράκτορας είναι υπεύθυνος για την απενεργοποίηση ή την ενεργοποίηση της πρόσβασης σε εφαρμογές που χρησιμοποιούν ευαίσθητα δεδομένα και γενικά ελέγχει όλες τις δραστηριότητες που σχετίζονται με την πρόσβαση.

5.2. Ανάλυση Περιεχομένου και Πλαισίου.

Στο σημείο αυτό χρειάζεται να γίνει ένας διαχωρισμός μεταξύ περιεχομένου και πλαισίου. Για να γίνει ευκολότερα κατανοητό, το πλαίσιο μπορεί να χαρακτηριστεί σαν ένας φάκελος και το περιεχόμενο σαν μια επιστολή.

Το πλαίσιο είναι πολύ σημαντικός παράγοντας και θα πρέπει να συμπεριλαμβάνεται η αντίστοιχη ανάλυσή του από τους μηχανισμούς DLP σαν μέρος της συνολικής ανάλυσης. Αυτό όμως που πρέπει να προστατευτεί είναι τα ίδια τα δεδομένα και όχι ο φάκελος που περιγράφει το είδος και τον τύπο των δεδομένων αυτών. Επομένως, για να γίνει αυτό θα πρέπει πρώτα να ανοιχθεί, να διαβαστεί και ανάλογα να γίνει η επιλογή της κατάλληλης ενέργειας.

5.2.1. Ανάλυση Πλαισίου / Περιβάλλοντος (context).

Στο πλαίσιο περιλαμβάνονται στοιχεία όπως [21] η πηγή, το μέγεθος, πληροφορίες κεφαλίδας, ο προορισμός, ο αποστολέας και οτιδήποτε άλλο μπορεί να οριστεί από το περιεχόμενο μιας επιστολής. Ένας μηχανισμός DLP *context based*, αξιοποιεί πληθώρα τεχνολογιών ασφαλείας, όπως συστήματα ανίχνευσης και πρόληψης (IDS / IPS), τείχη προστασίας (firewalls), φιλτράρισμα ανεπιθύμητης αλληλογραφίας (spam), διακομιστές μεσολάβησης (proxies) κ.τ.λ. Το περιβάλλον ορίζεται από τα συμφραζόμενα, από τη πληροφορία που εξάγεται και από τα επιτηρούμενα δεδομένα.

Ένας μηχανισμός DLP βάσει περιβάλλοντος μπορεί να εμποδίσει την αποστολή αρχείων έξω από έναν οργανισμό για αποφυγή διαρροής δεδομένων με χρήση των κάτωθι προληπτικών μέτρων:

- ***Απενεργοποίηση λειτουργιών:*** Αυτή η προληπτική ενέργεια περιλαμβάνει την απενεργοποίηση λειτουργιών, οι οποίες μπορούν να καταλήξουν σε μη ορθή χρήση ευαίσθητων δεδομένων, περιορίζοντας τις λειτουργίες αντιγραφής και επικόλλησης, ή περιορίζοντας την μεταφορά τους για παράδειγμα σε φορητά αποθηκευτικά μέσα.
- ***Κρυπτογράφηση:*** Προληπτικά εφαρμόζονται πολιτικές που ορίζουν ποια ευαίσθητα δεδομένα πρέπει να κρυπτογραφηθούν και από ποιον επιτρέπεται η αίτηση αποκρυπτογράφησης τους. Επίσης, επιτρέπεται η κρυπτογράφηση μόνο με εγκεκριμένες εφαρμογές, ενώ περιορίζονται εφαρμογές στις οποίες επιτρέπεται η πρόσβαση σε ευαίσθητα δεδομένα.
- ***Έλεγχος πρόσβασης:*** Η προσέγγιση αυτή περιλαμβάνει τη δυνατότητα απαγόρευσης ή χρήσης συγκεκριμένων πόρων από μια συγκεκριμένη συσκευή ή οντότητα. Ανάλογες πολιτικές μπορούν να απαγορεύσουν τη χρήση κάποιων πόρων, ακόμα και αν έχει χορηγηθεί για κάποιο λόγο πρόσβαση π.χ. ανάγνωσης και εγγραφής σε κάποια ευαίσθητη πληροφορία. Ένας τρόπος μεγαλύτερου ελέγχου πρόσβασης επιτυγχάνεται μέσω συνεργασίας με συμβατικούς μηχανισμούς ασφαλείας, όπως firewall, IDS κ.τ.λ.

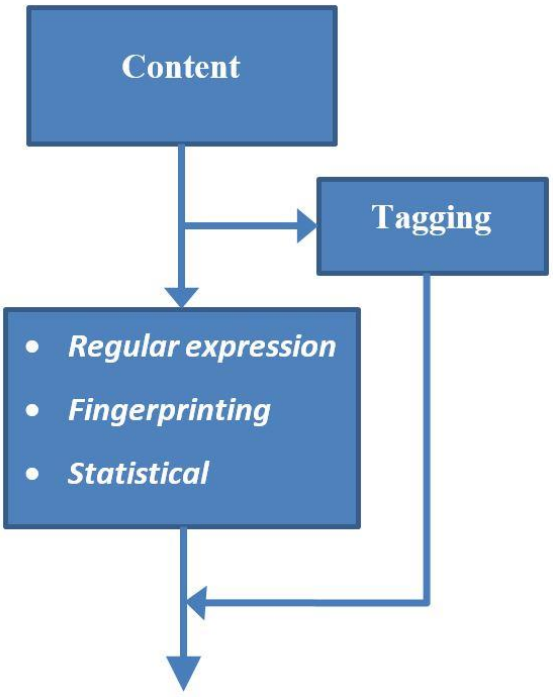
5.2.2. Ανάλυση Περιεχομένου (content).

Η ανάλυση περιεχομένου, είναι δύσκολη και χρονοβόρα λειτουργία, αλλά είναι καθοριστικό χαρακτηριστικό για μια εφαρμογή DLP [21] [26].

Το πρώτο βήμα στην ανάλυση περιεχομένου είναι ο έλεγχος του πλαισίου και το “άνοιγμά” του. Για ένα απλό κείμενο αυτό είναι εύκολο, αλλά όταν απαιτείται έλεγχος σε αρχεία άλλης μορφής, γίνεται ιδιαίτερα πολύπλοκο. Για να υλοποιηθεί αυτή η λειτουργία, η εφαρμογή DLP πραγματοποιεί διάσπαση του αρχείου για να ανιχνεύσει και να διαβάσει το περιεχόμενο, ακόμη κι αν βρίσκεται κάτω από άλλα επίπεδα. Για παράδειγμα, ένα αρχείο με κατάληξη (.zip) το οποίο έχει συμπιεστεί, η εφαρμογή χρειάζεται να το αποσυμπιέσει για να το διαβάσει, να το αναλύσει και να επεξεργαστεί την κρυμμένη πληροφορία, που μπορεί να είναι αρχείο άλλης μορφής ενσωματωμένο μέσα σε άλλου τύπου αρχείο, όπως pdf μέσα σε αρχείο word ή Excel κ.τ.λ. Κάποια εργαλεία υποστηρίζουν ακόμη και ανάλυση από κρυπτογραφημένα δεδομένα, εάν η κρυπτογράφηση του οργανισμού χρησιμοποιείται μαζί με τα κλειδιά ανάκτησης και μπλοκάρουν ή θέτουν σε καραντίνα το περιεχόμενο αντίστοιχα. Η ικανότητα των προϊόντων αυτών να αναλύουν σε βάθος τα περιεχόμενα των δεδομένων, είναι διαφορετική και δυσκολότερη από την ανάλυση του πλαισίου και η απόδοσή τους εξαρτάται άμεσα από την επεξεργαστική ισχύ των τελικών σημείων που εφαρμόζονται. Οι μηχανισμοί αυτοί δυστυχώς επιβαρύνουν την απόδοση ενός σταθμού εργασίας με πρόσθετες λειτουργίες και αυτό θα πρέπει να συνυπολογιστεί για την σωστή επιλογή και εγκατάσταση των κατάλληλων μηχανισμών.

Ένα τυπικό *content-based* DLP εφαρμόζει παρακολούθηση ευαίσθητων δεδομένων σε αποθετήριο (DAR) ή σε κατάσταση μεταφοράς (DIM) χρησιμοποιώντας [26]: **α)** ***Επισήμανση περιεχομένου***, **β)** ***Κανονικές εκφράσεις***, **γ)** ***Αποτυπώματα δεδομένων*** και δ) ***Στατιστική ανάλυση.***

Πιο αναλυτικά:



Εικόνα 5.6: *Ανάλυση Περιεχομένου (content).*

α) Επισήμανση περιεχομένου (content tagging). Στην προσέγγιση αυτή, αποδίδεται μια επισήμανση σε ένα αρχείο, που περιέχει ευαίσθητα δεδομένα, όπως φαίνεται στο πιο πάνω σχήμα και εφαρμόζεται μια πολιτική βάση της σήμανσης που έχει αποδοθεί. Η επισήμανση θα παραμείνει ακόμα και αν το περιεχόμενο επεξεργαστεί από άλλες εφαρμογές. Ένα αρχείο κειμένου για παράδειγμα, που έχει επισήμανθεί ως ευαίσθητο, θα παραμείνει επισημασμένο ακόμα και αν κρυπτογραφηθεί ή συμπιεστεί. Υπάρχουν διάφοροι τρόποι για να αποδοθεί μια επισήμανση σε δεδομένα όπως, αυτόματα σε αρχεία που έχουν δημιουργηθεί από συγκεκριμένους χρήστες ή συγκεκριμένες εφαρμογές και βρίσκονται σε συγκεκριμένη τοποθεσία ή με χρήση ανάλυσης περιεχομένου και περιβάλλοντος. Επίσης, μπορεί να γίνει επισήμανση και χειροκίνητα από τον δημιουργό των ευαίσθητων δεδομένων ή τον διαχειριστή του συστήματος αντίστοιχα.

β)Κανονικές εκφράσεις χρησιμοποιούνται συνήθως από έναν συγκεκριμένο κανόνα για παράδειγμα τον εντοπισμό αριθμών ταυτότητας, κοινωνικής ασφάλισης ή αριθμών πιστωτικών καρτών. Το πρόβλημα με τα

DLPS που χρησιμοποιούν ανάλυση κανονικών εκφράσεων είναι, ότι προσφέρουν σχετικά περιορισμένη προστασία δεδομένων και έχουν ψευδώς θετικά ποσοστά σφάλματος. Για παράδειγμα, είναι εύκολο να εντοπιστεί και να αποτραπεί η διαρροή ενός progect name μέσω email, χρησιμοποιώντας έναν κανόνα που εμποδίζει την αποστολή email που περιέχουν αυτό το συγκεκριμένο όνομα. Ωστόσο, είναι δύσκολο να αποφευχθεί η διαρροή των λεπτομερειών του συγκεκριμένου project εάν προσεκτικά δεν αναφερθεί πουθενά το όνομά του. Επιπλέον, εάν ο κανόνας είναι συνεχώς ενεργός, ένα email μπορεί εσφαλμένα να αποκλειστεί εάν το ίδιο όνομα έργου χρησιμοποιείται σε άλλη περίπτωση. Για να αντιμετωπιστεί η αδυναμία αυτής της μεθόδου χρησιμοποιείται η τεχνική της ***"δομημένης"*** αντιστοίχισης δεδομένων.

- ***Δομημένα*** είναι εκείνα τα δεδομένα τα οποία βρίσκονται σε καθορισμένες και τυποποιημένες μορφές, όπως π.χ. οι αριθμοί πιστωτικών καρτών, αριθμοί μητρώου κοινωνικών ασφαλίσεων κ.τ.λ. και εφαρμόζονται 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. Αντίστοιχα σε περίπτωση που η ενέργεια αυτή πραγματοποιηθεί από άγνωστο ή αναρμόδιο τμήμα, ο αντίστοιχος μηχανισμός DLP θα πρέπει να σημάνει συναγερμό. Ως εκ τούτου, με τη δομημένη αντιστοίχιση και διαβάθμιση των αρχείων επιτρέπεται ή όχι η πρόσβαση και επεξεργασία ξεχωριστά για κάθε περίπτωση, μειώνοντας έτσι τους ψευδώς θετικούς συναγερμούς, με αποτέλεσμα να απλοποιείται η κατασκευή και ταυτόχρονα να αυξάνεται η αξιοπιστία των πολιτικών που θα εφαρμοστούν από έναν οργανισμό για την προστασία του.
- ***Αδόμητα*** είναι τα δεδομένα που δεν ακολουθούν μια συγκεκριμένη μορφή και συμπεριλαμβάνουν οτιδήποτε άλλο. Ορισμένα παραδείγματα των αδόμητων δεδομένων είναι, πηγές κωδικών, αρχεία πολυμέσων κ.τ.λ.

γ) Τα DLPS που χρησιμοποιούν ***ψηφιακά αποτυπώματα δεδομένων*** (fingerprint) παρέχουν καλύτερη προστασία σε ευαίσθητα δεδομένα, επειδή έχουν την ικανότητα να εντοπίζουν και να αποτρέπουν διαρροή ενός ολόκληρου εγγράφου ή τμημάτων αυτού.

Αποτυπώματα (fingerprint) εφαρμόζονται κυρίως σε αδόμητα δεδομένα εξαιτίας της πολύπλοκης μορφής τους. Τα αποτυπώματα δεδομένων δημιουργούνται χρησιμοποιώντας one way secure hash, το οποίο στη συνέχεια σώζεται σε μια βάση δεδομένων. Έπειτα, οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για τον προσδιορισμό ευαίσθητων δεδομένων σε κάποιο σημείο 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. Ωστόσο, η παραδοσιακή λήψη αποτυπωμάτων μπορεί να χάσει το ίχνος τους όταν τα δεδομένα τροποποιηθούν. Αυτό συμβαίνει, επειδή ο παραδοσιακός κατακερματισμός που χρησιμοποιείται για τη δημιουργία αποτυπωμάτων, όπως MD5 και SHA1, είναι επιρρεπής σε αλλαγές. Μια μικρή αλλαγή στα δεδομένα μπορεί να έχει ως αποτέλεσμα ένα εντελώς διαφορετικό κατακερματισμένο αποτύπωμα κάθε φορά. Αυτό πιθανόν να παρακάμψει το DLP και έτσι προστατευμένα δεδομένα μπορεί να διαρρεύσουν. Το πρόβλημα αυτό μπορεί να επιλυθεί εν μέρει, χρησιμοποιώντας πολλαπλό κατακερματισμό δεδομένων χωρισμένων σε μικρότερα μέρη, δηλαδή παράγραφοι και προτάσεις ξεχωριστά. Έτσι, μπορεί να διασφαλιστεί ότι μέρη από τα αρχικά δεδομένα δεν είναι εύκολα ανακτήσιμα. Ωστόσο, αυτά τα μικρότερα αποτυπώματα, είναι επίσης ευαίσθητα σε αλλαγές και η πιο μικρή αλλαγή μπορεί να κάνει τη μέθοδο αναποτελεσματική.

Πιο προχωρημένες προσεγγίσεις προσπαθούν να ξεπεράσουν αυτό το πρόβλημα, αλλά δεν παύουν να έχουν περιορισμένες δυνατότητες και να επηρεάζονται από διάφορες μικροαλλαγές κειμένου.

δ) Η ***στατιστική ανάλυση*** μπορεί να λειτουργήσει σε ένα περιβάλλον όπου τα ευαίσθητα δεδομένα δεν είναι καλά δομημένα και η σημασιολογία τους κατανέμεται σε μεγάλο εύρος. Το σύστημα ανιχνεύοντας πιθανά συμβάντα, θα εφαρμόσει την αντίστοιχη ενέργεια και διορθωτική κίνηση, για να αποτραπεί οποιοδήποτε αναγνωρισμένο συμβάν διαρροής. Το κύριο

πλεονέκτημα μιας τέτοιας τεχνικής είναι η ικανότητα προσδιορισμού ευαίσθητων εγγράφων, ακόμη και μετά από ακραία τροποποίηση. Ειδικότερα, μπορούν να χρησιμοποιηθούν DLPS με δυνατότητες στατιστικής ανάλυσης και αλγόριθμους μηχανικής μάθησης για αναγνώριση τροποποιημένων εγγράφων. Μπορούν επίσης, να χρησιμοποιήσουν τεχνικές ομαδοποίησης κειμένου για να δημιουργήσουν διάσπαρτα ίχνη ευαίσθητων δεδομένων.

5.3. Προκλήσεις στα συστήματα DLPs.

Ανάλογα με τον τύπο των δεδομένων για προστασία, η ανάπτυξη των DLPS μπορεί να λάβει πολλές μορφές και όπως κάθε μηχανισμός ασφαλείας αντιμετωπίζει πολλές και μεγάλες προκλήσεις. Από έρευνες που πραγματοποιήθηκαν τόσο σε ακαδημαϊκούς όσο και σε εμπορικούς χώρους, εντοπίστηκαν κυρίως επτά περιπτώσεις, όπου στην ουσία είναι οι αδυναμίες των συμβατικών μηχανισμών IDS κ.τ.λ., που πρέπει να αντιμετωπιστούν για επιτυχημένη εφαρμογή και πρόληψη διαρροής δεδομένων.

Πιο κάτω αναφέρονται οι επτά προκλήσεις ασφαλείας [22] [27] για τα DLPS.

5.3.1. Δικαιώματα πρόσβασης.

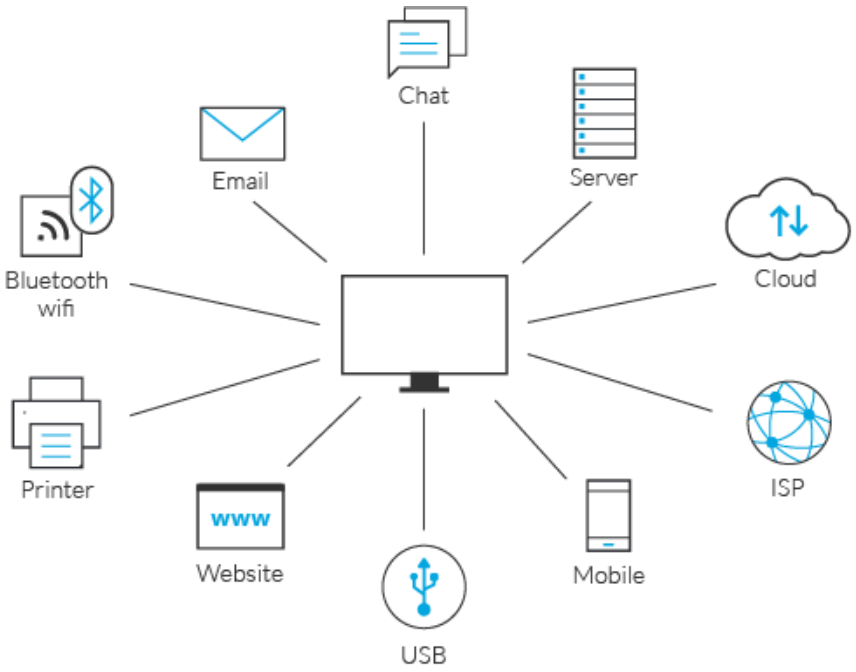
Είναι σημαντικό για τα DLPS να μπορούν να κάνουν διάκριση μεταξύ διαφορετικών χρηστών βάσει των προνομίων και των δικαιωμάτων τους. Χωρίς σωστό ορισμό των δικαιωμάτων πρόσβασης, τα DLPS δεν μπορούν να αποφασίσουν εάν υπάρχει πρόσβαση σε δεδομένα από μη νόμιμο χρήστη. Ορισμένα DLPS χρησιμοποιούν υπάρχουσες λίστες πρόσβασης, που παρέχονται από συστήματα όπως το Active Directory. Ωστόσο ξεπερασμένα δικαιώματα πρόσβασης μπορεί να επηρεάσουν αρνητικά τα DLPS. Για παράδειγμα, πρώην υπάλληλοι ή στελέχη, που έχουν π.χ. υποβαθμιστεί, μπορούν να αποκτήσουν πρόσβαση σε δεδομένα χρησιμοποιώντας τα παλιά τους προνόμια, εάν τα δικαιώματα πρόσβασής τους δεν έχουν ανακληθεί ή ακυρωθεί. Συνεπώς, τα DLPS δεν μπορούν να εντοπίσουν παραβίαση από τον συγκεκριμένο χρήστη. Επιπλέον, μια διαρροή μπορεί να προκληθεί και από νόμιμους χρήστες σκόπιμα ή και τυχαία.

Επομένως, τα συστήματα ελέγχου πρόσβασης έχουν σημαντικό ρόλο στην πρόληψη της διαρροής δεδομένων και ένα αποτελεσματικό DLP θα πρέπει να έχει την ικανότητα διατήρησης των σωστών δικαιωμάτων πρόσβασης προστατεύοντας τα δεδομένα, ακόμη και από τυχαίες διαρροές.

5.3.2. Διαρροή καναλιών επικοινωνίας.

Για να υπάρχει πρόσβαση και διαμοιρασμός δεδομένων μεταξύ χρηστών, συσκευών και άλλων οντοτήτων, πρέπει μεταξύ τους να είναι διαθέσιμα κανάλια διαφόρων τύπων και δίαυλοι επικοινωνίας. Με ορθή χρήση τα κανάλια αυτά χρησιμοποιούνται για ανταλλαγή δεδομένων, ωστόσο μπορεί να είναι υπεύθυνα και για διαρροή πληροφοριών. Περισσότερο δε, εάν υπάρχει ανάγκη για κοινή χρήση φακέλων και αρχείων, μερικά ή όλα αυτά τα κανάλια πρέπει να διατηρούνται ανοιχτά και προσβάσιμα προς όλους.

Το ακόλουθο σχήμα δείχνει τα πιο κοινά κανάλια επικοινωνιών που είναι υπεύθυνα για πιθανή διαρροή.



Εικόνα 5.7: *Κανάλια επικοινωνίας.*

Μερικοί από αυτούς τους τρόπους επικοινωνίας είναι εύκολοι στη διαχείριση, ενώ άλλοι απαιτούν σημαντική προσπάθεια για να διασφαλιστεί πλήρως η

κυκλοφορία μέσα από αυτούς. Δεδομένα "σε χρήση" και "σε ηρεμία" μπορούν να διαρρεύσουν μέσω τέτοιων καναλιών, όπως θύρες USB, μονάδες CD, υπηρεσίες διαδικτύου αλλά ακόμη και σε έντυπη μορφή. Διαρροές δεδομένων μέσω θυρών USB και μονάδων CD μπορούν να μετριαστούν μέσω κεντρικών κανόνων και πολιτικών προστασίας DLPS ή ακόμη και ενός απλούστερου IDS, αλλά αυτό δεν αρκεί γιατί υπάρχουν άλλοι τρόποι διαρροής πληροφοριών, όπως email, IM κ.τ.λ. Επιπλέον, μπορούν να οριστούν διαφορετικά δικαιώματα πρόσβασης, ανάλογα με το ρόλο του κάθε χρήστη, προκειμένου να έχει πρόσβαση σε εμπιστευτικά δεδομένα. Παρόλα αυτά, τα ίδια δεδομένα θα μπορούσαν να είναι προσβάσιμα σε άλλες μορφές όπως για παράδειγμα εκτυπώσιμων εγγράφων. Διαρροή μέσω καναλιών που σχετίζεται με δεδομένα "εν κινήσει", όπως υπηρεσίες διαδικτύου και κοινή χρήση αρχείων, μπορεί να είναι εξαιρετικά δύσκολη δεδομένου ότι συνήθως τα κανάλια αυτά ελέγχονται από συστήματα IDS ή τα διαχειρίζονται εμπορικοί ή ακόμη και κρατικοί πάροχοι με υψηλά στάνταρ ασφαλείας και επιτήρησης. Πρέπει όμως να μπορεί να διασφαλιστεί η μέγιστη ασφάλεια για τα δεδομένα που χρησιμοποιούν αυτούς τους διαύλους, χωρίς να παρεμποδίζεται η ροή εργασιών ή η παροχή δικτυακών υπηρεσιών. Έτσι, μια μεγάλη πρόκληση για τα DLPS είναι να μπορούν να παρέχουν ικανά επίπεδα ασφάλειας για δεδομένα “εν κινήσει” χωρίς να επηρεάζεται η συνδεσιμότητα μεταξύ διαφορετικών δικτύων, τομέων και κόμβων.

5.3.3. Τροποποίηση δεδομένων.

Ορισμένα DLPS χρησιμοποιούν πρότυπα δεδομένων και υπογραφές για σύγκριση μεταξύ εμπιστευτικών δεδομένων. Για τον εντοπισμό πιθανής διαρροής γίνεται έλεγχος για να διαπιστωθεί, εάν αυτά τα πρότυπα και οι υπογραφές ταιριάζουν ή αν παρατηρείται υψηλός βαθμός ομοιότητας. Ωστόσο τα εμπιστευτικά δεδομένα δεν αποστέλλονται πάντοτε αυτούσια δυσκολεύοντας έτσι την ανίχνευσή τους. Στην πραγματικότητα, τα εμπιστευτικά δεδομένα μπορούν να εκτεθούν σε πολλούς τύπους τροποποιήσεων. Για παράδειγμα, οι χρήστες μπορούν να επεξεργαστούν εμπιστευτικά έγγραφα με προσθήκη, αφαίρεση και αντικατάσταση γραμμών ή ακόμη και ολόκληρων

παραγράφων πριν από την αποστολή. Επιπλέον, η σημασιολογία ενός εγγράφου μπορεί να ξαναγραφεί με τη μορφή περιλήψεων. Αυτές οι παραλλαγές μπορούν να αλλάξουν την ταυτότητα του αρχικού εγγράφου και να παρακάμψουν τους μηχανισμούς ασφαλείας.

Για το λόγο αυτό, ορισμένα DLPS χρησιμοποιούν κατακερματισμό δεδομένων προκειμένου να ελεγχθεί η εξερχόμενη κίνηση. Τιμές κατακερματισμού, συμπεριλαμβανομένων των παραδοσιακών MD5 και SHA1, συγκρίνουν τα προς έλεγχο και τα υπάρχοντα δεδομένα για τυχόν ομοιότητες. Εάν οι δύο τιμές ταιριάζουν, τότε εντοπίζεται πιθανή διαρροή. Το πρόβλημα με τον κατακερματισμό είναι ότι οποιαδήποτε τροποποίηση του πρωτότυπου έγγραφου μπορεί να οδηγήσει σε τελείως διαφορετική τιμή κατακερματισμού, με αποτέλεσμα πιθανή αποκάλυψη του. Μια καλύτερη προσέγγιση είναι ο διαχωρισμός των έγγραφων σε μικρότερα μέρη και στη συνέχεια τον υπολογισμό διαφορετικής τιμής κατακερματισμού για κάθε μέρος. Σε αυτήν την περίπτωση, τμήματα του πρωτότυπου εγγράφου μπορούν να ανιχνευθούν ακόμα και μετά από τροποποίηση. Έχουν σχεδιαστεί εξελιγμένες μέθοδοι κατακερματισμού και σύγκρισης ομοιότητας με ψηφιακά αποτυπώματα για την ανίχνευση διαρροών, ωστόσο αυτές οι τεχνικές δεν είναι αρκετά αποτελεσματικές εάν το τα δεδομένα έχουν τροποποιηθεί εκτενώς.

5.3.4. Ο ανθρώπινος παράγοντας.

Είναι πολύ δύσκολο να προβλεφθεί η ανθρώπινη συμπεριφορά ενός χρήστη, επειδή επηρεάζεται από πολλούς ψυχολογικούς και κοινωνικούς παράγοντες. Πολλές ανθρώπινες ενέργειες, επηρεάζονται από την υποκειμενικότητα στη λήψη αποφάσεων, όπως ο καθορισμός του επιπέδου μυστικότητας δεδομένων ή εκχωρώντας τα σωστά δικαιώματα πρόσβασης στους σωστούς χρήστες και σωστή βαθμονόμηση του ορίου ανίχνευσης των DLPS. Επιπρόσθετα, κάποιοι υπάλληλοι / χρήστες δεν συμμορφώνονται εύκολα με τις πολιτικές ασφάλειας του οργανισμού, ακόμη και κι αν υπάρχουν αυστηροί κανονισμοί και οδηγίες.

Οι περισσότεροι άνθρωποι αλληλοεπιδρούν με πληροφορίες και δεδομένα "σε χρήση", συνήθως από κάποιο τερματικό σημείο, οπότε και τα περισσότερα δεδομένα μπορούν να διαρρεύσουν σε αυτήν την κατάσταση. Επιπλέον, πολλά DLP τείνουν να περιορίζουν την δυνατότητα του χρήστη να διαρρέει δεδομένα, απενεργοποιώντας τις θύρες για αφαιρούμενα μέσα, USB, μονάδες CD κ.τ.λ. Ωστόσο, οι χρήστες μπορούν να συνδυάσουν διάφορες τεχνικές, ακόμη και με περιορισμένο υπόβαθρο πληροφορικής, για την παράκαμψη αυτών των περιορισμών ή εν αγνοία τους μέσω κοινωνικής μηχανής (social engineering).

Αυτό που καθιστά την χρήση κοινωνικής μηχανής ιδιαίτερα επικίνδυνη είναι ότι βασίζεται στο ανθρώπινο λάθος και όχι σε τρωτά σημεία του λογισμικού και των λειτουργικών συστημάτων. Τα λάθη που γίνονται από τους νόμιμους χρήστες είναι λιγότερο προβλέψιμα, καθιστώντας τα πιο δύσκολο να εντοπιστούν και να αποτραπούν, σε σχέση με μια εισβολή που γίνεται από ένα κακόβουλο λογισμικό. Επιπλέον, οι χρήστες μπορούν να αντιγράψουν ή να τραβήξουν στιγμιότυπα οθόνης εγγράφων ή ακόμα και να κάνουν χρήση κάμερας κινητού τηλεφώνου για τη λήψη φωτογραφιών σε διαβαθμισμένα έγγραφα.

Όσο υπάρχει λοιπόν ο ανθρώπινος παράγοντας, θα υπάρχουν πάντα δυσκολίες αλλά και προκλήσεις για τα DLPS.

5.3.5. Επεκτασιμότητα και ενσωμάτωση.

Όπως πολλοί άλλοι μηχανισμοί ασφαλείας δικτύου, τα DLPS μπορούν επίσης να επηρεαστούν από την ποσότητα των δεδομένων που υποβάλλονται για επεξεργασία και θα πρέπει να είναι σε θέση να επεξεργάζονται δεδομένα χωρίς να παρεμποδίζεται η ροή εργασίας. Παράγοντες, όπως το επιθεωρούμενο μέγεθος δεδομένων, οι υπολογιστικές δυνατότητες και η τεχνική ανάλυσης που χρησιμοποιείται, θα πρέπει να διερευνώνται πλήρως για τη σωστή επιλογή ενός επεκτάσιμου συστήματος DLP. Επίσης, τα DLPS τείνουν να έχουν μια κακή ενσωμάτωση μέσα σε μια εγκατάσταση δικτύου. Αυτό συμβαίνει επειδή ορισμένα από τα βασικά χαρακτηριστικά τους υπάρχουν ήδη σε άλλες λύσεις, όπως firewalls, IDS και διακομιστές μεσολάβησης. Εάν πρόκειται να ενσωματωθεί ένα DLPS σε ένα δίκτυο, θα πρέπει να διενεργείται

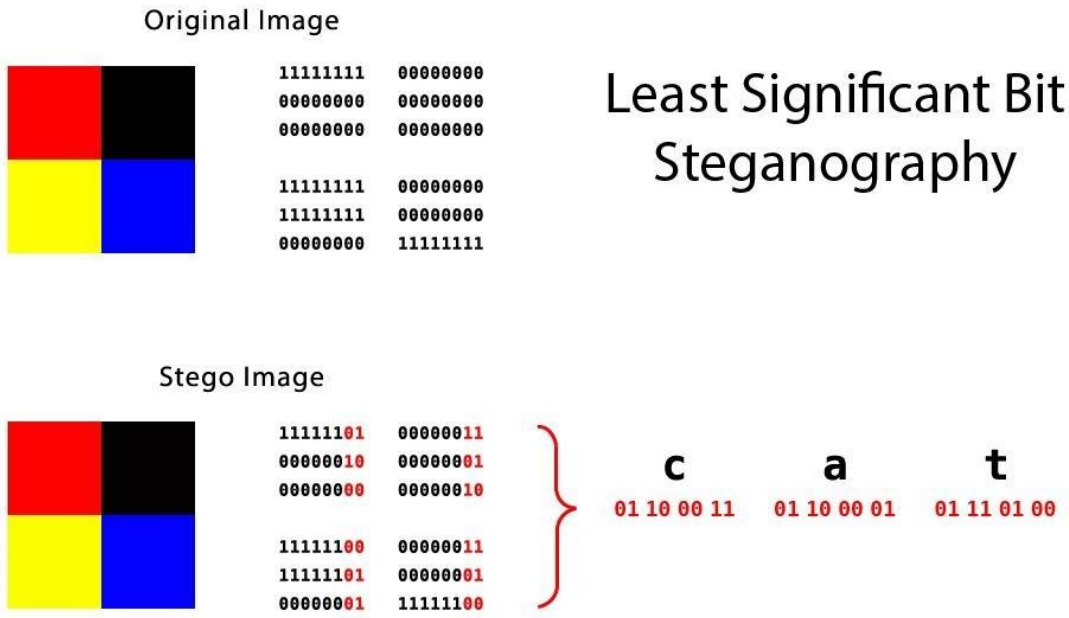
προσεκτικός έλεγχος για τη βέλτιστη συνολική απόδοση. Η παραπάνω ενέργεια είναι απαραίτητη, για να αποφευχθούν ασυνέπειες με άλλους μηχανισμούς ασφαλείας και να διευκολυνθεί το έργο των DLPS. Η ύπαρξη δύο παρόμοιων υπηρεσιών ταυτόχρονα μπορεί να καθυστερήσει ή να διαταράξει τη ροή στο δίκτυο και χρειάζεται ιδιαίτερη προσοχή.

5.3.6. Κρυπτογράφηση και Στεγανογραφία[4].

Για τα DLPS που εφαρμόζονται σε δίκτυο, η κρυπτογράφηση θεωρείται σημαντική πρόκληση. Τα DLPS προσπαθούν να εντοπίσουν αντίγραφα από εμπιστευτικά δεδομένα χρησιμοποιώντας διάφορες τεχνικές ανάλυσης και στη συνέχεια τα συγκρίνουν με τα αρχικά δεδομένα. Όμως η χρήση ισχυρών αλγορίθμων κρυπτογράφησης καθιστά πολύ δύσκολη ή σχεδόν αδύνατη την ανάλυση του περιεχομένου δεδομένων. Για παράδειγμα, ένα μυστικό έγγραφο μπορεί εύκολα να παρακαμφθεί του μηχανισμού ανίχνευσης εάν ένας χρήστης κρυπτογραφήσει το έγγραφο και στη συνέχεια το στείλει ως συνημμένο μέσω email. Σε αυτήν την περίπτωση, ο μηχανισμός ανίχνευσης δεν μπορεί να δει το κρυπτογραφημένο έγγραφο ως απειλή διαρροής και έτσι δεν καταφέρνει να την αποτρέψει. Επιπλέον, πολλές εφαρμογές παρέχουν υπηρεσίες κρυπτογράφησης σε χρήστες, όπως διακομιστές μεσολάβησης SSL και VPN. Σε αυτήν την περίπτωση, η κυκλοφορία δεδομένων είναι ανώνυμη και τα DLPS είναι αναποτελεσματικά, εκτός εάν υπάρχει σωστή συνεργασία και ενσωμάτωση με αυτές τις υπηρεσίες.

Η χρήση στεγανογραφίας, μπορεί να δημιουργήσει μια άλλη πρόκληση παρόμοια με αυτή της κρυπτογραφίας. Τα στεγανογραφικά εργαλεία, όπως φαίνεται στο ακόλουθο σχήμα, χρησιμοποιούν τεχνικές για την απόκρυψη δεδομένων μέσα σε αρχεία άλλης μορφής, όπως ψηφιακές εικόνες, αρχεία ήχου, εμπλουτισμένης μορφής κείμενα κ.τ.λ.

[4] ***Στεγανογραφία*** είναι η πρακτική της απόκρυψης ενός μηνύματος σε άλλο μήνυμα ή ενός φυσικού αντικειμένου. Σε υπολογιστικά / ηλεκτρονικά περιβάλλοντα, ένα αρχείο υπολογιστή, ένα μήνυμα, μια εικόνα ή ένα βίντεο κρύβεται μέσα σε ένα άλλο αρχείο, μήνυμα, εικόνα ή βίντεο.



Εικόνα 5.8: *Στεγανογραφία με τεχνική L.S.B* [28].

Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για να κλαπούν εμπιστευτικά στοιχεία, δεδομένου ότι είναι πολύ πιθανό να παρακαμφθούν από μηχανισμούς ανίχνευσης. Ως εκ τούτου, η κρυπτογράφηση και η στεγανογραφία θεωρούνται απόλυτη πρόκληση για τα τρέχοντα DLPS λόγω τις ιδιαιτερότητας τους.

5.3.7. Ταξινόμηση δεδομένων.

Τα DLPS εξαρτώνται σημαντικά από την κατάλληλη ταξινόμηση δεδομένων. Εάν τα δεδομένα δεν ταξινομούνται σε διαφορετικά επίπεδα και κατηγορίες, τα DLPS δεν είναι ικανά να διακρίνουν σωστά την χρήση κοινών ή εμπιστευτικών πληροφοριών. Σε εφαρμογές στρατιωτικού και κυβερνητικού τομέα μάλιστα, χρησιμοποιούνται όροι ταξινόμησης όπως '*restricted', 'confidential', 'secret'* και *'topsecret'*, που διευκολύνουν τον εντοπισμό εμπιστευτικών δεδομένων. Αυτό μπορεί να κάνει τα DLPS πιο προσανατολισμένα στην προστασία ενός συγκεκριμένου τύπου δεδομένων. Μια άλλη πρόκληση σχετικά με την ταξινόμηση δεδομένων είναι η ανάθεση ευθύνης για τα επίπεδα μυστικότητας. Ως καλή πρακτική είναι οι διαχειριστές ή οι ιδιοκτήτες των δεδομένων να είναι υπεύθυνοι για τον προσδιορισμό τους, δηλαδή για το πόσο ευαίσθητα είναι ή όχι και εάν πρέπει και σε τι βαθμό να προστατεύονται. Δυστυχώς, πολλοί

κάτοχοι δεδομένων αγνοούν αυτήν την πρακτική και αφήνουν εργασίες ταξινόμησης δεδομένων σε αναρμόδιους και λιγότερο καταρτισμένους υπαλλήλους. Αυτό μπορεί να δημιουργήσει ασάφειες που προκαλούν επιδείνωση στην απόδοση κάποιου μηχανισμού DLP. Έτσι, χωρίς κατάλληλα ταξινομημένα δεδομένα, οι εμπιστευτικές πληροφορίες μπορούν εύκολα να αποκαλυφθούν, ακόμη και με τη λειτουργία DLPS.

5.4. Χαρακτηριστικά DLP και Ολοκληρωμένες Λύσεις DLP.

Η παρουσία στην αγορά μηχανισμών DLP είναι σχετικά νέα και προσφέρονται με δύο εκδοχές. Αρχικά υπάρχει η δυνατότητα αγοράς προϊόντων που προσφέρουν συγκεκριμένες λύσεις ασφαλείας, όπως για παράδειγμα προστασία ηλεκτρονικού ταχυδρομείου ή προστασία μεταφοράς αρχείων, αντιγραφής, αποστολής κ.τ.λ., οι οποίες παρέχουν βασικές λειτουργίες προστασίας DLP. Δεύτερον, υπάρχουν ολοκληρωμένοι μηχανισμοί DLP οι οποίοι παρέχουν εξολοκλήρου έλεγχο και προστασία των ευαίσθητων δεδομένων. Οι διαφορές μεταξύ των δύο είναι ότι οι λύσεις με χαρακτηριστικά DLP, περιλαμβάνουν μερικές από τις δυνατότητες ανίχνευσης και τις εφαρμογές προστασίας DLP και δεν είναι στοχευμένες στην προστασία του περιεχομένου των δεδομένων.

Οι ολοκληρωμένες λύσεις DLP περιλαμβάνουν:

- Κεντρική διαχείριση με διεπαφή για το χρήστη σε ανάλογη πλατφόρμα.
- Δυνατότητα δημιουργίας κεντρικών αλλά και στοχευμένων Πολιτικών Ασφαλείας.
- Ειδικά χαρακτηριστικά ανίχνευσης απειλών, αποτελώντας συνήθως μια ολοκληρωμένη λύση λογισμικού DLP ή αυτόνομη συσκευή ή συνδυασμό αυτών.

Αυτή η διάκριση είναι σημαντική, γιατί προϊόντα με χαρακτηριστικά DLP λύνουν συνήθως μόνο συγκεκριμένα προβλήματα των επιχειρήσεων. Εγκαθίστανται δηλαδή για συγκεκριμένο σκοπό και εκτελούν μια προκαθορισμένη λειτουργία εν αντιθέσει με μια ολοκληρωμένη σουίτα DLP που είναι προσανατολισμένη στην παρακολούθηση και προστασία του περιεχομένου των δεδομένων. Την κεντρική αυτή σουίτα, διαχειρίζεται είτε

κάποιος από το τμήμα του οργανισμού που εφαρμόζεται η συγκεκριμένη πολιτική είτε ο διαχειριστής του συστήματος, ο οποίος είναι υπεύθυνος και για τις υπόλοιπες λειτουργίες ασφαλείας. Ορισμένοι οργανισμοί εμπιστεύονται την διαχείριση σε μη τεχνικό προσωπικό και τμήματα που δεν έχουν σχέση με θέματα ασφαλείας. Νομικοί και διοικητικοί υπάλληλοι για παράδειγμα, ορίζονται ως υπεύθυνοι για την προστασία περιεχομένου εμπιστευτικών δεδομένων και πληροφοριών.

Πρέπει να γίνει αντιληπτό από τις εταιρίες ότι η προστασία και η ασφάλεια των δεδομένων που κατέχουν, διαφοροποιείται από άλλα προβλήματα ασφαλείας όπως η απλή προστασία υπολογιστών π.χ. από ιούς ή η προστασία του δικτύου τους. Θα πρέπει να επικεντρωθούν σε χαρακτηριστικά ή ολοκληρωμένες λύσεις DLP ανάλογα για τη κάθε περίπτωση.

Αυτό βέβαια δεν σημαίνει ότι ένα χαρακτηριστικό DLP δεν θα ήταν σωστή λύση για έναν οργανισμό με σχετικά μεγάλο εύρος δραστηριοτήτων ή θα ήταν αντίστοιχα ανασταλτικός παράγοντας για να αγοραστεί μια ολοκληρωμένη σουίτα.

Η σωστή επιλογή του κατάλληλου μηχανισμού ασφαλείας DLP αποτελεί αντικείμενο μελέτης και έρευνας αγοράς για την εύρεση βέλτιστης λύσης προσαρμοσμένης στις ανάγκες ενός οργανισμού, ανάλογα με το μέγεθος και το αντικείμενο δραστηριοποίησής του.

Επίσης, η δημιουργία κεντρικών πολιτικών, η διαχείριση και η ροή εργασίας θα πρέπει να ελέγχονται αποκλειστικά από μια εφαρμογή DLP διαχωρισμένη από άλλους μηχανισμούς ασφαλείας. Θα πρέπει όμως να είναι μεταξύ τους συμβατές και να μπορούν να λειτουργούν συνδυαστικά για να μπορεί να επιτευχθεί το βέλτιστο αποτέλεσμα.

5.5. Εμπορικές και Ακαδημαϊκές προσεγγίσεις DLPS.

Οι δύο αυτοί τομείς έχουν ασχοληθεί με τους μηχανισμούς προστασίας ανεξάρτητα. Δεδομένου ότι τα DLPS είναι σχετικά νέα, τόσο στον ακαδημαϊκό όσο και στον εμπορικό τομέα, εξακολουθεί να μην υπάρχει συμφωνία για μια κατάλληλη κατηγοριοποίηση. Ένα ακαδημαϊκό DLPS συνήθως παρουσιάζεται

ως πλήρης μελέτη μιας συγκεκριμένης ιδέας, επομένως μπορούν να κατηγοριοποιηθούν με βάση τη μέθοδο που χρησιμοποιείται.

Από την άλλη πλευρά, λόγω έλλειψης διαθεσιμότητας ορισμένων από τα χαρακτηριστικά των εμπορικών DLPS, μια κατηγοριοποίηση που μπορεί να γίνει μεταξύ τους, είναι βάση των κοινών και των ειδικών χαρακτηριστικών που έχει κάθε τέτοιος μηχανισμός.

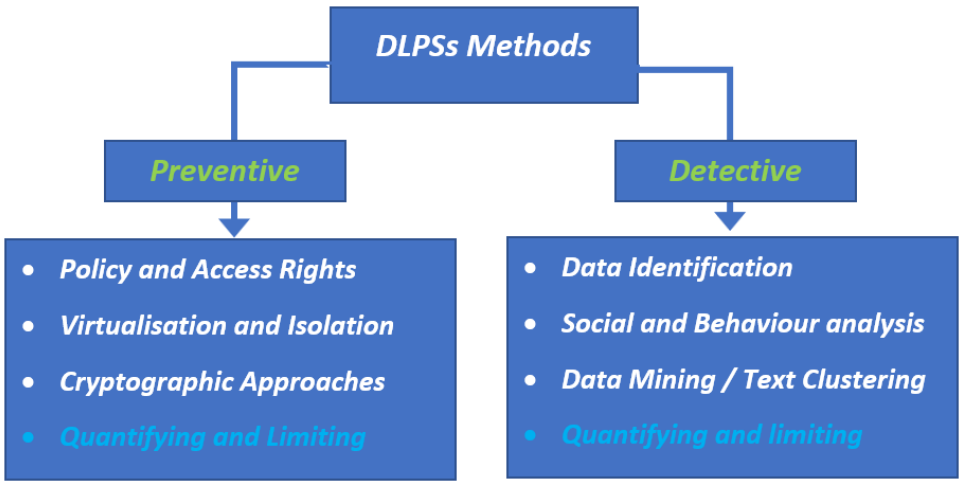
5.5.1. Ακαδημαϊκές προσεγγίσεις.

Αν και ο όρος DLP δεν χρησιμοποιείται ευρέως στην ακαδημαϊκή κοινότητα, πολλές προτεινόμενες μέθοδοι για την πρόληψη διαρροών δεδομένων μπορούν να βρεθούν στη βιβλιογραφία. Αυτές οι μέθοδοι χρησιμοποιούνται είτε για την ανίχνευση είτε για την πρόληψη διαρροών, έτσι ένα ακαδημαϊκό DLP παρουσιάζεται ως πλήρη μελέτη μιας συγκεκριμένης έννοιας.

Τα ακαδημαϊκά DLPS μπορούν να κατηγοριοποιηθούν σύμφωνα με το πεδίο εφαρμογής τους ή τη μέθοδο που χρησιμοποιούν. Καθώς εμφανίζονται συνεχώς νέες προτάσεις των DLPS, η κατηγοριοποίηση τους με βάση την εφαρμογή τους θα οδηγούσε σε πάρα πολλές κατηγορίες και υποκατηγορίες αυτών, ενώ με βάση την μέθοδο που χρησιμοποιούν σε πολύ λιγότερες.

Στο ακόλουθο σχήμα έχουν κατηγοριοποιηθεί τα DLPS με βάση τις δύο κύριες μεθόδους που έχουν επικρατήσει [22] [23]:

1. ***Μέθοδοι Ανίχνευσης*** και
2. ***Μέθοδοι Πρόληψης.***



Εικόνα 5.9: *Κατηγοριοποίηση DLPS μέσω μεθόδων πρόληψης και ανίχνευσης.*

Αυτές οι μέθοδοι συγκεντρώθηκαν και κατατάσσονται σε επτά κατηγορίες, όπως περιγράφονται πιο κάτω, με κάποια από τα δυνατά και αδύνατά τους σημεία.

- ***Ποσοτικοποίηση και Περιορισμός.***

Σημειώνεται ότι η κατηγορία “Ποσοτικοποίηση και Περιορισμός” (Quantifying and Limiting) θεωρείται κοινή και των δύο μεθόδων.

Πολλές δραστηριότητες, όπως η αναζήτηση στο διαδίκτυο, η εκτέλεση μιας διαδικασίας ή η πρόσβαση σε ένα συγκεκριμένο αρχείο, μπορεί να απελευθερώσουν ευαίσθητα δεδομένα. Ακόμα κι αν τα δεδομένα που έχουν κυκλοφορήσει δεν θεωρούνται ευαίσθητα από τον κάτοχο τους, μπορεί να βοηθήσουν έναν αντίπαλο για παράδειγμα, να αποκτήσει πληροφορίες σχετικά με άλλα δεδομένα που μπορεί να είναι σημαντικά.

Για να ξεπεραστούν τέτοια προβλήματα, οι διαχειριστές ασφαλείας προσπαθούν να μιμηθούν τη δράση ενός εισβολέα χρησιμοποιώντας μεθόδους ποσοτικοποίησης για τον έλεγχο ευαίσθητων δεδομένα και στη συνέχεια να μπλοκάρουν τις περιττές διαρροές. Μια προσέγγιση ποσοτικοποίησης χρησιμοποιεί τη βασική θεωρία των πληροφοριών για ανάλυση της ποσότητα ευαίσθητων δεδομένων. Αυτά τα ευαίσθητα δεδομένα ενδέχεται να κυκλοφορήσουν από προγράμματα γραμμένα σε μια πολύ απλή επιτακτική γλώσσα. Επιπλέον, η προσέγγιση αυτή προσπαθεί να ελέγξει το απόλυτο ποσοστό διαρροής, έως ενός bit, χρησιμοποιώντας δύο ποσοτικά μοντέλα διαρροής πληροφοριών. Μια άλλη προσέγγιση είναι η μέτρηση για τον περιορισμό του μέγιστου όγκου των ευαίσθητων δεδομένων κυκλοφορίας στον ιστό, αντί να προσπαθούν να εντοπίσουν την παρουσία ευαίσθητων δεδομένων. Η προσέγγιση αυτή χρησιμοποιεί έναν αλγόριθμο μέτρησης κυκλοφορίας για το πρωτόκολλο HTTP. Οι παραπάνω μέθοδοι μπορούν να λύσουν προβλήματα που σχετίζονται με τη διαρροή δεδομένων, όπως είναι η

Επίθεση Σαλαμιού[5] ή το ***Κρυφό Κανάλι***[6]***.*** Ωστόσο, υπάρχουν και μερικοί περιορισμοί. Για παράδειγμα δεν είναι σε θέση να φιλτράρουν μέρη ομοιόμορφων δεδομένων που περιέχουν τυχαίους αριθμούς και να τα αποτρέψουν. Μπορεί επίσης, να έχουν προβλήματα κατά τον ποσοτικό προσδιορισμό των δεδομένων που έχουν κυκλοφορήσει και δεν είναι γραμμένα σε απλή επιτακτική γλώσσα.

Στον πιο κάτω πίνακα αναφέρονται περιεκτικά κάποια από τα πλεονεκτήματα και μειονεκτήματα της συγκεκριμένης κατηγορίας.

Πίνακας 5.1: *Αδυναμίες και Πλεονεκτήματα κατηγορίας: (Ποσοτικοποίηση και Περιορισμός).*

Πλεονεκτήματα	***Αδυναμίες***
• Αποτελεσματικό για όλες τις καταστάσεις δεδομένων.	• Δεν εξασφαλίζει αποκλεισμό του διαύλου διαρροής.
• Χρήσιμο κατά συγκεκριμένων τύπων επιθέσεων, όπως επιθέσεις σαλαμιού.	• Περιορίζεται σε συγκεκριμένες καταστάσεις ή σενάρια επιθέσεων.
• Δεν εστιάζεται στη μελέτη ευαίσθητων δεδομένων αλλά επικεντρώνεται σε διαύλους διαρροής.	• Μπορεί να διαταράξει την ομαλή ροή εργασίας.

[5] Η ***Επίθεση σαλαμιού*** είναι μια σειρά μικρών επιθέσεων που μαζί οδηγούν σε μεγαλύτερη επίθεση, η ιδέα είναι να γίνονται αρκετά μικρές αλλοιώσεις / αλλαγές ώστε να μην μπορούν να εντοπιστούν.

[6] ***Κρυφό κανάλι*** είναι ένας τύπος επίθεσης που δημιουργεί τη δυνατότητα μεταφοράς πληροφοριών μεταξύ διαδικασιών που δεν επιτρέπεται να επικοινωνούν από τις πολιτικές ασφάλειας του υπολογιστή.

5.5.1.1. Μέθοδοι Πρόληψης.

- ***Πολιτικές και Δικαιώματα Πρόσβασης.***

Η πρόληψη διαρροών δεδομένων μέσω αυστηρών πολιτικών ασφαλείας και δικαιωμάτων πρόσβασης, εφαρμόζεται ευρέως από πολλούς οργανισμούς, ακόμη και πριν την εμφάνιση των DLPS, ως ανεξάρτητης τεχνολογίας. Στη βιβλιογραφία υπάρχουν ορισμένες προσεγγίσεις διαχείρισης DLPS που χρησιμοποιούν πολιτικές ασφάλειας, ταξινόμησης δεδομένων και δικαιωμάτων πρόσβασης. Μερικά DLPS εγκατεστημένα σε κεντρικούς υπολογιστές λειτουργούν απενεργοποιώντας τις μονάδες δίσκου USB και CD. Αυτά τα συστήματα DLP λειτουργούν σύμφωνα με μια πολιτική ασφαλείας, όπως είναι η αποτροπή μιας συγκεκριμένης ομάδας χρηστών ή τμημάτων από τη χρήση αφαιρούμενων μέσων σε προσωπικούς υπολογιστές. Τα DLPS που επιτηρούν δεδομένα σε κατάσταση ηρεμίας (DAR), ακολουθούν μία υπάρχουσα πολιτική ασφαλείας, βάσει της οποίας επιτρέπεται ή όχι η πρόσβαση και σε ποιο βαθμό. Για να λειτουργούν όσο το δυνατόν ορθότερα, αυτοί οι τύποι DLPS συνήθως εισάγουν τα δικαιώματα πρόσβασης του οργανισμού από καταλόγους, όπως το Microsoft Active Directory. Σε έναν τομέα οργανισμού, για να συνδεθεί μια συσκευή, θα πρέπει να επικοινωνήσει με τον κύριο ελεγκτή στέλνοντας ένα αίτημα. Σύμφωνα με μια πρόταση [29] ασφαλούς σύνδεσης, ο κύριος ελεγκτής θα πρέπει να είναι ικανός να προσδιορίσει τη δική του θέση, ενσωματώνοντας ένα δέκτη δορυφορικού εντοπισμού θέσης (GPS), ή χρησιμοποιώντας δίκτυα κινητής τηλεφωνίας, 3G για παράδειγμα. Στη συνέχεια, ο ελεγκτής μετρά την απόλυτη απόσταση μεταξύ του και της συσκευής που έστειλε το αίτημα σύνδεσης, υπολογίζοντας την τοποθεσία της. Ο ελεγκτής χρησιμοποιεί το αποτέλεσμα για να αποφασίσει εάν τα αίτημα γίνει δεκτό ή όχι. Για να επιτραπεί η σύνδεση θα πρέπει η τοποθεσία να είναι κάποια καταχωρημένη διεύθυνση ή η συσκευή να βρίσκεται κοντά με στον ελεγκτή, ελέγχοντάς την, χρησιμοποιώντας τεχνολογία (NFC) για παράδειγμα.

Με την χρησιμοποίηση υπηρεσιών τοποθεσίας, προστίθεται ένα επιπλέον επίπεδο προστασίας, διασφαλίζοντας ότι ο κύριος ελεγκτής και οι συνδεδεμένες συσκευές μπορούν να λειτουργήσουν μόνο μέσα στις εγκαταστάσεις ενός

οργανισμού ή σε προκαθορισμένες τοποθεσίες. Επιπλέον, αυτό διασφαλίζει τα δεδομένα σε περιπτώσεις που μπορεί να κλαπεί ο ελεγκτής, αφού δεν θα λειτουργήσει εκτός των εγκαταστάσεων του οργανισμού.

Τέλος, ένα DLP που βασίζεται σε πολιτικές ασφάλειας και δικαιώματα πρόσβασης, είναι ο απλούστερος τρόπος πρόληψης μιας διαρροής δεδομένων, επειδή στις μέρες μας είναι αρκετά ώριμη και ακολουθεί παγιωμένες και για χρόνια δοκιμασμένες μεθόδους.

Όπως αναφέρθηκε νωρίτερα, ακατάλληλη ταξινόμηση δεδομένων ή η μη συντήρηση των δικαιωμάτων πρόσβασης μπορούν να επηρεάσουν δραματικά την απόδοση ενός DLP.

Στον πιο κάτω πίνακα αναφέρονται κάποια από τα πλεονεκτήματα και μειονεκτήματα της συγκεκριμένης κατηγορίας.

Πίνακας 5.2: *Αδυναμίες και Πλεονεκτήματα κατηγορίας (Πολιτική και Δικαιώματα Πρόσβασης).*

Πλεονεκτήματα	***Αδυναμίες***
• Κατάλληλο για οργανισμούς όπου τα δικαιώματα πρόσβασης και η ταξινόμηση δεδομένων έχουν καθοριστεί σωστά.	• Επηρεάζεται από ακατάλληλη ταξινόμηση δεδομένων.
• Εύκολη διαχείριση.	• Επηρεάζεται από την πολιτική ελέγχου πρόσβασης που χρησιμοποιείται.
• Κατάλληλο για δεδομένα σε χρήση (DIU) και σε ηρεμία (DAR).	• Δεν είναι μέθοδος ανίχνευσης, επομένως εάν συμβαίνει διαρροή, η μέθοδος είναι αναποτελεσματική.
• Ισχυρός μηχανισμός πρόληψης.	

- ***Εικονικοποίηση και Απομόνωση.***

Η μέθοδος εικονικοποίησης και απομόνωσης DLP χρησιμοποιεί ετικέτες σήμανσης για την προστασία ευαίσθητων δεδομένων. Η μέθοδος βασίζεται στη δημιουργία εικονικού περιβάλλοντος κατά την πρόσβαση σε ευαίσθητα δεδομένα. Εκεί οι δραστηριότητες των χρηστών είναι απομονωμένες και αξιόπιστες, δημιουργώντας αξιόπιστους εικονικούς τομείς που είναι συνδεδεμένοι μέσω ασφαλών συνδέσεων. Οι υπολογιστικές λειτουργίες και υπηρεσίες μπορούν να λειτουργούν σε αξιόπιστα περιβάλλοντα και μπορούν έτσι να διατηρούν τις όποιες απαιτήσεις ασφαλείας. Μια άλλη ιδέα βασίζεται στη χρήση δύο διαφορετικών εικονικών μηχανών. Η μία έχει απεριόριστη πρόσβαση στο διαδίκτυο και σε εξωτερικό περιβάλλον και η άλλη χρησιμοποιείται μόνο για την επεξεργασία ευαίσθητων δεδομένων. Ο διαχωρισμός των δύο εικονικών μηχανών, αποτρέπει κάθε αρνητική επίδραση μεταξύ τους. Μόνο αξιόπιστες εφαρμογές επιτρέπεται να έχουν πρόσβαση στο διαδίκτυο χρησιμοποιώντας αποκλειστικά την δημόσια εικονική μηχανή.

Μία άλλη μέθοδος προτείνει την απομόνωση χρηστών όταν έχουν πρόσβαση σε ευαίσθητα δεδομένα. Ένα DLP παρέχει ασφαλή χώρο αποθήκευσης με τεχνολογίες εικονικής απομόνωσης, επειδή οι πιο σοβαρές απειλές προέρχονται εκ των έσω, δηλαδή από χρήστες με προνόμια, ειδικοί μηχανισμοί πραγματοποιούν μια ανάλυση ροής πληροφοριών για κάθε χρήστη. Για παράδειγμα, εάν ο χρήστης ζητήσει πρόσβαση σε ευαίσθητα δεδομένα, θα ελεγχθεί πρώτα η διαδικασία και εάν ο έλεγχος ταυτότητας περάσει, τότε θα δημιουργηθεί ένα απομονωμένο περιβάλλον με ένα αξιόπιστο κανάλι μεταξύ του χρήστη και των δεδομένων για να διασφαλιστεί ότι όλες οι διαδικασίες είναι διαθέσιμες και χρησιμοποιήθηκαν σωστά.

Κάποια από τα πλεονεκτήματα και τα μειονεκτήματα της συγκεκριμένης κατηγορίας αναφέρονται στον πιο κάτω πίνακα.

Πίνακας 5.3: *Αδυναμίες και Πλεονεκτήματα κατηγορίας (Εικονικοποίηση και Απομόνωση).*

Πλεονεκτήματα	***Αδυναμίες***
• Δεν απαιτεί μεγάλη υλοποίηση σε εξοπλισμό.	• Δεν είναι αρκετά ώριμη.
• Δεν χρειάζεται τακτική παρέμβαση από τους Διαχειριστές.	• Δεν είναι μέθοδος ανίχνευσης.
• Η πρόσβαση σε ευαίσθητα δεδομένα μπορεί να χρησιμοποιήσει την υπάρχουσα ταξινόμηση δεδομένων.	

- ***Κρυπτογραφικές Προσεγγίσεις.***

Η κρυπτογραφία χρησιμοποιείται συνήθως για την προστασία δεδομένων από μη εξουσιοδοτημένη αποκάλυψη. Τα κρυπτογραφικά εργαλεία και οι αλγόριθμοι έχουν φτάσει σε ένα επίπεδο ωριμότητας όπου είναι εξαιρετικά δύσκολη ή σχεδόν αδύνατη η αποκρυπτογράφηση δεδομένων χωρίς το σωστό κλειδί. Ο σκοπός της χρήσης κρυπτογραφίας είναι να κάνει δύσκολη την ανάγνωση και την κατανόηση της πληροφορίας. Ωστόσο αυτό δεν μπορεί να εμποδίσει κάποιον κακόβουλο, να αποκτήσει τα κρυπτογραφημένα δεδομένα. Για παράδειγμα, κρυπτογραφημένα email και ασφαλείς συνδέσεις μέσω HTTPS και VPN είναι μέθοδοι που χρησιμοποιούνται για την προστασία των δεδομένων από ανεπιθύμητη ανάγνωση κατά την μεταφορά τους. Αυτό επιτυγχάνεται, ακόμη και όταν τα δεδομένα ταξιδεύουν σε μη αξιόπιστα περιβάλλοντα και είναι ευάλωτα από τρίτους. Επομένως η κρυπτογράφηση, μπορεί να διασφαλίσει το απόρρητο του απλού κειμένου αλλά όχι του κρυπτογραφημένου (ciphertext). Αυτό μπορεί να οδηγήσει σε διάφορων τύπων επιθέσεις όπως:

- *ciphertext-attack* [7]
- *known-plaintext* [8] και
- *chosen-plaintext attacks.*[9]

Αν και η πρόληψη διαρροών δεδομένων ως γενικός όρος σημαίνει στην ουσία προστασία των δεδομένων, θα μπορούσαν κάποιοι μηχανισμοί κρυπτογράφησης να ονομαστούν DLPS. Όμως μέθοδοι κρυπτογράφησης, που διαχειρίζονται δεδομένα σε μεταφορά (DIM), δεν μπορούν να χαρακτηριστούν DLPS, γιατί εμπλέκονται στην απελευθέρωση ψηφιακών αποτυπωμάτων και κρυπτογραφημένων δεδομένων. Ωστόσο, ορισμένες προσεγγίσεις χρησιμοποιούν κρυπτογράφηση για να αποτρέψουν τη διαρροή σε δεδομένα που χρησιμοποιούνται σε κατάσταση ηρεμίας (DAR) και δεδομένα σε χρήση (DIU). Αυτά τα συστήματα προστατεύουν δεδομένα από αντιπάλους με φυσική πρόσβαση σε υπολογιστές και συσκευές αποθήκευσης. Για παράδειγμα, εάν ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε έναν κρυπτογραφημένο φάκελο, τότε θα ζητηθεί να εισάγει ένα κλειδί ή έναν κωδικό πρόσβασης για την αποκρυπτογράφηση του αρχείου, ενώ η πρόσβαση θα απορριφθεί εάν το κλειδί δεν είναι το σωστό.

---

[7] Στην κρυπτογραφία, η επίθεση ***ciphertext attack*** είναι ένα μοντέλο επίθεσης για κρυπτοανάλυση, όπου ο εισβολέας θεωρείται ότι έχει πρόσβαση μόνο σε ένα σύνολο ciphertexts. Από αυτά τα στοιχεία ο αντίπαλος μπορεί να επιχειρήσει να ανακτήσει το κρυφό μυστικό κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση.

[8] Η ***known-plaintext attack (KPA)*** είναι ένα μοντέλο επίθεσης για κρυπτοανάλυση όπου ο εισβολέας έχει πρόσβαση τόσο στο απλό κείμενο, όσο και στην κρυπτογραφημένη έκδοση (ciphertext). Αυτά μπορούν να χρησιμοποιηθούν για να αποκαλύψουν περαιτέρω μυστικές πληροφορίες, όπως μυστικά κλειδιά και κομμάτια κώδικα.

[9] Μια επίθεση ***chosen-plaintext attack (CPA)*** είναι ένα μοντέλο επίθεσης για κρυπτοανάλυση που προϋποθέτει ότι ο εισβολέας μπορεί να αποκτήσει τα κρυπτογραφήματα για αυθαίρετα απλό κείμενο. Ο στόχος της επίθεσης είναι να αποκτήσει πληροφορίες που μειώνουν την ασφάλεια του σχήματος κρυπτογράφησης.

Τα προϊόντα DLP θα πρέπει να είναι αρκετά «έξυπνα» ώστε να είναι επιλεκτικά σχετικά με την κρυπτογράφηση, χρησιμοποιώντας την μόνο όταν χρειάζεται. Στην πράξη, εάν ένας χρήστης τοποθετήσει π.χ. μια εμπιστευτική βάση δεδομένων σε ένα USB stick ή στείλει ένα e-mail που περιέχει ευαίσθητα δεδομένα, το DLP θα πρέπει να αναγνωρίσει ότι το περιεχόμενο πρέπει να προστατευτεί, για να ενεργοποιηθεί αυτόματα η κρυπτογράφηση. Σε αυτές τις περιπτώσεις, τα DLP θα πρέπει να λειτουργούν συνδυαστικά για βέλτιστο αποτέλεσμα.

Μια άλλη ιδέα είναι η χρήση ενός προσωρινού κρυπτογραφικού κλειδιού ανά σύνδεση χρήστη. Αυτό το κλειδί χρησιμοποιείται για την αποθήκευση ευαίσθητων δεδομένων απευθείας σε μια απομακρυσμένη συσκευή αποθήκευσης και έχει περιορισμένο αριθμό χρήσεων ή ακόμη και ισχύ για μία μόνο χρήση. Ωστόσο, αυτή η μέθοδος απαιτεί επιπρόσθετο και πολλές φορές πολύπλοκο εξοπλισμό προσαρμοσμένο με ένα υπάρχον σύστημα ασφαλών συνδέσεων, το οποίο ενδέχεται να μην είναι διαθέσιμο σε ορισμένους οργανισμούς.

Πλεονεκτήματα και μειονεκτήματα της συγκεκριμένης κατηγορίας αναφέρονται στον πιο κάτω πίνακα.

Πίνακας 5.4: *Αδυναμίες και Πλεονεκτήματα κατηγορίας (Κρυπτογραφικές Προσεγγίσεις).*

Πλεονεκτήματα	***Αδυναμίες***
• Ισχυρή κρυπτογράφηση, παράγει μέγιστη ασφάλεια.	• Η κρυπτογραφία μπορεί να εξασφαλίσει ευαίσθητα δεδομένα, αλλά δεν μπορεί να αποκρύψει την ύπαρξή τους.
• Αρκετές κρυπτογραφικές μέθοδοι σε χρήση με πολλές επιλογές.	• δεν εντοπίζει διαρροή δεδομένων.
	• Σε εμπιστευτικά δεδομένα μπορεί να υπάρχει πρόσβαση με αδύναμα διαπιστευτήρια.

5.5.1.2. Μέθοδοι Ανίχνευσης.

- ***Ταυτοποίηση Δεδομένων.***

Τα περισσότερα DLPS ανιχνεύουν ευαίσθητα δεδομένα εντός νόμιμης κυκλοφορίας πραγματοποιώντας επιθεώρηση πακέτων σε βάθος. Αυτή η μέθοδος χρησιμοποιείται σε πολλές εφαρμογές, όπως antivirus και spam filtering. Η μέθοδος αυτή απαιτεί προηγούμενη γνώση του στοχευμένου περιεχομένου, συμπεριλαμβανομένων ψηφιακών αποτυπωμάτων δεδομένων (fingerprints), κανονικών εκφράσεων και ακριβής ή μερικής αντιστοίχισης δεδομένων. Τα ψηφιακά αποτυπώματα δημιουργούνται μέσω κατακερματισμού εμπιστευτικών δεδομένων, ενώ η κανονική έκφραση δημιουργείται από ακολουθίες χαρακτήρων που σχηματίζουν μοτίβα ανίχνευσης. Η ακριβής και μερική αντιστοίχιση δεδομένων χρησιμοποιεί διάφορες λειτουργίες ομοιότητας για την αντιστοίχιση της επιθεωρημένης κίνησης με τα υπάρχοντα εμπιστευτικά δεδομένα.

Ένας μηχανισμός DLP που προτάθηκε, εισήγαγε μια τεχνική ανίχνευσης μέσω δικτύου με βάση την ανάγνωση μηνυμάτων ή τα ψηφιακά αποτυπώματα, για τον εντοπισμό ακούσιων διαρροών δεδομένων σε κίνηση. Όταν ένας υπάλληλος για παράδειγμα, επισυνάπτει κατά λάθος τις οικονομικές καταστάσεις του οργανισμού σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου και πατά «αποστολή». Ο μηχανισμός βοηθά σε αυτές τις περιπτώσεις, τα άτομα και τα συστήματα να κατανοήσουν πώς να χειρίζονται ορισμένους τύπους ευαίσθητων δεδομένων μέσω οπτικών σημάνσεων ή απενεργοποιώντας αντίστοιχες λειτουργίες.

Άλλες λύσεις επικεντρώνονται στον εντοπισμό δεδομένων σε κατάσταση ηρεμίας. Αυτό είναι σημαντικό επειδή οι οργανισμοί και οι εργαζόμενοι συνήθως αποθηκεύουν πολύ περισσότερα δεδομένα και πληροφορίες από ό,τι πραγματικά χρειάζονται. Αυτά τα δεδομένα συχνά βρίσκονται σε μη διαχειριζόμενους διακομιστές επ' αόριστον και παρουσιάζουν έναν συχνά υποτιμημένο κίνδυνο απορρήτου για τους οργανισμούς και τους υπαλλήλους. Η τεχνική ανίχνευσης χρησιμοποιεί ειδικές συγχωνεύσεις και δείγματα αντί να

χειρίζεται όλα τα ευαίσθητα δεδομένα, γεγονός που ελαχιστοποιεί την άσκοπη έκθεση τους σε κίνδυνο.

Υπάρχουν εργαλεία προστασίας και μηχανισμοί, που επιτυγχάνουν όλα τα παραπάνω χρησιμοποιώντας συνδυασμό τεχνολογιών, με τη λειτουργία μηχανικής εκμάθησης, για τον εντοπισμό ευαίσθητων δεδομένων και την εφαρμογή κατάλληλων προστασιών στο σημείο δημιουργίας τους. Τα εργαλεία αυτά, απαιτούν λιγότερη εκπαίδευση και επεξεργάζονται δεδομένα τόσο σε κίνηση όσο και κατά την αποθήκευσή τους. Εντοπίζουν και αναγνωρίζουν δεδομένα αμέσως μόλις δημιουργηθούν και τα παρακολουθούν κατά τη διάρκεια ολόκληρου του κύκλου ζωής τους.

Αυτός είναι ο λόγος για τον οποίο η ύπαρξη μιας λύσης αναγνώρισης και ταξινόμησης δεδομένων γίνεται όλο και πιο απαραίτητη και παράλληλα βοηθά να περιοριστούν στο ελάχιστο τα ανεπιθύμητα συμβάντα.

Κάποια από τα πλεονεκτήματα και μειονεκτήματα της συγκεκριμένης κατηγορίας αναφέρονται στον πιο κάτω πίνακα.

Πίνακας 5.5: *Αδυναμίες και Πλεονεκτήματα κατηγορίας (Ταυτοποίηση Δεδομένων).*

Πλεονεκτήματα	***Αδυναμίες***
• Πολύ ισχυρό στην ανίχνευση μη δομημένων δεδομένων.	• Εξαιρετικά τροποποιημένα δεδομένα δεν μπορούν να εντοπιστούν.
• Πολύ χαμηλό επίπεδο ψευδώς θετικών συναγερμών χρησιμοποιώντας αποτυπώματα δεδομένων.	• Στερείται σημασιολογικής κατανόησης.
• Με ισχυρό κατακερματισμό μπορεί να ανιχνεύσει τροποποιημένα δεδομένα.	

- ***Κοινωνική ανάλυση και ανάλυση Συμπεριφοράς.***

Η ανάλυση του κοινωνικού δικτύου εστιάζεται στη χαρτογράφηση και τη μέτρηση αλληλεπιδράσεων και σχέσεων μεταξύ ανθρώπων, ομάδων και οργανισμών, αναπαριστώντας τις αλληλεπιδράσεις σε όρους κόμβων και συνδέσμων. Οι κοινωνικές αλληλεπιδράσεις περιλαμβάνουν email, IM και κοινωνικά δίκτυα. Σχεδιάζοντας συνδέσμους μεταξύ κόμβων και αναλύοντας χαρακτηριστικά όπως η φύση, η συχνότητα και το μέγεθος των συναλλαγών, είναι δυνατό να απεικονιστεί ένας μεγάλος χάρτης σχέσεων επικοινωνιών μεταξύ οντοτήτων. Αν και η ανθρώπινη συμπεριφορά είναι απρόβλεπτη, δεν είναι πάντα τυχαία. Ως εκ τούτου, είναι χρήσιμο να διατηρείται ένα ιστορικό ανθρώπινων αντιδράσεων για ανάλυση συμπεριφοράς. Ένα DLP που χρησιμοποιεί ανάλυση κοινωνικής δικτύωσης και συμπεριφοράς, ελέγχει τη ροή δεδομένων μεταξύ των χρηστών, εντοπίζοντας τυχόν παρατυπίες και στη συνέχεια ενεργοποιεί έναν συναγερμό, ώστε ένας διαχειριστής ασφαλείας να μπορεί να αντιδράσει ανάλογα.

Μια άλλη προσέγγιση για την αποτροπή διαρροής δεδομένων μέσω ηλεκτρονικού ταχυδρομείου, βασίζεται σε ανάλυση και υλοποιείται με προσδιορισμό κοινών θεμάτων που πιθανώς υπάρχουν. Μια σχέση που χρησιμοποιεί συνάρτηση όρων και συχνότητας ανταλλαγής εγγράφων, σχεδιάζεται μεταξύ μελών που χρησιμοποιούν κοινά θέματα. Έπειτα, αναπτύσσεται ένα μοντέλο ταξινόμησης που αποτελείται από δύο φάσεις (εκπαίδευση και ταξινόμηση). Αυτό το μοντέλο ταξινόμησης χρησιμοποιεί την ομοιότητα του υπάρχοντος ιστορικού μεταξύ των χρηστών ως βασική γραμμή εντοπισμού. Εάν το ανταλλασσόμενο θέμα έχει μικρή ομοιότητα με το υπάρχον ιστορικό, θα μπορούσε να υπάρξει διαρροή. Αυτή η μέθοδος έχει περιορισμούς, όπως ψευδείς θετικές διαρροές εάν δεν υπάρχει επαρκές ιστορικό μεταξύ ενός αποστολέα και ενός παραλήπτη.

Ένα άλλο μοντέλο για την ανάλυση της ανθρώπινης συμπεριφοράς είναι να δημιουργηθεί ένα προφίλ συμμόρφωσης για κάθε περίπτωση ή παράβασης και στη συνέχεια να συγκρίνονται νέες περιπτώσεις με τα υπάρχοντα προφίλ χρηστών. Μια τέτοια μέθοδος μπορεί να προβλέψει ως ένα βαθμό τη μελλοντική ανθρώπινη συμπεριφορά.

Ωστόσο, χρειάζεται να αναλυθούν, υπάρχοντα ή εικονικά προφίλ συμμόρφωσης για τη διαδικασία εκμάθησης και σύγκρισης, αλλά δυστυχώς μπορεί να προκληθούν ορισμένες αστοχίες κατά τον προσδιορισμό των ορίων ανίχνευσης.

Επίσης, μια προσέγγιση που χρησιμοποιείται στην ασφάλεια πληροφοριών για την παρακολούθηση κακόβουλων δραστηριοτήτων, είναι τα honeypots. Τα honeypots είναι εικονικά περιβάλλοντα που δημιουργήθηκαν για να εξαπατήσουν τους αντιπάλους να πέσουν σε παγίδα, επιτρέποντας σε εξωτερικούς και κακόβουλους χρήστες να έχουν πρόσβαση σε πλαστά αποθετήρια δεδομένων. Εξελιγμένες προσεγγίσεις των honeypots, με χρήση μηχανικής μάθησης και τεχνητής νοημοσύνης, αλλάζουν τη συμπεριφορά τους ανάλογα με τις ενέργειες ενός επιτιθέμενου. Σε γενικές γραμμές, τα δυναμικά honeypots [30] έχουν συμπεριφορά που δεν είναι σταθερή αλλά αλλάζει με βάση κάποια κατάσταση και προσαρμόζονται στο τρέχον περιβάλλον. Τα honeypots μπορούν στρατηγικά να εμποδίσουν την εκτέλεση ή να αλλάξουν τα ονόματα ορισμένων προγραμμάτων, προκειμένου να δελεάσουν τους επιτιθέμενους και να τους εξαπατήσουν με σκοπό να αποκαλύψουν κάποιο στοιχείο για την ταυτότητά τους.

Μια άλλη προσέγγιση, είναι η ιδέα της διαστρέβλωσης και διανομής πλαστών στοιχείων [31] με σκοπό την αποκάλυψη πιθανών υποκλοπών. Έτσι ο διαχειριστής του συστήματος μπορεί να μελετήσει κάποια ύποπτη συμπεριφορά και να αποτρέψει πιθανή διαρροή δεδομένων. Τα ψεύτικα αντικείμενα πρέπει να δημιουργούνται προσεκτικά, έτσι ώστε να μην μπορούν να διακριθούν από τα αληθινά. Ωστόσο, μπορούν να επηρεάσουν την ορθότητα των πραγματικών δεδομένων, οπότε χρειάζεται ιδιαίτερη προσοχή, καθώς υπάρχουν και περιπτώσεις όπου η τεχνική αυτή δεν μπορεί να εφαρμοστεί. Για παράδειγμα, ας υποθέσουμε ότι τα κατανεμημένα δεδομένα είναι ιατρικά αρχεία ασθενών σε νοσοκομεία. Σε αυτή την περίπτωση, ακόμα και μικρές τροποποιήσεις στα αρχεία των πραγματικών ασθενών μπορεί να είναι ανεπιθύμητες. Όμως, η προσθήκη ορισμένων πλαστών ιατρικών φακέλων μπορεί να είναι αποδεκτή, καθώς κανένας ασθενής δεν θα ταιριάζει με αυτά τα αρχεία και ως εκ τούτου, κανείς δεν θα αντιμετωπιστεί ποτέ με βάση ψεύτικα αρχεία.

Στον πιο κάτω πίνακα αναφέρονται κάποια πλεονεκτήματα και μειονεκτήματα.

Πίνακας 5.6: *Αδυναμίες και Πλεονεκτήματα κατηγορίας (Κοινωνική ανάλυση και ανάλυση Συμπεριφοράς).*

Πλεονεκτήματα	***Αδυναμίες***
• Πρόληψη διαρροής δεδομένων με εντοπισμό κακόβουλων σχέσεων.	• Παράγει υψηλά επίπεδα ψευδώς θετικών συναγερμών.
• Κατάλληλο για όλες τις καταστάσεις δεδομένων.	• Απαιτεί συχνές παρεμβάσεις από διαχειριστές.
	• Απαιτεί τεράστιο αριθμό προφίλ και ευρετηρίασης.

- ***Εξόρυξη δεδομένων και Ομαδοποίηση κειμένων.***

Το πεδίο εξόρυξης δεδομένων έχει πολλές δυνατότητες για την εκτέλεση εξελιγμένων διαδικασιών, όπως *ανίχνευση ανωμαλιών, ομαδοποίηση* και *ταξινόμηση*, εξάγοντας μοτίβα από μεγάλα σύνολα δεδομένων. Η εξόρυξη δεδομένων σχετίζεται στενά με τη μηχανική μάθηση, η οποία έχει ένα σύνολο αλγορίθμων ικανών να χειρίζονται μεγάλα σύνολα δεδομένων και να αναγνωρίζουν πολύπλοκα μοτίβα, προσπαθώντας να λάβουν κατάλληλες αποφάσεις σχετικά με τη διαχείρισή τους. Ως εκ τούτου, η ιδέα είναι να χρησιμοποιηθούν φάσεις κατάρτισης και δοκιμών μηχανικής μάθησης για να είναι σε θέση να ανιχνεύσουν γεγονότα απώλειας δεδομένων μέσω ευφυών μοντέλων που βασίζονται σε υπάρχον ιστορικό διαχείρισης δεδομένων. Η μηχανική μάθηση και η βαθιά ανάλυση δεδομένων έχουν χρησιμοποιηθεί ιστορικά για την επιτυχή αντιμετώπιση διαφόρων προκλήσεων ασφάλειας στον κυβερνοχώρο και έχουν αποδεδειγμένη ικανότητα να εκπαιδεύονται από πραγματικά δεδομένα και να επιλύουν προβλήματα βοηθώντας στη πρόβλεψη και ανίχνευση διαρροής δεδομένων.

Επιπλέον, προτείνεται η εφαρμογή μιας προσέγγισης [32] βασισμένη σε βαθμολόγηση χρηστών, όπου μπορεί να υποδείξει πιθανή διαρροή δεδομένων

μέσω εσωτερικής απειλής. Κύριος στόχος είναι να κατατάξει τους χρήστες με βάση διάφορους παράγοντες, να τους βαθμολογήσει και να μπορέσει να προβλέψει ευάλωτους χρήστες που ενδεχομένως είναι επικίνδυνοι για τον οργανισμό και τα συστήματα πληροφορικής. Η βαθμολογία συγκρίνεται με την ταξινόμηση που ορίζεται από το σύστημα, προκειμένου κάθε χρήστης να συγκριθεί με προηγούμενη συμπεριφορά του καθώς και με τη συμπεριφορά της ομάδας που ανήκει. Εάν εντοπιστεί διαρροή, ο αποστολέας λαμβάνει ποινή και ο παραλήπτης λαμβάνει θετική ανταμοιβή. Οι βαθμολογίες βασίζονται σε αριθμό γνωστών χαρακτηριστικών και σε συγκεντρωτικά δεδομένα που παράγονται από τα υφιστάμενα συστήματα DLP.

Αν και αυτή η μέθοδος μηχανικής εκμάθησης μπόρεσε να εντοπίσει διαρροές δεδομένων σε αρκετά μεγάλο βαθμό, περιορίζεται μόνο σε ένα μικρό αριθμό παραληπτών και απαιτεί τεράστιο αριθμό υπολογισμών, κάνοντας τη μέθοδο αυτή να έχει περιορισμούς επεκτασιμότητας.

Η ομαδοποίηση κειμένου και ο τομέας επεξεργασίας φυσικών γλωσσών χρησιμοποιούνται επίσης σε DLPS. Με αυτές τις μεθόδους, τη χρήση τεχνητής νοημοσύνης και στατιστικής ανάλυσης, εισήχθη ένα πρωτότυπο σύστημα για να αποτραπεί η διαρροή δεδομένων σε κοινωνικά δίκτυα όπως Facebook, Twitter, email και διαδραστικές ιστοσελίδες. Αυτές οι μέθοδοι πέτυχαν πολύ υψηλό επίπεδο απόδοσης στην ταξινόμηση τόσο της αγγλικής όσο και της ισπανικής γλώσσας. Ωστόσο, υπήρξε περιορισμός κατά την εξαγωγή λέξεων από έγγραφα, καθώς μπορούσαν να επηρεαστούν από ορθογραφικά λάθη, συνδεδεμένες λέξεις και συντομογραφίες.

Πίνακας 5.7: *Αδυναμίες και Πλεονεκτήματα κατηγορίας (Εξόρυξη δεδομένων και Ομαδοποίηση κειμένων).*

Πλεονεκτήματα	***Αδυναμίες***
• Ευέλικτο και προσαρμόσιμο.	• Απαιτεί μεγάλη επεξεργασία.
• Ισχυρό στην ανίχνευση μη δομημένων δεδομένων.	• Απαιτεί φάση εκμάθησης, που σημαίνει πολλούς ψευδώς θετικούς συναγερμούς.

• Λιγότερο εξαρτημένο από επεμβάσεις διαχειριστών.	
• Μπορεί να προβλέψει μελλοντικές διαρροές δεδομένων.	

5.5.2. Εμπορικές λύσεις DLPS.

Οι λύσεις ανίχνευσης εντοπισμού και πρόληψης διαρροών δεδομένων προσφέρονται από ένα ευρύ φάσμα προμηθευτών.

Υπάρχουν δεκάδες λύσεις DLPS διαθέσιμες ως δυνατότητες που μπορούν να προστεθούν σε υπάρχοντα συστήματα ασφαλείας ή ως αυτόνομα συστήματα. Διάφοροι προμηθευτές ασφαλείας, αναπτύσσουν συνεχώς νέα DLPS με ειδικές δυνατότητες για την αντιμετώπιση νέων τύπων απειλών διαρροής δεδομένων. Websense, Symantec, Trend Micro, McAfee, είναι μερικά μόνο από τη μεγάλη λίστα προμηθευτών που παρέχουν λύσεις DLP. Οι περισσότερες από αυτές τις λύσεις έχουν σχεδιαστεί για τον εντοπισμό και την πρόληψη της διαρροής δεδομένων σε διαφορετικές καταστάσεις, χρησιμοποιώντας κυρίως ανάλυση περιεχόμενου και ανάλυση περιβάλλοντος. Οι μόνες σαφείς διαφορές μεταξύ τους είναι οι ***τεχνικές ανάλυσης*** που χρησιμοποιούνται, ***οι ενέργειες αποκατάστασης*** και τα ***ειδικά χαρακτηριστικά*** που προσφέρονται από κάθε προϊόν.

Επομένως, η κατηγοριοποίηση αυτών των λύσεων σε ομάδες μπορεί να μην είναι επαρκής. Για να επισημανθούν μερικές από τις κορυφαίες εμπορικές δυνατότητες DLPS, επιλέχθηκαν έξι κορυφαία DLPS σύμφωνα με την αποδοχή τους στην αγορά. Αυτά τα DLPS παρατίθενται και συγκρίνονται στους αντίστοιχους πίνακες που ακολουθούν με τα χαρακτηριστικά τους.

Όπως αναφέρθηκε προηγουμένως, ένα από τα ξεχωριστά σημεία μεταξύ όλων των DLP είναι τα ***ειδικά χαρακτηριστικά*** που προσφέρονται [27] [33].

- Η ***Triton***, για παράδειγμα, έχει τη δυνατότητα να ανιχνεύει ευαίσθητα δεδομένα σε εικόνες και κρυπτογραφημένα αρχεία. Επιπλέων, έχει τη δυνατότητα να ανιχνεύει μικρές διαρροές δεδομένων για μεγάλες χρονικές περιόδους χρησιμοποιώντας μια λειτουργία που ονομάζεται Drip DLP.

- Η ***Fidelis XPS*** προσφέρει ενσωματωμένη επιθεώρηση συνεδρίας σε πραγματικό χρόνο με χαμηλό αντίκτυπο στην απόδοση του συστήματος που εφαρμόζεται.
- Η ***McAfee*** παρέχει τη δυνατότητα εκτέλεσης μιας εγκληματολογικής ανάλυσης πριν από τη δημιουργία κανόνων DLP. Αυτό επιτρέπει στον διαχειριστή ασφαλείας να εντοπίσει υπάρχουσες, αλλά όχι μη ανιχνευμένες διαρροές δεδομένων.

Τα ακόλουθα DLPS προσφέρουν ειδικές λειτουργίες όπως:

- ***CheckPoint:*** επιθεώρηση SSL.
- ***Varonis:*** προηγμένη ανάλυση περιβάλλοντος και
- ***AirWatch:*** ανάπτυξη και προστασία για κινητές συσκευές.

Ένα από τα κοινά χαρακτηριστικά μεταξύ όλων των προαναφερόμενων DLPS είναι η δυνατότητα ενσωμάτωσής τους σε ήδη υπάρχοντα συστήματα ασφαλείας.

Ανάλογα με τις επιλογές που προσφέρονται από τις εταιρίες, μπορούν να εφαρμοστούν οι κατάλληλες ***ενέργειες αποκατάστασης*** όπως:
Ειδοποίηση, Μπλοκ, Κρυπτογράφηση, ***Έλεγχος*** και ***Καραντίνα***.
Το Triton και το McAfee είναι τα μόνα DLPS που προσφέρουν όλες τις προαναφερθείσες ενέργειες διόρθωσης.
Όλα τα DLPS είναι συνδυασμός λύσεων ανίχνευσης και πρόληψης διαρροής δεδομένων, εκτός από το AirWatch και το Varonis που χρησιμοποιούν μόνο τεχνικές πρόληψης και τεχνικές ανίχνευσης αντίστοιχα.
Εκτός από το AirWatch που εκτελεί μόνο ανάλυση περιβάλλοντος, τα υπόλοιπα DLPS έχουν τη δυνατότητα να εκτελούν ανάλυση περιεχομένου αλλά και περιβάλλοντος.

Πέντε από τα αναφερόμενα DLPS έχουν τη δυνατότητα να εκτελούν τουλάχιστον δύο από τις τρεις τεχνικές ανάλυσης περιεχομένου: ***Κανονικές εκφράσεις***, ***Αποτυπώματα δεδομένων*** και ***Στατιστική ανάλυση***.
Επιπλέον, όλα είναι λύσεις λογισμικού, εκτός από το Fidelis και το McAfee, τα οποία είναι διαθέσιμα ως αυτόνομες συσκευές.

Συνοπτικά πιο κάτω έχουν αποτυπωθεί τα κύρια χαρακτηριστικά των συγκεκριμένων DLP σε μορφή πινάκων [27] [33]:

Πίνακας 5.8: *Χαρακτηριστικά DLP (TRITON).*

				
ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ				
Περιεχόμενο		Πλαίσιο		
ΝΑΙ		ΝΑΙ		
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ				
Κανονικές εκφράσεις		Αποτυπώματα δεδομένων		Στατιστική ανάλυση
ΝΑΙ		ΝΑΙ		
ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ				
Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Ελέγχος	Καραντίνα
ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
ΜΕΘΟΔΟΣ				
ΑΝΥΧΝΕΥΣΗ		ΠΡΟΛΗΨΗ		
ΝΑΙ		ΝΑΙ		
ΑΝΑΠΤΥΞΗ				
Δεδομένα σε χρήση (DIU)		Δεδομένα σε κίνηση (DIM)		Δεδομ.σε ηρεμία (DAR)
ΝΑΙ		ΝΑΙ		ΝΑΙ
ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ				
Δυνατότητα ανιχνεύσης ευαίσθητων δεδομένων σε εικόνες και κρυπτογραφημένα αρχεία + Λειτουργία DLP Drip.				
ΔΙΑΘΕΣΙΜΟ ΣΕ:	**Λογισμικό**			

Πίνακας 5.9: *Χαρακτηριστικά DLP (VARONIS).*

VARONIS				
ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ				
Περιεχόμενο		Πλαίσιο		
ΝΑΙ		ΝΑΙ		
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ				
Κανονικές εκφράσεις		Αποτυπώματα δεδομένων		Στατιστική ανάλυση
ΝΑΙ		ΝΑΙ		
ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ				
Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Ελέγχος	Καραντίνα
ΝΑΙ			ΝΑΙ	
ΜΕΘΟΔΟΣ				
ΑΝΥΧΝΕΥΣΗ		ΠΡΟΛΗΨΗ		
ΝΑΙ				
ΑΝΑΠΤΥΞΗ				
Δεδομένα σε χρήση (DIU)		Δεδομένα σε κίνηση (DIM)		Δεδομ.σε ηρεμία (DAR)
ΝΑΙ		ΝΑΙ		ΝΑΙ
ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ				
Προηγμένη ανάλυση περιβάλλοντος με βάση τα συμφραζόμενα.				
ΔΙΑΘΕΣΙΜΟ ΣΕ:	**Λογισμικό**			

Πίνακας 5.10: *Χαρακτηριστικά DLP (McAfee).*

McAfee DLP Endpoint				
ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ				
Περιεχόμενο	Πλαίσιο			
ΝΑΙ	ΝΑΙ			
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ				
Κανονικές εκφράσεις	Αποτυπώματα δεδομένων	Στατιστική ανάλυση		
ΝΑΙ	ΝΑΙ	ΝΑΙ		
ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ				
Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Ελέγχος	Καραντίνα
ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
ΜΕΘΟΔΟΣ				
ΑΝΥΧΝΕΥΣΗ	ΠΡΟΛΗΨΗ			
ΝΑΙ	ΝΑΙ			
ΑΝΑΠΤΥΞΗ				
Δεδομένα σε χρήση (DIU)	Δεδομένα σε κίνηση (DIM)	Δεδομ.σε ηρεμία (DAR)		
ΝΑΙ	ΝΑΙ	ΝΑΙ		
ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ				
Εγκληματολογική ανάλυση πριν από τη δημιουργία κανόνων DLP.				
ΔΙΑΘΕΣΙΜΟ ΣΕ:	**Συσκευή**			

Πίνακας 5.11: *Χαρακτηριστικά DLP (FIDELIS).*

Fidelis Cybersecurity				
ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ				
Περιεχόμενο		Πλαίσιο		
ΝΑΙ		ΝΑΙ		
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ				
Κανονικές εκφράσεις		Αποτυπώματα δεδομένων		Στατιστική ανάλυση
				ΝΑΙ
ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ				
Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Ελέγχος	Καραντίνα
ΝΑΙ	ΝΑΙ		ΝΑΙ	ΝΑΙ
ΜΕΘΟΔΟΣ				
ΑΝΥΧΝΕΥΣΗ		ΠΡΟΛΗΨΗ		
ΝΑΙ		ΝΑΙ		
ΑΝΑΠΤΥΞΗ				
Δεδομένα σε χρήση (DIU)		Δεδομένα σε κίνηση (DIM)		Δεδομ.σε ηρεμία (DAR)
		ΝΑΙ		
ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ				
Ενσωματωμένη επιθεώρηση συνεδρίας σε πραγματικό χρόνο.				
ΔΙΑΘΕΣΙΜΟ ΣΕ:	**Συσκευή**			

Πίνακας 5.12: *Χαρακτηριστικά DLP (AIRWATCH).*

				
ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ				
Περιεχόμενο			Πλαίσιο	
			ΝΑΙ	
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ				
Κανονικές εκφράσεις		Αποτυπώματα δεδομένων		Στατιστική ανάλυση
		ΝΑΙ		
ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ				
Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Ελέγχος	Καραντίνα
	ΝΑΙ	ΝΑΙ	ΝΑΙ	
ΜΕΘΟΔΟΣ				
ΑΝΥΧΝΕΥΣΗ			ΠΡΟΛΗΨΗ	
			ΝΑΙ	
ΑΝΑΠΤΥΞΗ				
Δεδομένα σε χρήση (DIU)		Δεδομένα σε κίνηση (DIM)		Δεδομ.σε ηρεμία (DAR)
ΝΑΙ		ΝΑΙ		ΝΑΙ
ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ				
Ανάπτυξη σε κινητές συσκευές.				
ΔΙΑΘΕΣΙΜΟ ΣΕ:		**Λογισμικό**		

Πίνακας 5.13: *Χαρακτηριστικά DLP (Check Point).*

Check Point SOFTWARE TECHNOLOGIES LTD.				
ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ				
Περιεχόμενο		Πλαίσιο		
ΝΑΙ		ΝΑΙ		
ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ				
Κανονικές εκφράσεις		Αποτυπώματα δεδομένων		Στατιστική ανάλυση
ΝΑΙ		ΝΑΙ		
ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ				
Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Ελέγχος	Καραντίνα
ΝΑΙ	ΝΑΙ		ΝΑΙ	ΝΑΙ
ΜΕΘΟΔΟΣ				
ΑΝΥΧΝΕΥΣΗ		ΠΡΟΛΗΨΗ		
ΝΑΙ		ΝΑΙ		
ΑΝΑΠΤΥΞΗ				
Δεδομένα σε χρήση (DIU)		Δεδομένα σε κίνηση (DIM)		Δεδομ.σε ηρεμία (DAR)
		ΝΑΙ		
ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ				
Δυνατότητες επιθεώρησης SSL.				
ΔΙΑΘΕΣΙΜΟ ΣΕ:		**Λογισμικό**		

Στους πιο κάτω πίνακες έχουν αποτυπωθεί συγκεντρωτικά τα κύρια χαρακτηριστικά των συγκεκριμένων DLP.

Πίνακας 5.14: *Συγκεντρωτικός Πίνακας με Χαρακτηριστικά των DLP* [22] [27] [33].

	ΜΕΘΟΔΟΣ		ΑΝΑΠΤΥΞΗ			ΤΥΠΟΣ ΑΝΑΛΥΣΗΣ		ΤΕΧΝΙΚΕΣ ΑΝΑΛΥΣΗΣ ΠΕΡΙΕΧΟΜΕΝΟΥ		
	ΑΝΥΧΝΕΥΣΗ	ΠΡΟΛΗΨΗ	In use	In transit	At rest	Περιεχόμενο	Πλαίσιο	Κανονικές εκφράσεις	Αποτυπώματα δεδομένων	Στατιστική ανάλυση
websense TRITON	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	
Fidelis Cybersecurity	ΝΑΙ	ΝΑΙ		ΝΑΙ		ΝΑΙ	ΝΑΙ			ΝΑΙ
McAfee DLP Endpoint	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ
VARONIS	ΝΑΙ		ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	
airwatch		ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ		ΝΑΙ		ΝΑΙ	
Check Point SOFTWARE TECHNOLOGIES LTD.	ΝΑΙ	ΝΑΙ		ΝΑΙ		ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	

Πίνακας 5.15: *Συγκεντρωτικός Πίνακας με Χαρακτηριστικά των DLP* [22] [27] [33].

	ΕΝΕΡΓΕΙΕΣ ΑΠΟΚΑΤΑΣΤΑΣΗΣ					ΔΙΑΘΕΣΙΜΟ ΣΕ		ΕΙΔΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ
	Ειδοποίηση	Μπλοκ	Κρυπτογράφηση	Έλεγχος	Καραντίνα	Λογισμικό	Συσκευή	
websense TRITON	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ		Δυνατότητα ανιχνεύσης ευαίσθητων δεδομένων σε εικόνες και κρυπτογραφημένα αρχεία + Λειτουργία DLP Drip.
Fidelis Cybersecurity	ΝΑΙ	ΝΑΙ		ΝΑΙ	ΝΑΙ		ΝΑΙ	Ενσωματωμένη επιθεώρηση συνεδρίας σε πραγματικό χρόνο.
McAfee DLP Endpoint	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ	ΝΑΙ		ΝΑΙ	Εγκληματολογική ανάλυση πριν από τη δημιουργία κανόνων DLP.
VARONIS	ΝΑΙ			ΝΑΙ		ΝΑΙ		Προηγμένη ανάλυση περιβάλλοντος με βάση τα συμφραζόμενα.
airwatch		ΝΑΙ	ΝΑΙ	ΝΑΙ		ΝΑΙ		Ανάπτυξη σε κινητές συσκευές.
Check Point SOFTWARE TECHNOLOGIES LTD.	ΝΑΙ	ΝΑΙ		ΝΑΙ	ΝΑΙ	ΝΑΙ		Δυνατότητες επιθεώρησης SSL.

6. Κριτική και Συμπεράσματα.

Η διαρροή δεδομένων και κυρίως η προστασία τους, είναι ένα από τα μεγαλύτερα, αν όχι το μεγαλύτερο πρόβλημα στον τομέα της ασφάλειας πληροφοριών. Ένας οργανισμός θα πρέπει να είναι σε θέση να διασφαλίσει τα δεδομένα του από:

α) Υποκλοπή, ***β)*** τη ***Διαρροή τους προς τρίτους*.**

Μέχρι τώρα, οι συμβατικοί μηχανισμοί ασφαλείας είναι προσανατολισμένοι είτε προς τη μια είτε προς την άλλη κατεύθυνση, προσφέροντας έτσι ελλιπή προστασία. Η δυνατότητα *υποκλοπής* πληροφοριών από εσωτερική ή εξωτερική οντότητα, δεν παύει να αποτελεί *διαρροή δεδομένων.* Ουσιαστικά οι δύο αυτές περιπτώσεις ταυτίζονται και ο ρόλος των νέων μηχανισμών ασφαλείας DLP θα πρέπει να είναι διττός, για να μπορούν να παρέχουν ολοκληρωμένη προστασία. Τόσο οι ακαδημαϊκοί, όσο και οι επαγγελματίες του χώρου, εργάζονται για την ανάπτυξη κοινών μεθόδων πρόληψης και ανίχνευσης *διαρροής / υποκλοπής* δεδομένων προς τρίτους, αντιμετωπίζοντάς τα με κοινούς μηχανισμούς και στις δύο περιπτώσεις. Κάθε νέα πρόκληση λοιπόν που καλούνται να αντιμετωπίσουν οι νέοι μηχανισμοί DLPS, αντιστοιχεί και σε μία αδυναμία παροχής προστασίας των συμβατικών μέσων ασφαλείας (IDS, VPN, κ.τ.λ.) που πρέπει να ξεπεραστεί.

Για να μπορούν τα DLPS να παρέχουν ολοκληρωμένη προστασία, πρέπει να εφαρμόζουν μεθόδους ανίχνευσης ή πρόληψης ή συνδυασμό αυτών ανάλογα την περίπτωση. Υπάρχουν πολλά περιστατικά δυστυχώς που ανακαλύφθηκαν τυχαία, αυτό σημαίνει πως με κάποιο τρόπο ξεπεράστηκαν οι μηχανισμοί ανίχνευσης, ενώ πιθανόν υπάρχουν περιστατικά που δεν έχουν ακόμη αποκαλυφθεί ή ακόμα χειρότερα δεν θα μάθουμε ποτέ ότι έγιναν. Ένα πρόσφατο παράδειγμα καθυστερημένης αποκάλυψης και μιας από τις πιο μεγάλες επιβεβαιωμένες διαρροές προσωπικών δεδομένων παγκοσμίως, είναι αυτή του Facebook, που έγινε γνωστή στις αρχές Απριλίου του 2021. Η διαρροή αφορούσε προσωπικά δεδομένα, περισσότερων από 500 εκατ. χρηστών της δημοφιλούς πλατφόρμας από 106 χώρες, συμπεριλαμβανομένης και της Ελλάδας, με στοιχεία από 617.722 λογαριασμούς. Πρόκειται για μία από τις

σοβαρότερες μέχρι στιγμής διαρροές δεδομένων προσωπικού χαρακτήρα, τα οποία πιθανότατα θα τύχουν εμπορικής ή άλλης αξιοποίησης. Εκπρόσωπος της Facebook ανέφερε ότι «τα συγκεκριμένα δεδομένα είναι πολύ παλιά και σχετίζονται με συμβάν που επιδιορθώθηκε τον Αύγουστο του 2019».

Είναι σημαντικό για κάθε οργανισμό να έχει ισχυρούς μηχανισμούς ανίχνευσης έτσι ώστε να μπορούν να προλάβουν μια ενδεχόμενη διαρροή σε αρχικό στάδιο, ιδανικά σε πραγματικό χρόνο, για να ελαχιστοποιηθούν οι συνέπειες που πιθανώς προκύψουν.

Εξίσου σημαντικός, είναι και ο ρόλος των μηχανισμών πρόληψης σε έναν οργανισμό, όπου θα μπορούν να διασφαλίσουν στο μέγιστο την προστασία των δεδομένων από διαρροή, πριν αυτή γίνει. Αν με κάποιο τρόπο διαρρεύσουν στοιχεία προς τρίτους, αυτό είναι κάτι που δεν μπορεί να διορθωθεί εκ των υστέρων και η ζημιά που πιθανόν προκύψει είναι ανεπανόρθωτη. Σε αντίθεση για παράδειγμα, με μια απώλεια από διαγραφή δεδομένων, που μπορεί σχετικά εύκολα να αποκατασταθεί. Πρέπει να κατανοηθεί ότι τα δεδομένα συμπεριλαμβάνονται στα περιουσιακά στοιχεία ενός οργανισμού και κατ' επέκταση χρήζουν της αντίστοιχης προστασίας και ιδιαίτερης προσοχής. Πέρα από την οικονομική απώλεια που μπορεί να προκληθεί, δημιουργείται πρόβλημα και στην ομαλή λειτουργία του, με πολλές αρνητικές επιπτώσεις.

Τα DLPS επικεντρώνονται επίσης σε δύο βασικές τεχνικές, την ***ανάλυση περιβάλλοντος*** και την ***ανάλυση περιεχομένου***. Οι προσεγγίσεις των εμπορικών προμηθευτών και των ερευνητών έχουν επικεντρωθεί στην ανάπτυξη τεχνικών ανάλυσης περιεχομένου, ελέγχοντας τη σημασιολογία των δεδομένων για την παραγωγή ισχυρών μηχανισμών DLPS, ενώ από ορισμένους υπάρχει η άποψη ότι η ανάλυση περιβάλλοντος είναι το μέλλον ενός αποτελεσματικού DLP. Αυτό συμβαίνει, επειδή οι τεχνικές ανάλυσης περιεχομένου είναι πολύπλοκες, αρκετά δύσχρηστες και συνήθως απαιτούν μεγάλη επεξεργαστική ισχύ. Επομένως, σύμφωνα με αυτή την εκδοχή, έχοντας μια ισχυρή ανάλυση με βάση το περιβάλλον και τα συμφραζόμενα, τα συστήματα ελέγχου μπορούν να παρέχουν την προστασία που απαιτείται για τα δεδομένα.

Ως εκ τούτου, ένα αποτελεσματικό DLP, όποια μέθοδο ανάλυσης κι αν χρησιμοποιεί, θα πρέπει να μπορεί να εκτελεί τις εργασίες εντοπισμού, με ελάχιστες απαιτήσεις σε υπολογιστική ισχύ και αποθηκευτικό χώρο.

Ένας άλλος τομέας ανάπτυξης DLPS, καθώς και μια από τις κύριες ανησυχίες, αλλά και μεγάλη πρόκληση για τους ερευνητές, είναι η εσωτερική κατάχρηση. Τα νέα DLPS πρέπει να εστιάζουν στο πεδίο της εσωτερικής ανίχνευσης της κακόβουλης χρήσης. Τα άτομα με προνόμια θεωρούνται ίσως η πιο μεγάλη απειλή για πιθανή κακόβουλη χρήση εμπιστευτικών δεδομένων. Όχι μόνο ξέρουν τι δεδομένα πρέπει να στοχεύσουν και πού φυλάσσονται, αλλά γνωρίζουν επίσης και την αξία τους. Μια τέτοια πρόκληση λόγο της ιδιαιτερότητάς της και της δυσκολίας της, μπορεί να αντιμετωπιστεί συνδυάζοντας τις δυνατότητες ανάλυσης περιεχομένου και της ανάλυσης περιβάλλοντος μαζί με άλλα μέτρα ασφάλειας, εξετάζοντας επίσης και την ανθρώπινη συμπεριφορά. Επομένως, θα πρέπει τα DLPS να μπορούν να στοχεύουν προνομιακούς και κακόβουλους χρήστες “insiders”, να είναι ικανά να ενσωματώσουν δυνατότητες άλλων τεχνικών και μηχανισμών ασφαλείας και να μπορούν να προστατεύουν τα δεδομένα ενός οργανισμού σε όποια κατάσταση κι αν βρίσκονται, σε κίνηση (DIM), ηρεμία (DAR), και χρήση (DIU).

Επιπρόσθετα, είναι επιβεβλημένη η ανάγκη για την εφαρμογή και λειτουργία συστημάτων προστασίας, που εστιάζουν στις διαδικασίες διαχείρισης των δεδομένων. Σημαντικός παράγοντας γι’ αυτό, είναι η ευαισθητοποίηση της διοίκησης ενός οργανισμού και στην συνέχεια του αντίστοιχου προσωπικού το οποίο χειρίζεται δεδομένα, ώστε να διασφαλιστεί ότι έχουν κατανοηθεί οι κίνδυνοι που μπορούν να προκαλέσουν τυχαία διαρροή δεδομένων. Σε αντίθετη περίπτωση τα συστήματα θα παραμένουν απλώς εργαλεία αντιμετώπισης, αφού έχει συμβεί κάποιο συμβάν απώλειας.

Σε αυτό το σημείο αξίζει να αναφερθεί, ότι κάποιες αναφορές ερευνητών συγκλίνουν στο ότι ένας μεγάλος αριθμός περιστατικών δεν γίνονται κακόβουλα ή σκόπιμα, αλλά οφείλονται σε αμέλεια ή ακόμη και σε αφέλεια κάποιων υπαλλήλων. Έχουν καταγραφεί περιπτώσεις, όπου υπάλληλοι έχουν στείλει έγγραφα και δεδομένα εκτός οργανισμού, απλά για να τα ελέγξει κάποιος ειδικός ή φίλος τους με μεγαλύτερη εμπειρία από αυτούς ή ακόμη χειρότερα

απλά για να τους πει κάποιος τρίτος τη γνώμη του για τη δουλειά τους. Όλο αυτό γίνεται, χωρίς ο υπάλληλος να καταλαβαίνει σε τι μεγάλο κίνδυνο θέτει την εταιρία και τα δεδομένα της, με απρόβλεπτες και πιθανώς καταστροφικές συνέπειες. Σε αυτές τις περιπτώσεις οι περισσότεροι μηχανισμοί ασφαλείας κρίνονται ανεπαρκείς, χωρίς ουσιαστικά αποτελέσματα, ενώ αντίστοιχα οι χρήστες χρειάζονται ένα κανονιστικό πλαίσιο βάση του οποίου πρέπει να λειτουργούν και να κατευθύνονται. Είναι πολύ σημαντικό ένας οργανισμός να έχει στρατηγικές πρόληψης απώλειας δεδομένων, που να μπορούν να ανταπεξέλθουν σε αυτές τις περιπτώσεις όπου χρειάζεται συνδυασμός και συνεργασία του ανθρώπινου παράγοντα με τους αντίστοιχους μηχανισμούς ασφαλείας και όχι μόνο απόκτηση εξελιγμένων και σύγχρονων συστημάτων, που από μόνα τους ίσως παρέχουν μικρή προστασία έναντι απώλειας δεδομένων.

Στα προηγούμενα κεφάλαια αναφέρθηκαν κάποια εμπορικά DLPS και σχετικές ακαδημαϊκές μελέτες, όπου και κατηγοριοποιήθηκαν ανάλογα με τις μεθόδους που χρησιμοποιούν, καθώς αναφέρθηκαν και κάποιοι από τους περιορισμούς τους. Παρόλα αυτά, αν και οι εφαρμογές και τα εργαλεία DLPS είναι σχετικά νέα στον χώρο, μπορούν να παρέχουν υψηλής ποιότητας προστασία σε όσους οργανισμούς έχουν αναλύσει σωστά και λεπτομερώς τις ανάγκες τους, ώστε να μπορούν να εκμεταλλευτούν τις πλήρεις δυνατότητες μιας επιτυχημένης εφαρμογής ενός μηχανισμού DLPS. Πριν ξεκινήσει η εφαρμογή των μηχανισμών DLPS, απαιτείται να γίνει προσεκτικός και λεπτομερής σχεδιασμός, δημιουργία ομάδων εργασίας, καθώς επίσης σωστή και καταρτισμένη εκπαίδευση στα εμπλεκόμενα τμήματα του οργανισμού. Ακόμα, θα πρέπει να δοθεί μεγάλη προσοχή στην αντίστοιχη δημιουργία πολιτικών και στην εφαρμογή των μεθόδων προστασίας, ώστε να μπορέσει να διασφαλιστεί στο μέγιστο βαθμό η διαρροή των δεδομένων του οργανισμού που χρήζουν ιδιαίτερη προστασία.

Τα DLPS αναγνωρίζονται όλο και περισσότερο κερδίζοντας έδαφος έναντι των συμβατικών λύσεων, που κρίνονται ανεπαρκείς για την αντιμετώπιση των σημερινών προκλήσεων. Επίσης, πρέπει να δοθεί ιδιαίτερη προσοχή και στην αντίστοιχη επιλογή των ατόμων που θα τα διαχειρίζονται.

6.1. Μελλοντικές τάσεις.

Ένα αποτελεσματικό μελλοντικό DLP θα πρέπει να έχει την ικανότητα ταξινόμησης εμπιστευτικών δεδομένων σημασιολογικά, ακόμη κι όταν αυτά εξελίσσονται γρήγορα και σε μεγάλο βαθμό. Αν και ορισμένοι ερευνητές επιμένουν να βασίζονται στην ανάλυση περιβάλλοντος, είναι δύσκολο να προστατευθεί η σημασιολογία χωρίς να γνωρίζουμε το περιεχόμενο.

Ένα πιθανό ερευνητικό ερώτημα σε αυτόν τον τομέα ίσως είναι, πώς να εντοπιστεί σημασιολογικά το περιεχόμενο των εμπιστευτικών δεδομένων σε τέτοιο βαθμό ώστε να γίνεται αντιληπτή κάθε κίνηση που μπορεί να είναι ύποπτη. Ενδεχομένως μελλοντικά, με εφαρμογή τεχνητής νοημοσύνης, να εκπαιδεύονται κατάλληλα τα DLPS και να μην είναι στατικά, όπως τα σημερινά αλλά να προσαρμόζονται κατάλληλα σε κάθε περίπτωση για την βέλτιστη αποτροπή διαρροής δεδομένων.

Ένας άλλος τομέας όπου οι εφαρμογές DLPS επιβάλλεται να δώσουν ιδιαίτερη προσοχή αλλά και οι ερευνητές πρέπει να μελετήσουν εκτεταμένα και να αναπτύξουν μηχανισμούς ασφαλείας, είναι ο χώρος των έξυπνων τηλεφώνων (smart-phones). Όλο και περισσότερες δυνατότητες προστίθενται σε κινητά τηλέφωνα, γεγονός που τους επιτρέπει να χειρίζονται μεγάλο όγκο δεδομένων. Αυτό μπορεί να θέσει σε κίνδυνο την ασφάλεια εταιρικών ευαίσθητων δεδομένων, τα οποία είναι ευάλωτα σε κλοπή και απώλεια. Έτσι ένας νέος χώρος πρέπει να αναπτυχθεί και να δοθούν νέες λύσεις DLPS από ερευνητές και κατασκευαστές κινητών συσκευών. Η διαχείριση των περιεχομένων κινητής τηλεφωνίας πρέπει να ανασχεδιαστεί για την προστασία των δεδομένων στα οποία έχουν πρόσβαση τα τηλέφωνα και τα tablet οποιαδήποτε στιγμή και οπουδήποτε. Αυτό επιβάλλεται να γίνει, ίσως με τη δημιουργία ασφαλέστερων κρυπτογραφημένων συνδέσεων, ώστε να επιτρέπεται στους χρήστες να έχουν πρόσβαση, να αποθηκεύουν και να ενημερώνουν δεδομένα με ασφάλεια από κινητές συσκευές με περιορισμό μη εξουσιοδοτημένης κοινής χρήσης δεδομένων. Μια μεγάλη δυσκολία όλου αυτού, είναι ότι εκτός από ανάπτυξη αντίστοιχων μηχανισμών DLP για κινητές συσκευές, θα πρέπει να υπάρξει συνεργασία με εταιρίες κινητής τηλεφωνίας

και παρόχους δικτύων, ώστε να μπορέσουν από κοινού να εφαρμοστούν ασφαλείς συνδέσεις και νέα πρωτόκολλα για την αποτροπή διαρροής δεδομένων μέσω κινητών συσκευών και ασύρματων δικτύων.

Επίσης κάτι που ισχύει τώρα αλλά και στο μέλλον, είναι η συνεχόμενη προσπάθεια ευαισθητοποίησης του προσωπικού, η καθοδήγησή του και η συνεχόμενη εκπαίδευση μέσα από σεμινάρια, παρουσιάσεις και συνεχώς επικαιροποιημένες οδηγίες ανάλογα με τις εξελίξεις και τις απαιτήσεις κάθε περίστασης. Η διοίκηση και τα στελέχη ενός οργανισμού έχοντας κατανοήσει την αναγκαιότητα της σωστής δομής, σχεδίασης, λειτουργικής διακίνησης και αποθήκευσης δεδομένων, θωρακίζουν κατ' αυτό τον τρόπο τη σωστή λειτουργία και την ασφάλεια, μειώνοντας σημαντικά τον κίνδυνο απώλειας δεδομένων.

Από τις εμπορικές αναφορές και τη βιβλιογραφία, είναι προφανές ότι οι μέθοδοι ανίχνευσης και πρόληψης διαρροών δεδομένων όσο κι αν έχουν μελετηθεί, είναι ένας συνεχώς εξελισσόμενος χώρος όπου προκύπτουν όλο και περισσότερες προκλήσεις. Χρειάζεται να εφαρμοστούν νέες τεχνολογίες και εξελιγμένοι μηχανισμοί, αφού οι περισσότερες από τις τρέχουσες μεθόδους πάσχουν από σημαντικούς περιορισμούς, όταν τα εμπιστευτικά δεδομένα εξελίσσονται, αλλάζουν μορφή και τα διαχειρίζονται αναρμόδιοι και μη σωστά ενημερωμένοι χρήστες.

Η επιστήμη των υπολογιστών εξελίσσεται ραγδαία και κανείς δεν μπορεί να προβλέψει τι επιφυλάσσει το μέλλον. Ο τομέας της ασφάλειας δυστυχώς, δίνει καθημερινά μάχες για την προστασία των δεδομένων και πληροφοριών και ο ιστορικός του μέλλοντος θα κληθεί να καταγράψει, ποιος τελικά θα βγει νικητής.

ΒΙΒΛΙΟΓΡΑΦΙΑ.

[1] M. Hassan, C. Jincai, A. Iftekhar, A. Shehzad, and X. Cui, “Implementation of security systems for detection and prevention of data loss/leakage at organization via traffic inspection,” *arXiv*. 2020.

[2] G. Stalidis, D. Kardaras, Γ. Σταλίδης, and Δ. Καρδαράς, “Data Management and Business Intelligence,” Jan. 2016, [Online]. Available: https://repository.kallipos.gr/handle/11419/1161.

[3] The International Organization for Standardization, “ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls,” *ISO.org [Online]*, vol. 2013, p. 80, 2013, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en.

[4] Σ. Κάτσικας, “ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ,” 2000.

[5] Σ. Κάτσικας and Δ. Γκρίτζαλης, *Ασφάλεια πληροφοριακών συστημάτων*. Εκδόσεις Νέων Τεχνολογιών, 2004.

[6] I. Kantzavelou and S. Katsikas, “A game-based intrusion detection mechanism to confront internal attackers,” *Comput. Secur.*, vol. 29, no. 8, pp. 859–874, Nov. 2010, doi: 10.1016/j.cose.2010.06.002.

[7] N. R. Mead, “Computer security: Art and science [Book Review],” *IEEE Secur. Priv.*, vol. 1, no. 3, pp. 14–14, 2003, doi: 10.1109/msecp.2003.1203217.

[8] S. J. Stolfo, S. M. Bellovin, S. Hershkop, A. D. Keromytis, S. Sinclair, and S. W. Smith, “Advances in information security: Insider attack and cyber security - Beyond the hacker.” p. 228, 2008.

[9] G. Silowash, T. J. Shimeall, D. Cappelli, A. Moore, L. Flynn, and R. Trzeciak, “Common Sense Guide to Mitigating Threats,” 2018.

[10] F. L. Greitzer and R. E. Hohimer, “Modeling Human Behavior to Anticipate Insider Attacks,” *J. Strateg. Secur.*, vol. 4, no. 2, pp. 25–48, Jun. 2011, doi: 10.5038/1944-0472.4.2.2.

[11] J. Hunker and C. W. Probst, “Insiders and insider threats an overview of

definitions and mitigation techniques," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 4–27, 2011.

[12] M. M. R. Randazzo, M. Keeney, E. Kowalski, D. M. Cappelli, and A. Moore, "Insider threat study: Illicit cyber activity in the banking and finance sector," *Finance*, vol. 38, no. August, pp. 3–14, 2005, [Online]. Available: http://www.sei.cmu.edulpublications/pubweb.htnml.

[13] C. P. Pfleeger, "Reflections on the Insider Threat," in *Insider Attack and Cyber Security*, vol. 39, Boston, MA: Springer US, 2008, pp. 5–16.

[14] A. P. Moore, D. M. Cappelli, and R. F. Trzeciak, "The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures," in *Insider Attack and Cyber Security*, vol. 39, Boston, MA: Springer US, 2008, pp. 17–52.

[15] E. Sugawara and H. Nikaido, "Properties of AdeABC and AdeIJK efflux systems of Acinetobacter baumannii compared with those of the AcrAB-TolC system of Escherichia coli.," *Antimicrob. Agents Chemother.*, vol. 58, no. 12, pp. 7250–7, Dec. 2014, doi: 10.1128/AAC.03728-14.

[16] C. Y. Ho, Y. C. Lai, I. W. Chen, F. Y. Wang, and W. H. Tai, "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 146–154, Mar. 2012, doi: 10.1109/MCOM.2012.6163595.

[17] I. Kantzavelou and S. K. Katsikas, "An attack detection system for secure computer systems — Outline of the solution," in *Information Security in Research and Business*, Boston, MA: Springer US, 1997, pp. 123–135.

[18] I. Kantzavelou, "Intrusion Detection in Information Technology Security," University of the Aegean, Samos, Greece, 2011.

[19] A. Shabtai, Y. Elovici, and L. Rokach, "A survey of data leakage detection and prevention solutions," in *SpringerBriefs in Computer Science*, no. 9781461420521, Boston, MA: Springer US, 2012, pp. 1–92.

[20] Frost and Sullivan, "World Data Leakage Prevention Market, Technical Report ND34D-74," United States, 2008.

[21] R. Mogull, "Understanding and Selecting a Data Loss Prevention Solution," 2010. https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf.

[22] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on

data leakage prevention systems," *J. Netw. Comput. Appl.*, vol. 62, pp. 137–152, Feb. 2016, doi: 10.1016/j.jnca.2016.01.008.

[23] A. Kush, "A Learning oriented DLP System based on Classification Model," *INFOCOMP J. Comput. Sci.*, vol. 19, no. 2, pp. 98–108, Dec. 2020, [Online]. Available: http://infocomp.dcc.ufla.br/index.php/infocomp/article/view/1008.

[24] Sealpath, "The Three States of Data Guide - Description and How to Secure them," 2020. https://www.sealpath.com/blog/protecting-the-three-states-of-data/.

[25] B. Hauer, "Data and Information Leakage Prevention Within the Scope of Information Security," *IEEE Access*, vol. 3, pp. 2554–2565, 2015, doi: 10.1109/ACCESS.2015.2506185.

[26] "Tool for automatic enforcement of DLP policies in cloud applications."

[27] V. O. Waziri, I. Idris, J. K. Alhassan, and B. O. Adedayo, "Data loss prevention and challenges faced in their deployments," in *CEUR Workshop Proceedings*, 2019, vol. 1830, pp. 90–96.

[28] "Matlab Code for LSB Steganography -Image processing project." https://www.pantechsolutions.net/matlab-code-for-lsb-steganography/.

[29] I. M. Abbadi and M. Alawneh, "Preventing insider information leakage for enterprises," in *Proceedings - 2nd Int. Conf. Emerging Security Inf., Systems and Technologies, SECURWARE 2008, Includes DEPEND 2008: 1st Int. Workshop on Dependability and Security in Complex and Critical Inf. Sys.*, Aug. 2008, pp. 99–106, doi: 10.1109/SECURWARE.2008.14.

[30] M. Tsikerdekis, S. Zeadally, A. Schlesener, and N. Sklavos, "Approaches for Preventing Honeypot Detection and Compromise," Feb. 2019, doi: 10.1109/GIIS.2018.8635603.

[31] P. Papadimitriou and H. Garcia-Molina, "Data leakage detection," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 1, pp. 51–63, 2011, doi: 10.1109/TKDE.2010.100.

[32] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An insider threat prediction model," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture*

Notes in Bioinformatics), 2010, vol. 6264 LNCS, pp. 26–37, doi: 10.1007/978-3-642-15152-1_3.

[33] B. Hauer, “Data leakage prevention a position to state-of-The-art capabilities and remaining risk,” in *ICEIS 2014 - Proceedings of the 16th International Conference on Enterprise Information Systems*, 2014, vol. 2, pp. 361–367, doi: 10.5220/0004951703610367.