Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά και Επικοινωνιακά Συστήματα

Εργαλεία Αποτροπής Απώλειας Δεδομένων
(Data Loss Prevention Tools)

Μιχάλης Σάββα

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Μάιος 2014

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Εργαλεία Αποτροπής Απώλειας Δεδομένων (Data Loss Prevention Tools)

Μιχάλης Σάββα

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2014

Περίληψη

Στη σημερινή εποχή οι επιχειρήσεις επεξεργάζονται, μέσω των πληροφοριακών τους συστημάτων, μεγάλο εύρος ιδιαίτερα κρίσιμων προσωπικών δεδομένων. Η ανάγκη προστασίας αυτών καθίσταται επιτακτική, όχι μόνο για τη φήμη της εταιρείας αλλά και λόγω σχετικών νομικών επιταγών. Στο πλαίσιο αυτό, τα εργαλεία αποτροπής απώλειας δεδομένων αποτελούν μία ουσιαστική λύση, γιατί παρακολουθούν αυτοματοποιημένα την κάθε είδους δικτυακή κίνηση (εισερχόμενη ή/και εξερχόμενη) στην επιχείρηση και είναι σε θέση να αναγνωρίζουν περιπτώσεις όπου μπορούν να οδηγήσουν σε (εσκεμμένο ή ακούσιο) περιστατικό παραβίασης δεδομένων. Οι βασικές τεχνικές ανίχνευσης συμβάντων που χρησιμοποιούνται από τα ανωτέρω εργαλεία είναι ποικίλες και αποτελούν τρέχον αντικείμενο έρευνας. Εν τούτοις, πρέπει πάντα να συνυπολογίζεται το γεγονός ότι με τα εργαλεία αυτά ελλοχεύει ο κίνδυνος μη νόμιμης παρακολούθησης των εργαζομένων (αν, για παράδειγμα, ελέγχεται αυτοματοποιημένα το περιεχόμενο των εξερχόμενων ηλεκτρονικών μηνυμάτων). Ως εκ τούτου, ο αποτελεσματικός σχεδιασμός τέτοιων εργαλείων χρήζει ιδιαίτερης προσοχής και από την πλευρά της ιδιωτικότητας.

Αντικείμενο της παρούσας εργασίας είναι η καταγραφή των τεχνολογικών λύσεων, αλλά και των υποκείμενων αλγορίθμων, που υπάρχουν αναφορικά με το ζήτημα της αποτροπής απώλειας δεδομένων (Data Loss Prevention Tools). Περιγράφονται οι διάφορες κατηγορίες εργαλείων αποτροπής απώλειας δεδομένων ως προς τις σχεδιαστικές τους αρχές, ενώ επίσης γίνεται καταγραφή των υφιστάμενων τεχνολογικών λύσεων. Παράλληλα, η εργασία πραγματεύεται και ζήτημα της ιδιωτικότητας των υπαλλήλων, που εκ των πραγμάτων ανακύπτει με τη χρήση αυτών των εργαλείων. Απώτερος σκοπός είναι μία συγκριτική αποτίμηση των υπαρχουσών τεχνολογιών, λαμβάνοντας υπόψη τόσο την απόδοσή τους ως προς την προστασία από διαρροή ευαίσθητων πληροφοριών όσο και την «επέμβαση» στην ιδιωτικότητα, με βάση και το υπάρχον νομικό πλαίσιο περί προστασίας προσωπικών δεδομένων.

Summary

Business nowadays process huge amounts of critical personal data via ICT systems. As a direct consequence, there is a strong need for protecting these data; such a protection is prerequisite for company's reputation, whilst it also stems from relevant legal obligations. In this context, data loss prevention tools (DLPs) are an effective solution, since they automatically monitor any kind of network traffic (incoming and / or outgoing), being able to identify situations that may lead to (intentional or unintentional) personal data breach. There are many possible detection techniques that can be adopted by such tools, whereas improving such techniques is still an active research area. However, these tools, apart from their obvious advantages, may pose a risk from an employees' personal data protection point of view, since they often incorporate monitoring of communication initiated by employees (e.g. outgoing e-mails), which in turn threatens their privacy. Therefore, the effective design of such tools requires special attention with regard to privacy issues.

In this thesis, data loss prevention tools are studied, focusing on of the existing technological solutions, as well as on the underlying detection algorithms. .The different types of such tools , as well as their design principles, are described in detail.. Furthermore, this thesis also discusses the aforementioned issue of privacy that arises when such tools are being used, taking into account the legislation regarding personal data protection.. The ultimate goal is a comparative study of existing DLP technologies, considering both their effectiveness towards thwarting any possible personal data breach, as well as their "intervention" to privacy, on the basis of the existing legal framework on data protection.

Ευχαριστίες

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο του Μεταπτυχιακού Προγράμματος Σπουδών «Πληροφοριακά και Επικοινωνιακά Συστήματα» του Ανοικτού Πανεπιστήμιου Κύπρου.

Ιδιαίτερες ευχαριστίες αποδίδονται στον Επιβλέποντα καθηγητή Δρ. Λιμνιώτη Κωνσταντίνο για τη συνεργασία, την καθοδήγηση, τις συμβουλές και τη βοήθεια που μου παρείχε κατά τη διάρκεια εκπόνησης της μεταπτυχιακής διατριβής μου.

Επίσης θα ήθελα να ευχαριστήσω τη σύζυγο μου Παρασκευή, που με συνόδεψε με αγάπη, κατανόηση, υποστήριξη και υπομονή σε όλη τη διάρκεια αυτού του μεταπτυχιακού.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Στη σημερινή εποχή οι επιχειρήσεις επεξεργάζονται, μέσω των πληροφοριακών τους συστημάτων, μεγάλο εύρος ιδιαίτερα κρίσιμων προσωπικών δεδομένων. Η ανάγκη προστασίας αυτών των δεδομένων καθίσταται επιτακτική, όχι μόνο για τη φήμη της εταιρείας αλλά και λόγω σχετικών νομικών επιταγών. Στο πλαίσιο αυτό, τα εργαλεία αποτροπής απώλειας δεδομένων αποτελούν μία ουσιαστική λύση, γιατί αυτοματοποιημένα παρακολουθούν την κάθε είδους δικτυακή κίνηση (εισερχόμενη ή/και εξερχόμενη) στην επιχείρηση και είναι σε θέση να αναγνωρίζουν περιπτώσεις όπου μπορούν να οδηγήσουν σε (εσκεμμένο ή ακούσιο) περιστατικό παραβίασης δεδομένων. Οι βασικές τεχνικές ανίχνευσης συμβάντων που χρησιμοποιούνται από τα ανωτέρω εργαλεία είναι ποικίλες και αποτελούν τρέχον αντικείμενο έρευνας. Εν τούτοις, πρέπει πάντα να συνυπολογίζεται το γεγονός ότι από τα εργαλεία αυτά ελλοχεύει ο κίνδυνος μη νόμιμης παρακολούθησης των εργαζομένων (αν, για παράδειγμα, ελέγχεται αυτοματοποιημένα το περιεχόμενο των εξερχόμενων ηλεκτρονικών μηνυμάτων). Ως εκ τούτου, ο αποτελεσματικός σχεδιασμός τέτοιων εργαλείων χρήζει ιδιαίτερης προσοχής και από την πλευρά της ιδιωτικότητας.

Στο πρώτο κεφάλαιο της παρούσας μεταπτυχιακής διατριβής θα παρουσιαστούν μερικοί όροι και ορολογίες που θα βοηθήσουν στην κατανόηση των θεμάτων που θα επακολουθήσουν.

Επιπλέον, θα διατυπωθεί ο ορισμός της Αποτροπής Απώλειας Δεδομένων, ενώ επίσης θα περιγραφούν και ιδιότητες των δεδομένων που χρήζουν ιδιαίτερης προσοχής και προστασίας όπως το είδος αυτών αλλά και το πού συναντώνται.

1.1 Βασικοί Ορισμοί

Υπάρχουν δυο τύποι δεδομένων των οποίων γίνεται η αναζήτηση: τα καταχωρημένα δεδομένα (**Registered Data**) και τα περιγραφικά δεδομένα (**Described Data**). Τα **καταχωρημένα δεδομένα** είναι δεδομένα τα οποία είναι γνωστή η εμφάνισή τους (δηλ. η μορφή τους) ενώ τα **περιγραφικά δεδομένα** τα προσδιορίζουμε με βάση το μοτίβο τους. Τα καταχωρημένα δεδομένα είναι χρήσιμα στο εντοπισμό ευαίσθητων πληροφοριών όπως φράσεις (phrases), αριθμοί και ακολουθίες δυαδικών ψηφίων (bit sequences). Τα περιγραφικά δεδομένα είναι αρκετά χρήσιμα όταν προσπαθούμε να εντοπίσουμε συγκεκριμένα είδη πληροφοριών που δεν περιορίζονται σε γνωστά δεδομένα. Για παράδειγμα περιγραφικά είναι οι πιστωτικές κάρτες (Visa Card), οι διευθύνσεις κατοικίας (Street Address) και οι αριθμοί κοινωνικών ασφαλίσεων (SSN). [026]

Απώλεια δεδομένων (Data Loss) χαρακτηρίζεται ως η απώλεια των δεδομένων που βρίσκονται αποθηκευμένα σε οποιαδήποτε συσκευή του οργανισμού. Το πρόβλημα αφορά τον κάθε χρήστη ηλεκτρονικού υπολογιστή. Η απώλεια δεδομένων συμβαίνει όταν τα δεδομένα αφαιρεθούν από τον οργανισμό με φυσικό ή τεχνικό τρόπο είτε αυτό γίνεται εκούσια, είτε πολλές φορές ακούσια. Η απώλεια δεδομένων είναι ένα από τα μεγαλύτερα προβλήματα που συναντάμε σε οργανισμούς τις σημερινές μέρες, πράγμα που οι οργανισμοί έχουν ευθύνη να το ξεπεράσουν. [026]

Διαρροή Δεδομένων (Data Leakage) συναντάμε όταν η εμπιστευτικότητα (Confidentiality) των πληροφοριών έχει παραβιαστεί. Συμβαίνει όταν γίνεται μη εξουσιοδοτημένη μετάδοση (Unauthorized Transmission) των δεδομένων από το εσωτερικό ενός οργανισμού σε ένα εξωτερικό προορισμό. [026]

Οι όροι Απώλεια Δεδομένων (Data Loss) και Διαρροή Δεδομένων (Data Leakage) παρουσιάζονται πολλές φορές μόνοι τους ή και μαζί με τελικό στόχο να θέλουν να τονίσουν την παραβίαση δεδομένων (data breach) η οποία είναι ένας από τους μεγαλύτερους φόβους των οργανισμών σήμερα.

Ψευδώς Θετικές Ειδοποιήσεις (False Positives) συμβαίνει όταν το εργαλείο ειδοποιήσει για μη θεμιτή πρόσβαση (π.χ. πρόσβαση σε εμπιστευτικό αρχείο), αλλά τελικά η πρόσβαση ήταν θεμιτή.

Ψευδώς Αρνητικές Ειδοποιήσεις (False Negatives) υποδηλώνουν ότι συνέβη μία μη θεμιτή πρόσβαση, την οποία όμως το εργαλείο δεν εντόπισε (την χαρακτήρισε ως θεμιτή).

Αποτροπή Απώλειας Δεδομένων (Data Loss Prevention DLP) είναι όρος της Ασφάλειας Πληροφοριακών Συστημάτων ο οποίος αναφέρεται στο Σύστημα το οποίο χρησιμοποιείται για την παρακολούθηση, εντόπιση και ανάλυση εμπιστευτικών δεδομένων με σκοπό την αποτροπή της απώλειας τους. Οι τεχνολογίες της αποτροπής απώλειας δεδομένων χρησιμοποιούνται για να προστατευόσουν ευαίσθητα δεδομένα που βρίσκονται σε αδράνεια (Data At Rest), δεδομένα σε κίνηση (Data In Motion), και δεδομένα που βρίσκονται σε καταληκτικό σημείο (Data at the Endpoint) (συχνά τα δεδομένα σε αυτό το επίπεδο αναφέρονται και δεδομένα κατά τη χρήση Data In Use). Η Τεχνολογία Αποτροπής Απώλειας Δεδομένων εντοπίζει εμπιστευτικά δεδομένα χρησιμοποιώντας τεχνικές ανάλυσης περιεχομένου στα αρχεία του οργανισμού. Έχει σχεδιαστεί με σκοπό να προστατεύει τα δεδομένα και τις πληροφορίες των οργανισμών έτσι ώστε να επηρεάζει στο ελάχιστο τις επιχειρηματικές διαδικασίες του οργανισμού. [026]

- **Δεδομένα σε κίνηση (Data in Motion):** είναι τα δεδομένα που κινούνται μέσω δικτύου.

- **Δεδομένα σε αδράνεια (Data at Rest):** είναι δεδομένα που είναι αποθηκευμένα σε φορητούς υπολογιστές (Laptops), υπολογιστές γραφείου (Desktop Pcs), διακομιστές (Servers).

- **Τα δεδομένα σε καταληκτικό σημείο (Data at the Endpoint):** είναι τα δεδομένα που χειρίζονται οι τελικοί χρήστες. [028, 044, 058]

Εμπιστευτικά δεδομένα (Confidential data) είναι κάθε πολύτιμη πληροφορία ενός οργανισμού η οποία χρήζει υψηλού επιπέδου προστασίας και στην οποία έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα.[137]

Μία άλλη κατηγοριοποίηση των δεδομένων βάση του περιεχομένου τους, που ενδεχομένως εμπίπτουν πολλές φορές στην κατηγορία των εμπιστευτικών, είναι τα **προσωπικά δεδομένα** (Personal data) και τα **ευαίσθητα δεδομένα** (Sensitive data).

Προσωπικά δεδομένα είναι κάθε πληροφορία (άμεση ή έμμεση) που αναφέρεται σε φυσικό πρόσωπο και χαρακτηρίζει το υποκείμενο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη. Οποιαδήποτε πληροφορία αναφορικά με το άτομο θεωρείται εν γένει προσωπικό του δεδομένο Ονοματεπώνυμο, διεύθυνση, τηλέφωνο, αρ. πιστωτικής κάρτας κτλ. αλλά και, IP διεύθυνση, nickname (π.χ. σε κάποιο blog) κτλ. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία. [137]

Ευαίσθητα δεδομένα είναι τα προσωπικά δεδομένα που προσδιορίζουν την φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, την συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια, την ερωτική ζωή, τις ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις Τα πιο πάνω ευαίσθητα δεδομένα εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας και χρήζουν ακόμα μεγαλύτερης προστασίας (προβλέπεται στους σχετικούς νόμους).[137]

1.2 Δομή της Εργασίας

Στο πρώτο κεφάλαιο της παρούσας μεταπτυχιακής διατριβής θα παρουσιαστούν μερικοί όροι και ορολογίες που θα βοηθήσουν στην κατανόηση των θεμάτων που θα επακολουθήσουν. Επιπλέον, θα διατυπωθεί ο ορισμός της Αποτροπής Απώλειας Δεδομένων, ενώ επίσης θα περιγραφούν και ιδιότητες των δεδομένων που χρήζουν ιδιαίτερης προσοχής και προστασίας όπως το είδος αυτών αλλά και το πού συναντώνται.

Στο δεύτερο κεφάλαιο με τίτλο Εργαλεία Αποτροπής Απώλειας Δεδομένων θα γίνει μια σύντομη ανασκόπηση των υπάρχων τεχνολογιών ασφαλείας. Επιπλέον θα εξετάσουμε τα Εργαλεία Αποτροπής Απώλειας Δεδομένων ως προς την Αρχιτεκτονικής τους. Πιο συγκεκριμένα θα χρησιμοποιήσουμε την τεχνολογική λύση της εταιρείας RSA με ονομασία EMC RSA Data Loss Prevention suite V9.0.

Στο τρίτο κεφάλαιο θα παρουσιαστούν οι διάφορες τεχνικές ανίχνευσης Διαρροής Δεδομένων καθώς επίσης και η λειτουργία τους.

Στο τέταρτο κεφάλαιο γίνεται μια εκτενείς αναφορά στις Σύγχρονες Τεχνολογίες Αποτροπής Απώλειας Δεδομένων στην αρχιτεκτονική τους καθώς επίσης ποιες από της τεχνικές ανίχνευσης

Διαρροής Δεδομένων χρησιμοποιεί το κάθε εργαλείο. Στην συνέχεια θα παρουσιαστεί μέσα από πραγματικά συμβάντα η λειτουργία του εργαλείου της εταιρείας CA με ονομασία CA DataMinder.

Στο κεφάλαιο πέντε με τίτλο Ζητήματα ιδιωτικότητας θα μελετήσουμε τα εργαλεία Αποτροπής Απώλειας Δεδομένων ως προς την ιδιωτικότητα. Θα γίνει μια εκτενής αναφορά στο νομικό πλαίσιο και στο τι έχει ειπωθεί για την παρακολούθηση στο χώρο εργασίας.

Στο κεφάλαιο έξι θα γίνει μια συγκριτική αποτίμηση των διαφόρων τεχνικών, μεθόδων ανίχνευσης δεδομένων των οποίων εφαρμόζονται στα εργαλεία Αποτροπής Απώλειας Δεδομένων. Οι διάφορες τεχνικές ανίχνευσης θα αξιολογηθούν ως προς την αποτελεσματικότητα ανίχνευσης διαρροής δεδομένων και ταυτόχρονα θα εξεταστούν κατά πόσο οι μέθοδοι αυτές είναι φιλικές ως προς την ιδιωτικότητα.

Στο κεφάλαιο επτά με τίτλο Επίλογο θα παρουσιαστούν τα τελικά μας συμπεράσματα όσο αφορά τα Εργαλεία Αποτροπής Απώλειας Δεδομένων.

Κεφάλαιο 2
Εργαλεία Αποτροπής Απώλειας Δεδομένων

Στο παρόν κεφάλαιο θα περιγράψουμε αρχικά τις τεχνολογίες οι οποίες προσφέρουν ασφάλεια σε ένα οργανισμό: όπως θα καταδείξουμε, οι περισσότερες εξ αυτών παρέχουν ασφάλεια μόνο από εξωτερικές επιθέσεις. Αντίθετα, η τεχνολογία Αποτροπής Απώλειας Δεδομένων που μελετάται στην παρούσα εργασία ελέγχει όχι μόνο την εισερχόμενη αλλά και την εξερχόμενη ροή δεδομένων. Επιπλέον, θα μελετηθεί η τεχνολογία Αποτροπής Απώλειας Δεδομένων ως προς την Αρχιτεκτονική της. Θα γίνει μια παρουσίαση των εργαλείων και των δομικών τους συστατικών ως προς το πού τοποθετούνται και για ποιο σκοπό είναι υπεύθυνα.

2.1 Υπάρχουσες Τεχνολογίες Ασφαλείας

Υπάρχουν πολύ ισχυρές τεχνολογίες οι οποίες συμβάλουν στην πρόληψη και αποτροπή απώλειας κρίσιμων δεδομένων στους οργανισμούς από μια εξωτερική επίθεση (outside attack) που θα λάβει χώρα. Οι τεχνολογίες αυτές ωστόσο αντιμετωπίζουν μόνο εξωτερικές επιθέσεις, σε αντίθεση με την τεχνολογία που μελετούμε στην παρούσα Μεταπτυχιακή Διατριβή και αφορά τα Εργαλεία Αποτροπής Απώλειας Δεδομένων (DLP), τα οποία επικεντρώνονται κυρίως στις εσωτερικές επιθέσεις (inside attacks) που ξεκινούν από ενέργειες εντός του οργανισμού και οι οποίες επίσης μπορούν να προκαλέσουν απώλεια και διαρροή δεδομένων.

Μερικές από τις τεχνολογίες για την αντιμετώπιση των εξωτερικών επιθέσεων είναι:

Α) Anti - Malware. Το κακόβουλο Λογισμικό (Malicious Software-Malware) είναι λογισμικό που σχεδιάστηκε για να επηρεάζει την λειτουργία του ηλεκτρονικού υπολογιστή, να συγκεντρώνει ευαίσθητες πληροφορίες, ή να αποκτά μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφορικής. Τύποι κακόβουλου Λογισμικού είναι οι Ιοί (Virus), και τα Σκουλήκια (Worms). Ένας ιός απαιτεί την παρέμβαση του χρήστη για να εξαπλωθεί, ενώ το Σκουλήκι εξαπλώνεται από μόνο του. Το κακόβουλο λογισμικό μολύνει το ηλεκτρονικό υπολογιστή και κλέβει προσωπικά δεδομένα. Τα κακόβουλα λογισμικά που κλέβουν δεδομένα είναι τα key loggers, οι screen scrapers, το spyware, το adware, τα backdoors και τα bots.

Το Anti – Malware εγκαθίσταται στο πυρήνα (Kernel) του Λειτουργικού Συστήματος (Operating System OS) με το ίδιο τρόπο όπως το κακόβουλο λογισμικό και προσπαθεί να ενεργήσει από εκεί. Κάθε φορά που το Λειτουργικό Σύστημα εκτελεί μια εργασία, το anti – malware ελέγχει ότι το λειτουργικό σύστημα κάνει εγκεκριμένες εργασίες. Το λογισμικό anti – malware είναι πολύ αποτελεσματικό αλλά κοιτάζει μόνο απειλές από το εξωτερικό περιβάλλον. Το λογισμικό anti – malware βοηθά στην πρόληψη της απώλειας δεδομένων από εξωτερικές απειλές, αλλά όμως δεν παρέχει προστασία έναντι εσωτερικών απειλών. [074, 128]

Β) Αναχώματα Ασφαλείας (Firewalls) χαρακτηρίζουμε μια συλλογή από κατάλληλα συστήματα, τοποθετημένα στο σημείο σύνδεσης της υπό- προστασία δικτυακής περιοχής με τα υπόλοιπα δίκτυα, η οποία επιβάλλει προκαθορισμένη πολιτική ασφαλείας. Το Ανάχωμα ασφαλείας μπορεί να είναι είτε Υλικό (Hardware) είτε Λογισμικό (Software). Ο ρόλος του Αναχώματος Ασφαλείας μπορεί να είναι τόσο η αποτροπή μη εξουσιοδοτημένων προσβάσεων σε μια ασφαλή περιοχή, όσο και η αποτροπή μη εξουσιοδοτημένης εξόδου πληροφορίας από μια περιοχή. Μπορεί δηλαδή

να λειτουργήσει ως θύρα έλεγχου της κίνησης και προς τις δυο κατευθύνσεις. Ελέγχει την εισερχόμενη και εξερχομένη κίνηση του δικτύου αναλύοντας τα πακέτα δεδομένων και καθορίζει ποια επιτρέπονται να περάσουν και ποια όχι. Τα Αναχώματα Ασφαλείας είναι ένα από τα καλύτερα εργαλεία ασφαλείας τα οποία χρησιμοποιούν οι οργανισμοί. [074,076,128]

Γ) Εργαλεία Ανίχνευσης Ευπαθειών. Η ανίχνευση ευπαθειών είναι εν γένει μια συνεχής διαδικασία η οποία εντοπίζει και προστατεύει πολύτιμα δεδομένα και μετριάζει τα τρωτά σημεία (Vulnerabilities). Τα τρωτά σημεία αντιμετωπίζονται με την εφαρμογή επικαιροποιημένων εκδόσεων λογισμικού (Patches) και αλλαγή ρυθμίσεων. Με αυτόν τον τρόπο αντιμετωπίζονται τα κύρια αίτια και δημιουργείται ασπίδα (Shield) των συστημάτων από τις απειλές (Threats). Οι ανιχνευτές ευπαθειών (Vulnerability Scanners) χρησιμοποιούνται για να αναγνωρίσουν και να ταξινομήσουν τα τρωτά σημεία. Αναζητούν για ευπάθειες τις οποίες γνωρίζουν, δηλαδή ευπάθειες οι οποίες έχουν ανακοινωθεί από την κοινότητα της ασφαλείας και έχουν ήδη διορθώσει οι κατασκευαστές με ενημερώσεις ασφαλείας. Από το αποτέλεσμα του ελέγχου, εφόσον υλοποιηθούν τα κατάλληλα μέτρα, προκύπτει ισχυροποίηση των εφαρμογών και ανθεκτικότητα τους έναντι εξωτερικών επιθέσεων (Outside Attacks). [076]

Δ) Τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDS) είναι υλικό ή λογισμικό το οποίο παρακολουθεί τις δραστηριότητες του δικτύου ή του συστήματος για κακόβουλες δραστηριότητες (Malicious Activities). Το Σύστημα Ανίχνευσης εισβολών εντοπίζει μια πιθανή παραβίαση ασφαλείας, καταγράφει τις πληροφορίες και δίνει ειδοποίηση με σηματοδότηση. [076,088]

Ε) Τα Συστήματα Πρόληψης Εισβολών (Intrusion Prevention Systems - IPS) είναι υλικό, ή λογισμικό, που παρακολουθούν τις δραστηριότητες του δικτύου και του συστήματος για κακόβουλες δραστηριότητες. Κυρίως προσδιορίζουν κακόβουλες ενέργειες, καταγράφουν πληροφορίες, προσπαθούν να εμποδίσουν και να σταματήσουν δραστηριότητες. Τα Συστήματα Πρόληψης Εισβολών αποτελούν προέκταση των Συστημάτων Ανίχνευσης Εισβολών. Τα Συστήματα Πρόληψης Εισβολών προλαμβάνουν και εμποδίζουν τις εισβολές που ανιχνεύονται, όπως για παράδειγμα μπορεί να παρεμποδίσει κίνηση από μια κακόβουλη διεύθυνση IP. [023, 026]

2.2 Σουίτα Εργαλείων Αποτροπής Απώλειας Δεδομένων

Οι τεχνολογίες που αναφέραμε πιο πάνω χρησιμοποιούνται για την πρόληψη εξωτερικών επιθέσεων και ελάχιστα για τις εσωτερικές επιθέσεις και απειλές (Attacks/Threats).

Σε αντίθεση με τις πιο πάνω τεχνολογίες , η τεχνολογία αποτροπής απώλειας δεδομένων παρέχει προστασία στα κρίσιμα δεδομένα που βρίσκονται σε αδράνεια (Data at Rest), σε κίνηση (Data in Motion) και που βρίσκονται σε καταληκτικό σημείο (Data at the Endpoint), προλαμβάνοντας τυχόν απώλεια και διαρροή τους.

Οι Σουίτες Εργαλείων Αποτροπής Απώλειας Δεδομένων (Data Loss Prevention Suites) σε ένα οργανισμό, ανιχνεύουν τις εμπιστευτικές πληροφορίες ο οποίες διακινούνται μέσω των τεχνολογιών πληροφορικής και αποτρέπουν την απώλεια και διαρροή τους.

Οι Σουίτες Εργαλείων Αποτροπής Απώλειας Δεδομένων παρέχουν προστασία στις τρεις πιο κάτω περιοχές:

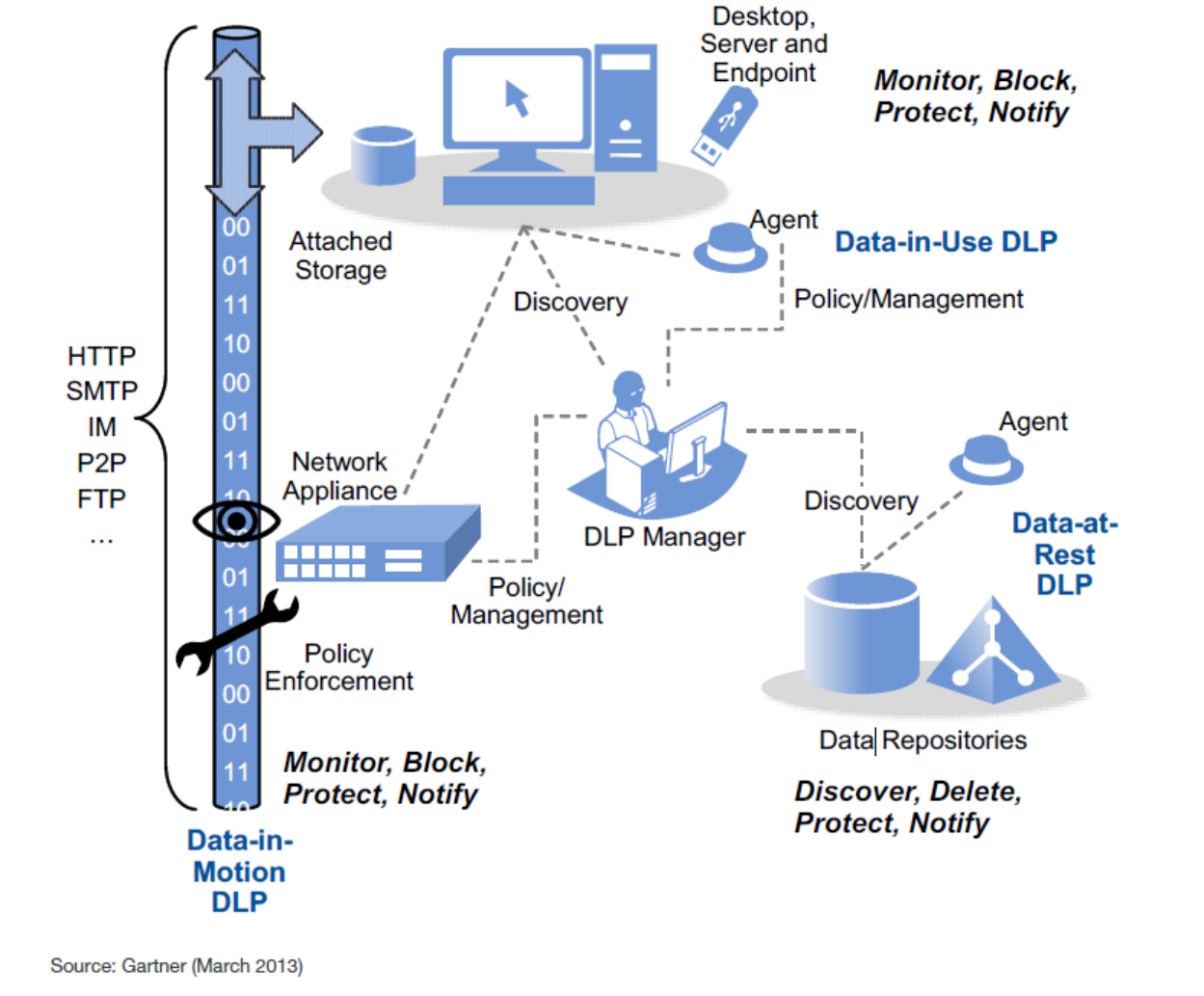
- **Δεδομένα σε κίνηση (Data in Motion):** είναι τα δεδομένα που κινούνται μέσω δικτύου.

- **Δεδομένα σε κατάσταση ηρεμίας (Data at Rest):** είναι δεδομένα που είναι αποθηκευμένα σε φορητούς υπολογιστές (Laptops), υπολογιστές γραφείου (Desktop Pcs), διακομιστές (Servers).

- **Τα δεδομένα σε καταληκτικό σημείο (Data at the Endpoint):** είναι τα δεδομένα που χειρίζονται οι τελικοί χρήστες. [028, 044, 058]

2.2.1 Αρχιτεκτονική της Τεχνολογίας

Στο παρόν κεφάλαιο περιγράφεται η συνήθης αρχιτεκτονική ενός δικτύου με εγκατεστημένη την τεχνολογία Data Loss Prevention. Η πιο κάτω περιγραφή και τα σχήματα βασίζεται στο προϊόν EMC RSA Data Loss Prevention suite V9.0 της εταιρείας RSA. [074]



Εικόνα 2.1: Αρχιτεκτονική Εργαλείων Αποτροπής Απώλειας Δεδομένων. [022]

Μια **Σουίτα Εργαλείων Αποτροπής Απώλειας Δεδομένων** DLP αποτελείται από τέσσερα δομικά συστατικά: τον DLP Enterprise Manager, τον DLP Datacenter, τον DLP Network και τον DLP Endpoint. Ο **DLP Enterprise Manager** διαχειρίζεται τα υπόλοιπα τρία εργαλεία (DLP Datacenter, DLP Network και DLP Endpoint) μέσω μιας εφαρμογής ιστού (Web Application). Τα προϊόντα DLP Datacenter, DLP Network και DLP Endpoint δουλεύουν ανεξάρτητα το ένα με το άλλο. Ένας οργανισμός μπορεί να έχει μόνο ένα από αυτά τα τρία ή και τα τρία ταυτόχρονα. Για να δουλέψει οποιοδήποτε προϊόν από τα τρία χρειάζεται να είναι εγκατεστημένος ο DLP Enterprise Manager, διότι είναι απαραίτητος για να παρέχει διαχείριση της πρόσβασης στα άλλα προϊόντα. Χωρίς τον DLP Enterprise Manager δεν μπορεί κανείς να χειριστεί τα άλλα τρία εργαλεία.

Όπως διακρίνεται στο παρακάτω σχήμα κάθε εργαλείο αποτελείται από δικά του συστατικά μέρη.

Το εργαλείο **DLP Network** συμπεριλαμβάνει τα ακόλουθα εξαρτήματα:

- DLP Network Controller
- DLP Network Sensor
- DLP Network Interceptor
- DLP Network ICAP Server
- DLP Network Exchange Transport Agent

Το εργαλείο **DLP Endpoint** συμπεριλαμβάνει τα ακόλουθα εξαρτήματα.

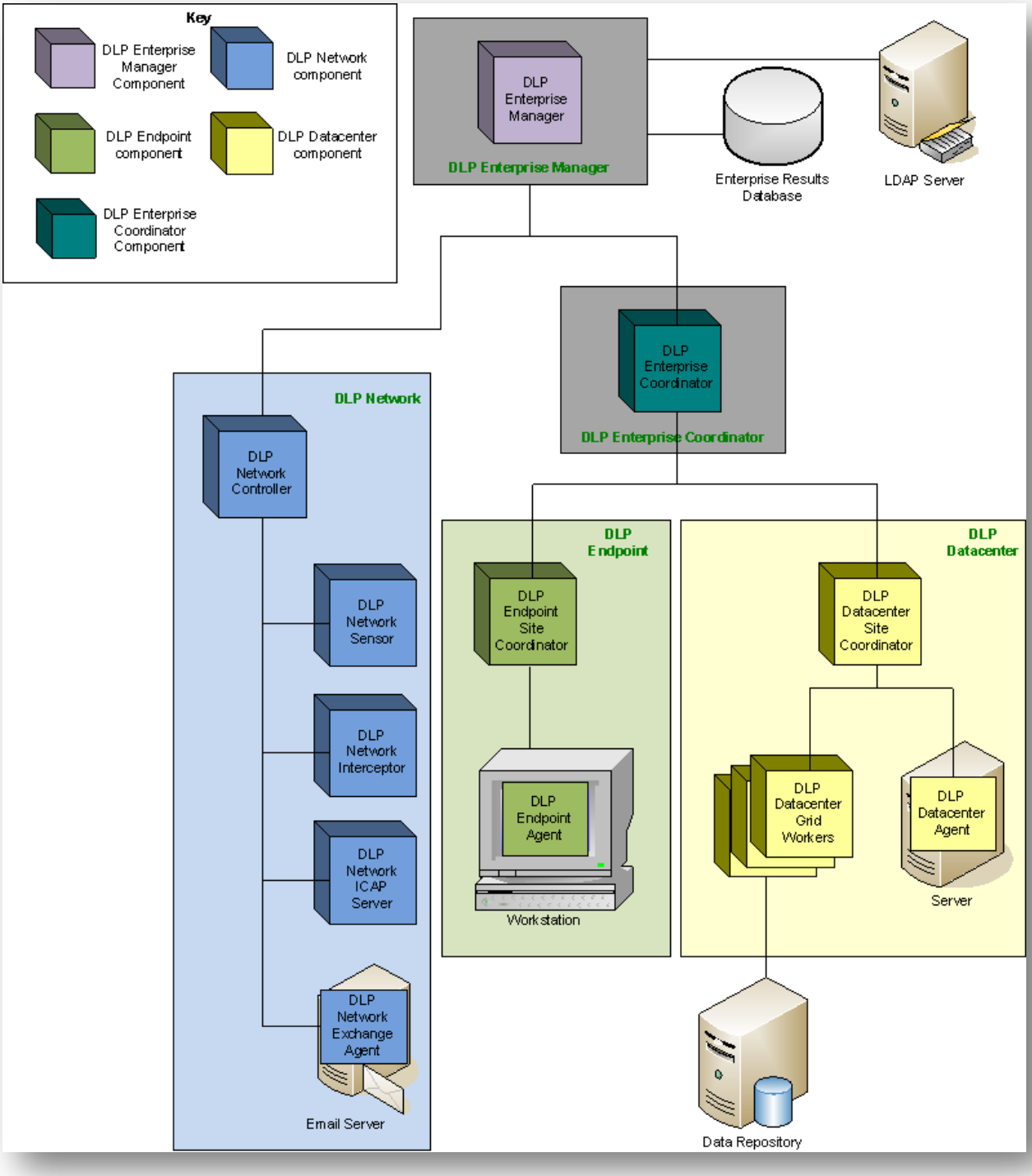
- DLP Enterprise Coordinator
- DLP Endpoint Site Coordinator
- DLP Endpoint Agent

Το εργαλείο **DLP Datacenter** συμπεριλαμβάνει τα ακόλουθα εξαρτήματα.

- DLP Enterprise Coordinator
- DLP Datacenter Site Coordinator
- DLP Datacenter Grid Worker
- DLP Datacenter Agent

Το εργαλείο **DLP Enterprise Manager** είναι το κεντρικό σημείο όπου γίνεται ο έλεγχος των υπολοίπων προϊόντων.

Στα παρακάτω σχήματα διακρίνουμε τα τέσσερα DLP προϊόντα εργαλεία που υπάρχουν σε μια : Αρχιτεκτονική Εργαλείων Αποτροπής Απώλειας Δεδομένων.



Εικόνα 2.3: Αρχιτεκτονική Εργαλείων Αποτροπής Απώλειας Δεδομένων.[074]

2.2.1.1 DLP Enterprise Manager

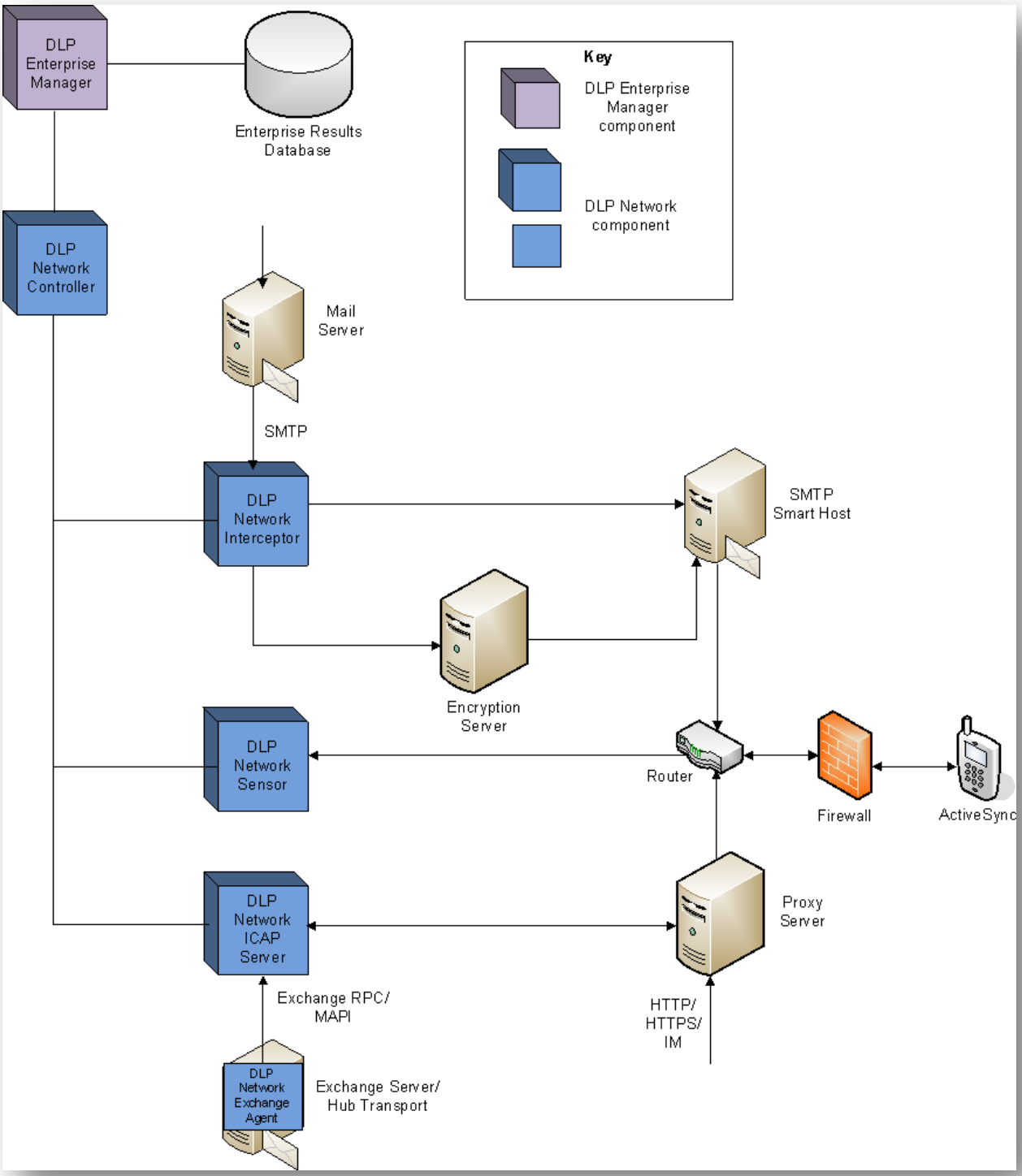
Ο **DLP Enterprise Manager** είναι μια εφαρμογή ιστού (Web Application) με την οποίαν ο Διαχειριστής (Administrator) ρυθμίζει και διαχειρίζεται τα άλλα προϊόντα DLP.

2.2.1.2 DLP Network

Το προϊόν **DLP Network** ανιχνεύει κρίσιμα δεδομένα τα οποία μεταδίδονται μέσω δικτύου. Τα δεδομένα που εξετάζονται αναφέρονται ως Δεδομένα σε Κίνηση. Το προϊόν **DLP Network** μπορεί αυτόματα να παρακολουθεί, να βάζει σε καραντίνα, αλλά και να αποτρέπει την εξαγωγή δεδομένων από το δίκτυο του οργανισμού.

Το προϊόν **DLP Network** έχει τη δυνατότητα παρακολούθησης και έλεγχου σε ένα ευρύ φάσμα πρωτοκόλλων του επιπέδου εφαρμογής OSI (Application Layer Protocols) που είναι τα ακόλουθα: Πρωτόκολλο Μεταφοράς Υπερκείμενου (Hypertext Transport Protocol-HTTP), Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκείμενου (HTTPS), ActiveSync, Πρωτόκολλο Μεταφοράς Απλών Μηνυμάτων (Simple Mail Transport Protocol-SMTP), Πρωτόκολλο Μεταφοράς Αρχείων (File Transfer Protocol-FTP), Telnet, Πρωτόκολλο Προσπέλασης Μηνυμάτων Διαδικτύου (Internet Message Access Protocol-IMAP), Πρωτόκολλο Ταχυδρομείου (Post Office Protocol 3-POP3), Άμεσα Μηνύματα (Instant Messaging-IM) όπως Yahoo, MSN, Google, and AOL.

Στο παρακάτω σχήμα διακρίνουμε μια τυπική τοπολογία για το **DLP Network**..



Εικόνα 2.4: Τοπολογία DLP Network.[074]

Το προϊόν **DLP Network** περιλαμβάνει συγκεκριμένες λειτουργικές μονάδες οι οποίες βοηθούν στην πρόληψη της απώλειας και διαρροής πληροφοριών.

Ο **DLP Network Controller** (Ελεγκτής δικτύου) είναι η κύρια συσκευή που διατηρεί πληροφορίες σχετικά με κρίσιμα δεδομένα και το περιεχόμενο των πολιτικών μεταφοράς. Υπάρχουν τρεις τύποι συσκευών οι οποίες διαχειρίζονται από το **DLP Network Controller:** οι **DLP Network Sensors** (Αισθητήρες), **Interceptors** (Αναχαιτιστές) και **ICAP Servers** (Διακομιστές). Οι συσκευές αυτές παρακολουθούν τις μεταδόσεις που γίνονται στο δίκτυο και δίνουν αναφορές σχετικά με τους εντοπισμούς που έχουν γίνει.

Οι **DLP Network Sensors** εγκαθίστανται στα σύνορα του δικτύου. Μπορούν να παρακολουθούν την κίνηση IPV4 και IPV6 που διασχίζει τα σύνορα του δικτύου και να αναλύουν το εμπιστευτικό περιεχόμενο.

Το **DLP Network Interceptor** (Αναχαιτιστής) εγκαθίσταται και αυτό στα σύνορα του δικτύου, αλλά αυτό δίνει την δυνατότητα στους διαχειριστές να εφαρμόσουν πολιτικές οι οποίες βάζουν σε καραντίνα ή απορρίπτουν κίνηση ηλεκτρονικού ταχυδρομείου, το οποίο περιλαμβάνει εμπιστευτικό περιεχόμενο.

Ο **DLP Network ICAP Server** δίνει την δυνατότητα στους διαχειριστές να παρακολουθούν το Πρωτόκολλο Μεταφοράς Υπερκείμενου, το Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκείμενου και το Πρωτόκολλο Μεταφοράς Αρχείων να τα απορρίπτουν όταν αυτά έχουν εμπιστευτικό ή οποιουδήποτε άλλου τύπου κρίσιμο περιεχόμενο. Ο **DLP Network ICAP Server** μπορεί να ενσωματωθεί απευθείας με ένα Microsoft Exchange Server, με αυτό τον τρόπο μπορεί να παρακολουθεί και να ελέγχει ActiveSync μεταδόσεις για την αποφυγή εμπιστευτικών ή άλλων κρίσιμων μηνυμάτων ηλεκτρονικού ταχυδρομείου, από χρήστες που έχουν πρόσβαση στο σύστημα ηλεκτρονικού ταχυδρομείου με κινητές συσκευές έξω από το δίκτυο του οργανισμού. Ο **DLP Network Exchange Transport Agent** μπορεί να εγκατασταθεί σε ένα **Exchange Server/Hub Transport** και να παρέχει προστασία και παρακολούθηση για την εσωτερική ηλεκτρονική αλληλογραφία που κινείται στο δίκτυο του οργανισμού σε συνεργασία με το **DLP Network ICAP Server.** [074]

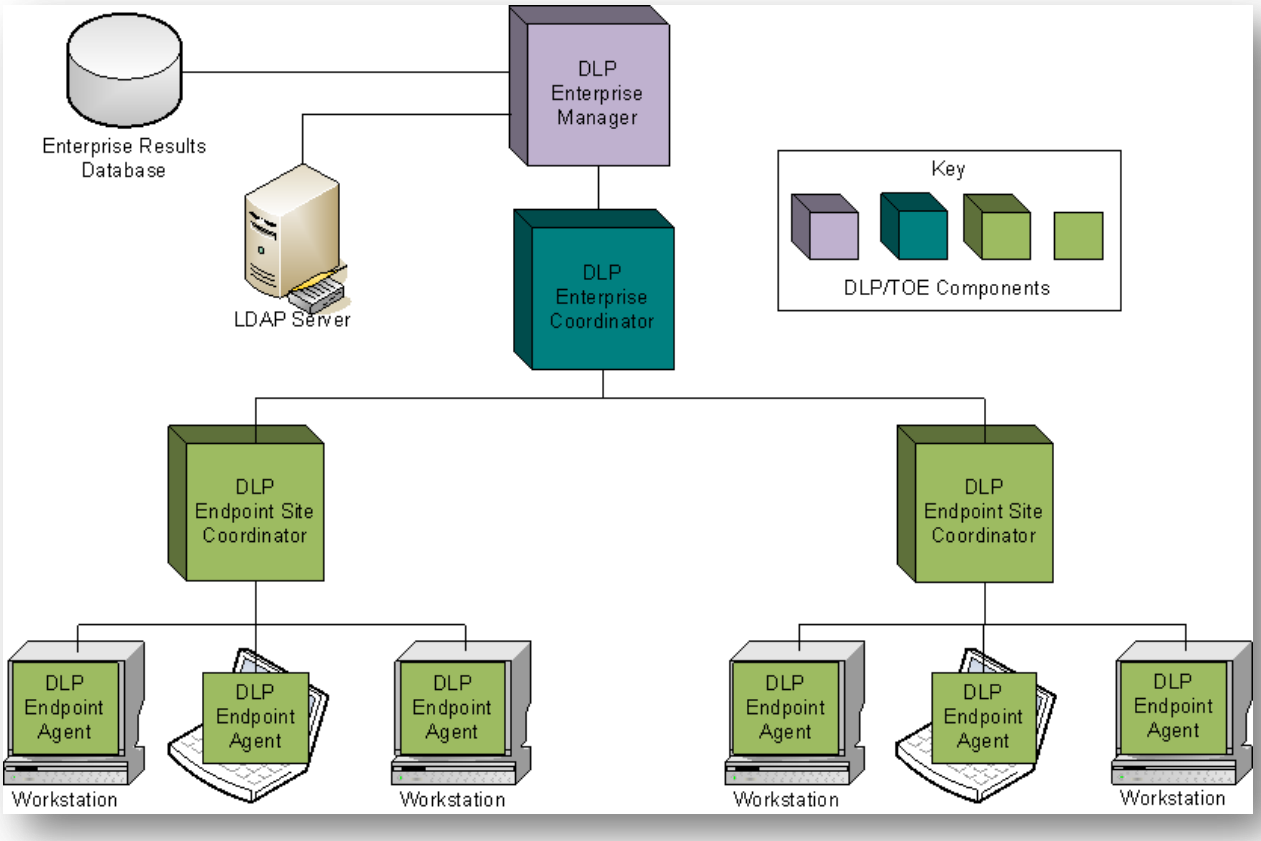
2.2.1.3 DLP Endpoint

Το προϊόν **DLP Endpoint** παρέχει έλεγχο στις ευαίσθητες πληροφορίες οι οποίες χειρίζονται οι τελικοί χρήστες (End-Users). Τα στοχευόμενα δεδομένα αναφέρονται ως Δεδομένα σε Καταληκτικό σημείο. Το προϊόν **DLP Endpoint** παρακολουθεί την δραστηριότητα των δεδομένων για παρατυπίες ή ύποπτες κινήσεις, ειδοποιεί τους διαχειριστές για διεργασίες που

είναι ενδεχομένως επικίνδυνες και εμποδίζει την απώλεια ευαίσθητου περιεχομένου από τους υπολογιστές του δικτύου.

Στο παρακάτω σχήμα διακρίνουμε την τοπολογία **DLP Endpoint.**

Το προϊόν **DLP Endpoint** περιλαμβάνει τρία εξαρτήματα το **DLP Endpoint Agent,** το **DLP Enterprise Coordinator**, το **DLP Endpoint Site Coordinator**.



Εικόνα 2.5: Τοπολογία DLP Endpoint.[074]

Ο **DLP Endpoint Agent** εφαρμόζει πολιτικές για τη χρήση των δεδομένων με αποτέλεσμα το μπλοκάρισμά τους (όταν κάτι τέτοιο κρίνεται απαραίτητο) και δημιουργεί εγγραφές συμβάντων που περιγράφουν την παραβίαση.

Ο **DLP Endpoint Agent** προωθεί τα συμβάντα (Events) στον **DLP Endpoint Site Coordinator.** Ο **DLP Endpoint Agent** ανακτά τις προκαθορισμένες πολιτικές και ρυθμίσεις από τον **DLP Endpoint Site Coordinator**.

Ο **DLP Endpoint Agent** είναι η υπηρεσία η οποία ξεκινά με το έναρξη του ηλεκτρονικού υπολογιστή και παρακολουθεί τις ενέργειες του τελικού χρήστη όσο ο υπολογιστής είναι σε λειτουργία. Οι **DLP Endpoint Agents** εκτελούνται μέσα από το Λειτουργικό Σύστημα και τις Εφαρμογές (Desktop Applications). Ο **DLP Endpoint Agent** εισβάλει σε κάθε τρέχουσα διαδικασία (Running Process) και παρακολουθεί/ελέγχει τις εφαρμογές. Για παράδειγμα όταν ο τελικός χρήστης επιχειρήσει να αντιγράψει, μετακινήσει ή τυπώσει , τότε ο **DLP Endpoint Agent** κάνει ανάλυση του περιεχομένου του αρχείου και ελέγχει αν αντίκειται στις πολιτικές του οργανισμού.

Εάν δεν συνάδει με τις πολιτικές του οργανισμού, τότε ο **DLP Endpoint Agent** στέλνει ένα συμβάν στον **DLP Endpoint Site Coordinator** και η ενέργεια (action) είτε επιτρέπεται είτε όχι ανάλογα με την πολιτική. Ο **DLP Endpoint Agent** εμφανίζει ένα εικονίδιο συστήματος (System Tray Icon) στον τελικό χρηστή, το οποίο εικονίδιο παρέχει μηνύματα και αποδέχεται το κείμενο αιτιολόγησης από τους τελικούς χρήστες.

Οι Διαχειριστές μπορούν επίσης να προσδιορίσουν ειδικές ενέργειες (Custom Actions) που επιτρέπουν στον **DLP Endpoint Agent** να επιβάλει προσαρμοσμένες ενέργειες κατά την ανίχνευση της παραβίασης.

Κάθε **DLP Endpoint Agent** λαμβάνει οδηγίες από τον **DLP Endpoint Site Coordinator** και επιστρέφει τα αποτελέσματα σε αυτόν.

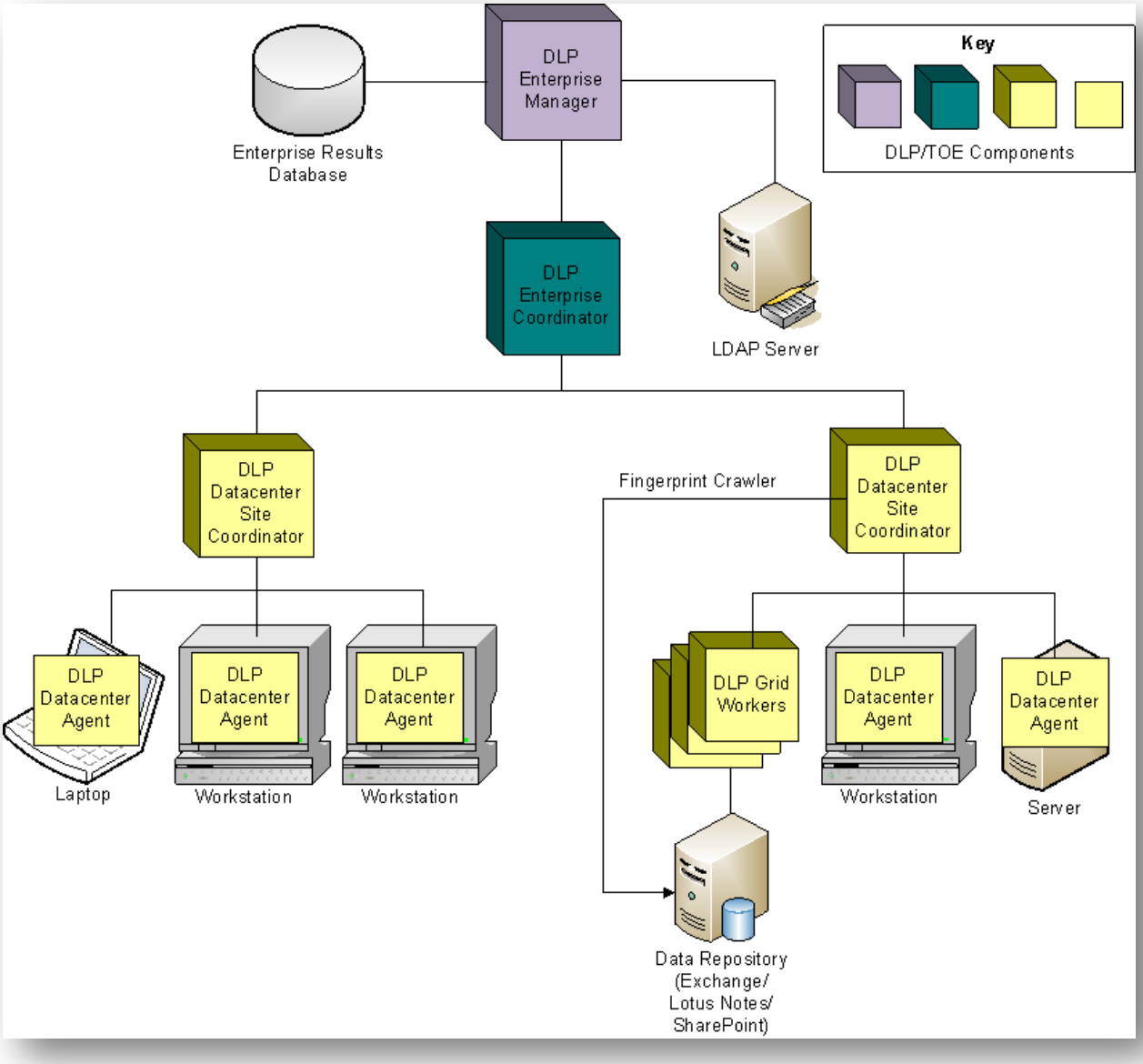
Ο **DLP Endpoint Site Coordinator** είναι η υπηρεσία που διαχειρίζεται τις σαρώσεις στο τοπικό δίκτυο (Local Network). Σε ένα οργανισμό μπορούμε να εγκαταστήσουμε όσους **DLP Datacenter Site Coordinator** χρειάζεται για να συντονίζουν τους **DLP Datacenter Agent,** οι οποίοι είναι διάσπαρτοι στην επιχείρηση.

Ο **DLP Enterprise Coordinator** είναι ο κύριος ελεγκτής μιας τυπικής εγκατάστασης **DLP Endpoint.** Στέλνει οδηγίες και συλλέγει τα αποτελέσματα των σαρώσεων από όλους τους **DLP Endpoint Site Coordinator** οι οποίοι είναι εγκατεστημένοι στον οργανισμό.

Ο **DLP Enterprise Coordinator** διαχειρίζεται τις πολιτικές και συλλέγει συμβάντα (events) από τον **DLP Endpoint Site Coordinator** σε όλο το δίκτυο και περνά τις πληροφορίες στον **DLP Enterprise Manager** για την προβολή του σε γραφικό περιβάλλον χρήστη (Graphical User Interface-GUI). Επιπλέον, ο **DLP Enterprise Coordinator**, ο **DLP Endpoint Site Coordinator** και ο **DLP Endpoint Agent** συλλέγουν τα αρχεία καταγραφής έλεγχου (Audit logs) και τα κατεβάζουν (Download) στο **DLP Enterprise Manager** όπου μπορούν να προβληθούν μέσω του γραφικού περιβάλλοντος χρήστη.[074]

2.2.1.4 DLP Datacenter

Το προϊόν **DLP Datacenter** εντοπίζει δεδομένα τα οποία περιέχουν κρίσιμο περιεχόμενο και τα οποία είναι αποθηκευμένα σε Φορητούς Υπολογιστές, Υπολογιστές Γραφείου ή Διακομιστές τα οποία διανέμονται στο οργανισμό. Τα δεδομένα που εξετάζονται αναφέρονται ως Δεδομένα σε Αδράνεια. Ο **DLP Datacenter** σαρώνει τα δίκτυα του οργανισμού, και εξετάζει τα αρχεία που βρίσκονται στις μηχανές που έχουν προσδιοριστεί. Στο παρακάτω σχήμα διακρίνουμε την



Εικόνα 2.6: Τοπολογία DLP Datacenter.[074]

τοπολογία ενός **DLP Datacenter.**

Ο **DLP Datacenter** συμπεριλαμβάνει διάφορα εργαλεία τα οποία λειτουργούν ταυτόχρονα για να παρέχουν σαρώσεις και πληροφορίες που συγκεντρώθηκαν από αυτά.

Ο **DLP Enterprise Coordinator** έχει περιγραφτεί στην ενότητα DLP Endpoint.

Ο **DLP Datacenter Site Coordinator** έχει την ίδια λειτουργιά με τον DLP Endpoint Site Coordinator και έχει περιγραφτεί στην ενότητα DLP Endpoint.

Ο **DLP Datacenter Grid Worker** είναι πράκτορας σάρωσης που χρησιμοποιείται για ειδικούς σκοπούς. Χρησιμοποιείται κυρίως για ανάλυση μεγάλου όγκου αποθηκευμένων δεδομένων.

Ο **DLP Datacenter Agent** έχει την ίδια λειτουργιά με τον DLP Endpoint Agent και έχει περιγραφτεί στην ενότητα DLP Endpoint.

Ο **DLP Enterprise Manager** είναι η εφαρμογή όπου οι διαχειριστές μπορούν να διαχειρίζονται το **DLP Datacenter**. Οι Διαχειριστές μπορεί να είναι ειδικοί στην ασφάλεια (Security Specialists) οι οποίοι αναλύουν τα συμβάντα που παράγονται από τα εργαλεία του **DLP Datacenter** ή άλλοι ειδικοί ή Διαχειριστές Συστήματος οι οποίοι δημιουργούν, σχεδιάζουν και τρέχουν σαρώσεις.

Όταν το προϊόν **DLP Datacenter** σαρώνει έχει πρόσβαση σε (συγκεκριμένη ομάδα σάρωσης ή) σύνολο μηχανημάτων στο δίκτυο τα οποία έχει καθορίσει ο Διαχειριστής.

Οι Διαχειριστές μπορούν να ορίσουν όσες ομάδες σάρωσης οποιουδήποτε μεγέθους επιθυμούν και όσες απαιτούνται.

Υπάρχουν τέσσερεις τύποι ομάδων σαρώσεων:

1. Ομάδες Agent-scan για σαρώσεις στους υπολογιστές γραφείου και φορητούς υπολογιστές.

2. Ομάδες Grid-scan για τις σαρώσεις του δικτύου σε μεγάλα αποθετήρια δεδομένων.

3. Ομάδες Repository scan για αποθετήρια.

4. Ομάδες Repository scan για βάσεις δεδομένων.

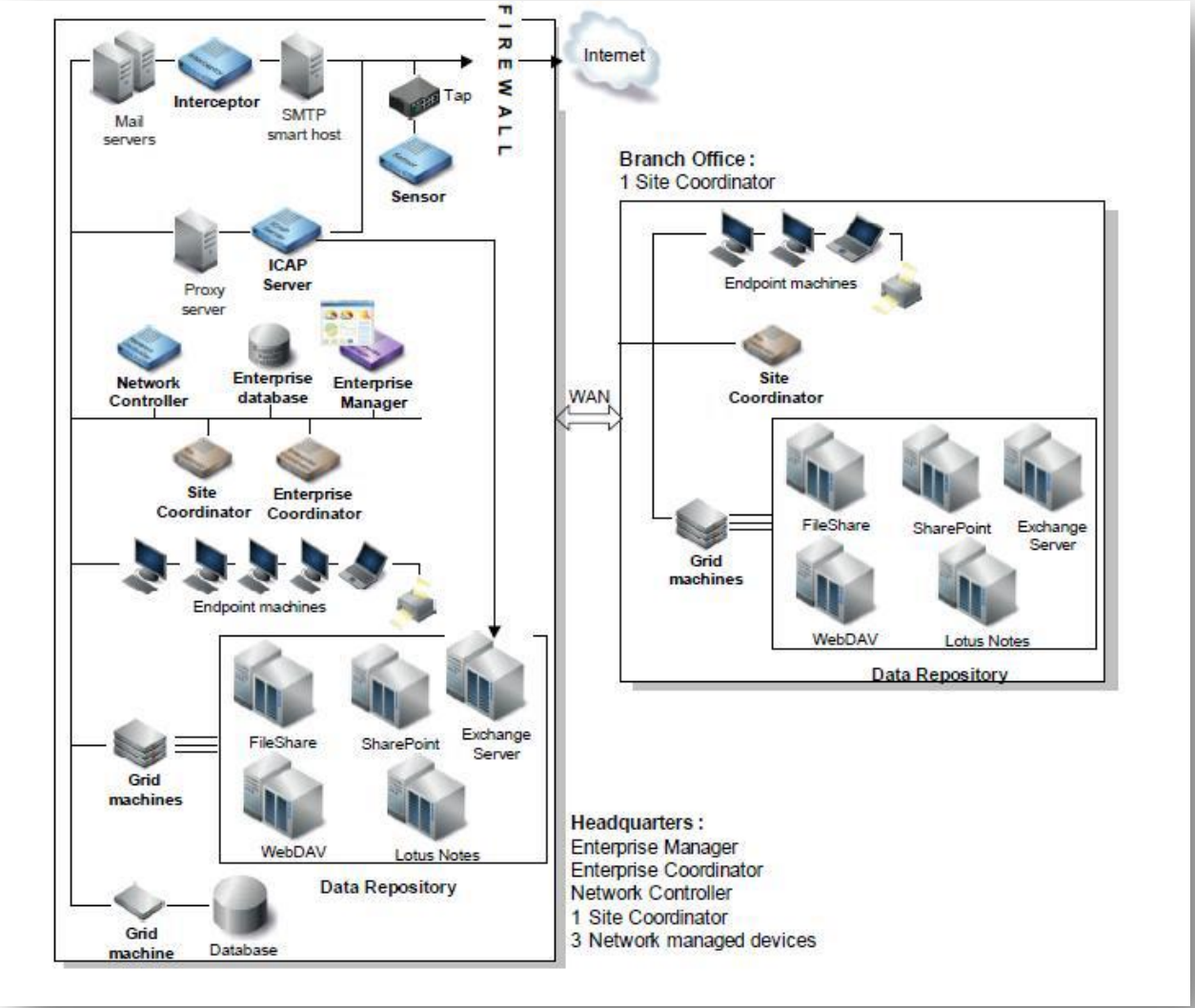
Επιπλέον, οι DLP Datacenter Agents μπορούν να είναι προσωρινοί ή μόνιμοι.

Οι **DLP Datacenter Grid workers** είναι πράκτορες σάρωσης οι οποίοι χρησιμοποιούνται για συγκεκριμένους σκοπούς. Κυρίως χρησιμοποιούνται για να αναλύουν μεγάλες αποθήκες δεδομένων.

Οι **DLP Datacenter Site Coordinators** διαχειρίζονται επίσης τις ομάδες **grid-scan** στα οποία ένας αριθμός από **Datacenter Grid-workers** συνεργάζονται για να σαρώσουν μεγάλο αριθμό από κοινόχρηστα αρχεία (File Share). Οι **DLP Datacenter site Coordinators** διαχειρίζονται επίσης τις ομάδες **repository-scan** και **database-scan** οι οποίες αναλύουν ιδιόκτητα αρχεία (Proprietary Files) όπως SharePoint και Βάσεις Δεδομένων αντίστοιχα. [074]

2.2.2 Σχεδιασμός της ανάπτυξης μιας DLP σουίτας σε ένα οργανισμό.

Έχοντας περιγράψει τα επιμέρους συστατικά, μπορούμε πλέον να καταδείξουμε την αρχιτεκτονική ενός DLP συστήματος σε υψηλό επίπεδο. Στο παρακάτω διάγραμμα παρουσιάζεται ένα παράδειγμα αρχιτεκτονικής ψηλού επίπεδου πλήρους ανάπτυξης μιας DLP σουίτας σε ένα οργανισμό.



Εικόνα 2.7: Αρχιτεκτονική ψηλού επίπεδου πλήρους ανάπτυξης μιας DLP σουίτας.[076]

Στο διάγραμμά μας παρουσιάζονται τα πιο κάτω χαρακτηριστικά:

Ο οργανισμός αποτελείται από τα κεντρικά γραφεία (Headquarters Office) τα οποία περιέχουν τους εργαζομένους (Employees), τις συναφείς υποδομές τους καθώς και τα υποκαταστήματα (Branch Offices).

Τα υποκαταστήματα είναι συνδεδεμένα με τα κεντρικά γραφεία με τη βοήθεια υψηλής ταχύτητας Δικτύου Ευρείας Περιοχής (WAN). Τα κεντρικά γραφεία περιέχουν επιπλέον Ανάχωμα Ασφάλειας και σύνδεση στο Διαδίκτυο.

Τα υποκαταστήματα συνδέονται στο Διαδίκτυο μέσω των Διακομιστών Ιστού (Web Servers) των κεντρικών γραφείων.

Τα υποκαταστήματα για να έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο (Email) συνδέονται με το Διακομιστή ταχυδρομείου (Mail Server) των κεντρικών γραφείων.

Τα περισσότερα εταιρικά αρχεία και οι μεγάλες Βάσεις Δεδομένων (Databases) είναι τοποθετημένες στα κεντρικά γραφεία, ενώ κάποια υποκαταστήματα έχουν τους δικούς τους μεγάλους Διακομιστές Αποθήκευσης Αρχείων (File Servers).

Στο οργανισμό τοποθετούνται τρία προϊόντα DLP το DLP Datacenter, DLP Endpoint και DLP Network για να προστατευτούμε Δεδομένα τα οποία βρίσκονται σε Αδράνεια, Δεδομένα σε Καταληκτικό σημείο και Δεδομένα σε Κίνηση.

DLP Datacenter

Σε ένα DLP Datacenter περιλαμβάνονται τα πιο κάτω χαρακτηριστικά:

- Ένα Site Coordinator στα κεντρικά γραφεία, και ένα σε κάθε υποκατάστημα.

- Υπάρχουν ομάδες από Agent-scan, μία στα κεντρικά γραφεία και μία σε κάθε υποκατάστημα για να σαρώνει τα τερματικά τους ηλεκτρονικούς υπολογιστές των χρηστών.

- Υπάρχουν ομάδες από Grid-scan μια για κάθε μεγάλο Διακομιστή Αρχείων (NAS, SAN) στα κεντρικά γραφεία ή υποκαταστήματα.

- Υπάρχουν ομάδες από Repository-scan, μία για κάθε αποθετήριο αρχείων (όπως το SharePoint) στα κεντρικά γραφεία.

- Υπάρχουν Ομάδες από Database-scan - μία για κάθε εταιρική Βάση Δεδομένων στα κεντρικά γραφεία.

- Μηχανές από Grid-workers – ρυθμισμένες για χρήση από κάθε grid, repository, ή ομάδα από σαρωτών βάσεων δεδομένων. Είναι εγκατεστημένα σύμφωνα με τις ανάγκες.

- Scanning agents- εγκαθίσταται όπου χρειάζεται σε κάθε τερματικό (endpoint) και grid-worker μηχάνημα. [074, 076]

DLP Endpoint

Σε ένα DLP Endpoint περιλαμβάνονται τα πιο κάτω χαρακτηριστικά:

- Ένα Site Coordinator στα κεντρικά γραφεία, και σε καθένα από τα υποκαταστήματα (έχει δημιουργηθεί ήδη από το DLP Datacenter).

- Ομάδες Endpoint – μια στα κεντρικά γραφεία και μια για κάθε υποκατάστημα, για την παρακολούθηση των ενεργειών των χρηστών στα τερματικά.

- Enforcement agents – εγκαθίσταται όπου χρειάζεται σε κάθε τερματικό.[074,076]

DLP Network

Σε ένα DLP Network περιλαμβάνονται τα πιο κάτω χαρακτηριστικά:

- Network Sensor (Αισθητήρας Δικτύου) το οποίο συνδέεται μεταξύ του εσωτερικού δικτύου του οργανισμού και του διαδικτύου.

- Network Interceptor (Αναχαιτιστής Δικτύου) είναι μια συσκευή που συνδέεται στο δίκτυο για την σύλληψη εξερχόμενης και εισερχόμενης ηλεκτρονικής αλληλογραφίας.

- Network ICAP Server συνδέεται στο δίκτυο με συνδυασμό του Διακομιστή Μεσολάβησης (Proxy Server) για σύλληψη μεταδόσεων του Πρωτοκόλλου Μεταφοράς Υπερκειμένου και του Πρωτοκόλλου Μεταφοράς Αρχειων.[074, 076]

Κεφάλαιο 3
Τεχνικές Ανίχνευσης Διαρροής Δεδομένων

Τα Εργαλεία Αποτροπής Απώλειας Δεδομένων εφαρμόζουν διαφορές τεχνικές για να αποτρέψουν την εσκεμμένη ή την ακούσια απώλεια και διαρροή εμπιστευτικών δεδομένων ενός οργανισμού. Μερικές από αυτές είναι: η Αντιστοίχηση Λέξεων Κλειδιών (Keyword Matching), η Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων (Rule and Regular Expression Matching), το Αποτύπωμα Δεδομένων (Data Fingerprinting), τα Χαρακτηριστικά των Αρχείων (File Attribute), η Ανάλυση Βάσει Εννοιών (Conceptual/Lexicon Analysis), οι Κατηγορίες (Categories) και οι Αλγόριθμοι Μηχανικής Μάθησης (Machine Learning Algorithms).

Η ανάλυση δεδομένων (Data Analysis) εκτελείται σε δυο επίπεδα (Domains), στο επίπεδο Περιεχομένου (**Content**) και στο επίπεδο Πλαισίου (**Context**). Το περιεχόμενο (Content) του αρχείου συμπεριλαμβάνει την ανάλυση του ιδίου του πραγματικού αρχείου. Το πλαίσιο ενός αρχείου χωρίζεται σε μετά δεδομένα (Meta-Data) και επιχειρησιακό πλαίσιο (Business Context).

Τα μετά δεδομένα συνδέονται άμεσα με το αρχείο, περιλαμβάνουν χαρακτηριστικά όπως τον ιδιοκτήτη του αρχείου (File Owner), το μέγεθος του αρχείου (File Size), την ημερομηνία δημιουργίας (Date of Creation), καθώς και την ημερομηνία τελευταίας πρόσβασης στο αρχείο (Data at Last Access). Το επιχειρησιακό πλαίσιο είναι οι πληροφορίες που δεν συνδέονται άμεσα με το ίδιο το αρχείο. Για παράδειγμα, τέτοιες είναι οι πληροφορίες του συστήματος όπου είναι αποθηκευμένο το αρχείο, ποιες εφαρμογές έχουν πρόσβαση στο αρχείο, ποιες ώρες της ημέρας έχουν πρόσβαση στο αρχείο, καθώς και ο αποστολέα (Sender) και ο παραλήπτης (Recipient) στην περίπτωση της ηλεκτρονικής αλληλογραφίας (e-mail).

Υπάρχουν δυο τύποι δεδομένων των οποίων γίνεται η αναζήτηση: τα καταχωρημένα δεδομένα (**Registered data**) και τα περιγραφικά δεδομένα (**Described data**). Τα καταχωρημένα δεδομένα είναι δεδομένα με γνωστή εμφάνιση ενώ τα περιγραφικά δεδομένα προσδιορίζονται με βάση το μοτίβο τους. Τα καταχωρημένα δεδομένα είναι χρήσιμα στο εντοπισμό συγκεκριμένων κρίσιμων πληροφοριών όπως φράσεις, αριθμοί και ακολουθίες δυαδικών ψηφίων. Τα περιγραφικά δεδομένα είναι αρκετά χρήσιμα όταν προσπαθούμε να εντοπίσουμε συγκεκριμένα είδη πληροφοριών που δεν περιορίζονται σε γνωστά δεδομένα. Για παράδειγμα περιγραφικά δεδομένα είναι οι πιστωτικές κάρτες, οι διευθύνσεις κατοικίας και οι αριθμοί κοινωνικών ασφαλίσεων.[026]

Στη συνέχεια γίνεται μία ανάλυση των πιο πάνω τεχνικών.

3.1 Αντιστοίχηση Λέξεων-Κλειδιών

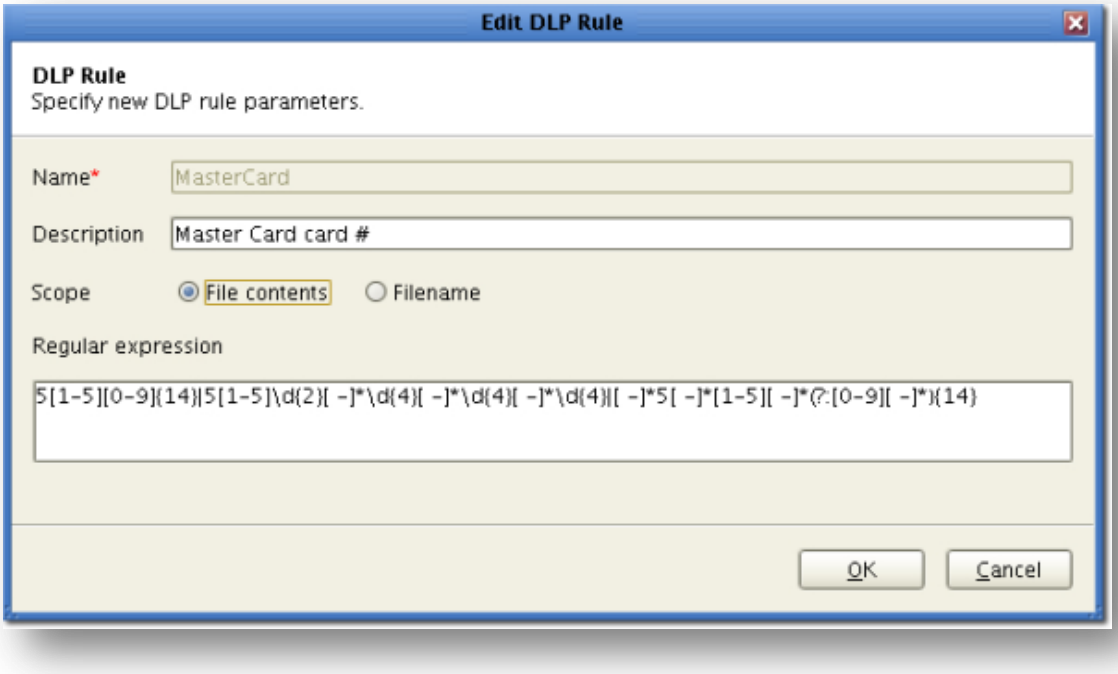
Η μέθοδος Ανάλυσης περιεχομένου Αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching) σαρώνει τα αρχεία του συστήματος κάνοντας αναζητήσεις ως προς προκαθορισμένες λέξεις-κλειδιά, που βρίσκονται σε μια προκαθορισμένη λίστα. Όταν εντοπιστεί μια αντιστοίχηση, το Εργαλείο Αποτροπής Απώλειας Δεδομένων ειδοποιεί τους διαχειριστές του συστήματος.

Η μέθοδος Αντιστοίχηση Λέξεων-Κλειδιών είναι αρκετά γρήγορη και αποτελεσματική εάν τα κρίσιμα δεδομένα περιέχουν κείμενο. Δυστυχώς όμως, ένας οργανισμός δεν έχει μόνο εμπιστευτικά δεδομένα σε μορφή κειμένου. Η χρήση της τεχνικής Αντιστοίχηση Λέξεων-Κλειδιών συνίσταται να χρησιμοποιείται σε απλά έγγραφα όπου περιέχουν στατικό κείμενο. Ευτυχώς όμως τα εργαλεία αποτροπής απώλειας δεδομένων δεν περιορίζονται σε μόνο αυτήν την τεχνική ανάλυσης περιεχομένου.[026, 042, 058, 061, 069, 075, 088]

3.2 Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων

Όπως προκύπτει από τα ανωτέρω, με την μέθοδο Ανάλυσης Περιεχομένου Αντιστοίχηση Λέξεων-Κλειδιών δεν είναι δυνατός ο εντοπισμός διαρροής ευαίσθητων δεδομένων όπως πιστωτικές κάρτες ή αριθμοί κοινωνικών ασφαλίσεων. Η πιο αποτελεσματική μέθοδος για εντοπισμό αυτού του είδους εμπιστευτικών δεδομένων είναι η τεχνική Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων (Rule-Based και Regular Expression Matching) .

Η τεχνική Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων αναλύει το περιεχόμενο των δεδομένων με βάση συγκεκριμένους κανόνες, όπως για παράδειγμα τα 16 ψηφία από τα οποία αποτελείται μια πιστωτική κάρτα, τον έλεγχο αθροίσματος (Checksum) για συγκεκριμένους κωδικούς κ.α.. Τα περισσότερα εργαλεία αποτροπής απώλειας δεδομένων έχουν δικούς τους προκαθορισμένους κανόνες ενσωματωμένους, όμως ταυτόχρονα μπορεί οποιοσδήποτε να δημιουργήσει τους δικούς του κανόνες με βάση τις απαιτήσεις του οργανισμού του. Η πιο κάτω εικόνα περιγράφει την τεχνική Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων που χρησιμοποιείτε για την Master Card.



Εικόνα 3.1: Κανόνας της τεχνικής αντιστοίχιση κανόνων και τυπικών εκφράσεων. [080]

Ο κανόνας Regular Expression είναι:

5[1-5][0-9]{14}|5[1-5]\d{2}[-]*\d{4}[-]*\d{4}[-]*\d{4}|[-]*5[-]*[1-5][-]*(?:[0-9][-]*){14}

Στο παρόν κανόνα υπάρχουν δυο κάθετες μπάρες **|,** οι οποίες μεταφράζονται με το διαχωριστικό- διαζευκτικό σύνδεσμο «ή» (or).

Όποτε ο πιο πάνω μακροσκελής κανόνας regular expression αποτελείται από τρεις μικρότερους κανόνες, που χωρίζονται από τις δυο κάθετες μπάρες **(|)** και ο καθένας αναφέρεται στην **Master Card** .

- **5[1-5][0-9]{14}**
- **5[1-5]\d{2}[-]*\d{4}[-]*\d{4}[-]*\d{4}**
- **[-]*5[-]*[1-5][-]*(?:[0-9][-]*){14}**

Τα άγκιστρα αγκύλες (Curly brackets) **{ }** χρησιμοποιούνται για να καθορίσουν των αριθμών των χαρακτήρων. Μπορούν να χρησιμοποιηθούν με τους ακόλουθους τρεις τρόπους.

1. **{min, max}** με το min συμβολίζει το ελάχιστο αριθμό χαρακτήρων και το max το μέγιστο αριθμό.

2. **{min,}** με το min συμβολίζει το ελάχιστο αριθμό χαρακτήρων και ο μέγιστος είναι το άπειρο (Infinitive ∞).

3. **{exact}** με το exact συμβολίζει το ακριβή αριθμό χαρακτήρων.

Ας πάρουμε για παράδειγμα το πρώτο κανόνα regular expression **5[1-5][0-9]{14}**. Ο κανόνας πρέπει να ξεκινήσει με το αριθμό 5, ακολουθεί με ένα αριθμό από το 1 μέχρι το 5 και στην συνεχεία να ακολουθείτε από 14 χαρακτήρες με τιμές που κυμαίνονται από το 0 μέχρι το 9 έτσι μπορεί να θεωρηθεί μια Master Card η οποία αποτελείτε από 16 ψηφία.

Για παράδειγμα ο αριθμός Master Card 5201 5555 8135 7985 ικανοποιεί το κανόνα μας ενώ ο αριθμός Master Card 4502 5555 4275 4563 δεν ικανοποίει για το λόγο ότι αρχίζει με το ψηφίο 4.

Ας πάρουμε το δεύτερο κανόνα regular expression **5[1-5]\d{2}[-]*\d{4}[-]*\d{4}[-]*\d{4}**, και το χωρίσουμε σε μικρότερα τμήματα.

5[1-5]\d{2}[-]*\d{4}[-]*\d{4}[-]*\d{4}

Όπως και στον πρώτο κανόνα έτσι και στο δεύτερο το **5[1-5]** εννοεί πως πρέπει να ξεκινήσει με το αριθμό 5 και ακολουθεί ένας αριθμός από το 1 μέχρι το 5. Όσο για το **\d{2}** εννοεί ότι θα ακολουθήσουν 2 χαρακτήρες {2}, οι οποίοι είναι από το 0 μέχρι το 9 **\d**.

5[1-5]\d{2}**[-]*\d{4}[-]***\d{4}[-]*\d{4}

Στο δεύτερο κομμάτι περιέχεται η έκφραση **[-]*** η οποία μεταφράζεται με ένα κενό, μια παύλα ή τίποτα. Αυτή ακολουθείται από 4 ψηφία **(\d(4))** και ξανά από ένα κενό, μια παύλα ή τίποτα **([-]*)**

5[1-5]\d{2}[-]*\d{4}[-]***\d{4}[-]*\d{4}**

Στο τελευταίο τμήμα θα παρουσιαστούν 4 ψηφία μετά ένα κενό μια παύλα ή τίποτα και μετά ξανά 4 ψηφία, έτσι μπορεί να θεωρηθεί μια Master Card η οποία αποτελείτε από 16 ψηφία.

Για παράδειγμα, ο αριθμός Master Card 5423-4576-2298-5523 ικανοποιεί το κανόνα μας ενώ ο αριθμός Master Card 5423-4576 2298 5523 δεν ικανοποίει για το λόγο ότι περιέχει ταυτόχρονα παύλες και κενά.

Ο τρίτος και τελευταίος κανόνας Regular Expression είναι:

[-]*5[-]*[1-5][-]*(?:[0-9][-]*){14}

Ο κανόνας πρέπει να ξεκινά **[-]*** με οποιοδήποτε αριθμό ακόμα και μηδενικό, από παύλες ή/και κενά και ακολουθείται από οποιοδήποτε αριθμό, παύλες ή/και κενό. Το δεύτερο ψηφίο του κανόνα **5[-]*** μπορεί να είναι οποιοσδήποτε αριθμός από το 1 μέχρι το 5 και να ακολουθείται από οποιοδήποτε αριθμό, παύλες ή/και κενά. Κάθε ένα από τα 14 ψηφία ακολουθείται από οποιοδήποτε αριθμό, παύλα ή/και κενό.

Ακολουθούν μερικά παραδείγματα όπου ταιριάζουν στο τρίτο κανόνα regular expression.

- 5 1 0 1 2 3 4 5 6 7 8 9 1 2 3 4
- 5-1-0-1-2-3-4-5-6-7-8-9-1-2-3-4
- 5-1 0 1 2345-6-7-89123 4
- 5- -1-0 1 2---3- 4--5 - 678-9 1 -2- 3 4

Σημαντικό πλεονέκτημα της μεθόδου είναι το γεγονός πως οι κανόνες μπορούν εύκολα να δημιουργηθούν, να ρυθμιστούν και να επεξεργαστούν. Κατ΄ επέκταση, η εν λόγω τεχνολογία μπορεί εύκολα να κατανοηθεί., ενώ είναι και προσαρμόσιμη στις εκάστοτε ανάγκες. Στα περισσότερα προϊόντα DLP οι κανόνες είναι ενσωματωμένοι στον προϊόν με την αγορά του, έτσι οι διαχειριστές εξοικονομούν πολύτιμο χρόνο στο να δημιουργήσουν κανόνες.

Μειονέκτημα της μεθόδου είναι το γεγονός ότι είναι επιρρεπής σε ψηλά ποσοστά Ψευδών Θετικών (False Positive) ειδοποιήσεων. Επιπλέον, προσφέρει μικρή προστασία σε αρχεία με μη δομημένο περιεχόμενο (Unstructured Content). [026, 042, 058, 061, 069, 075, 080, 088]

3.3 Αποτύπωμα Δεδομένων

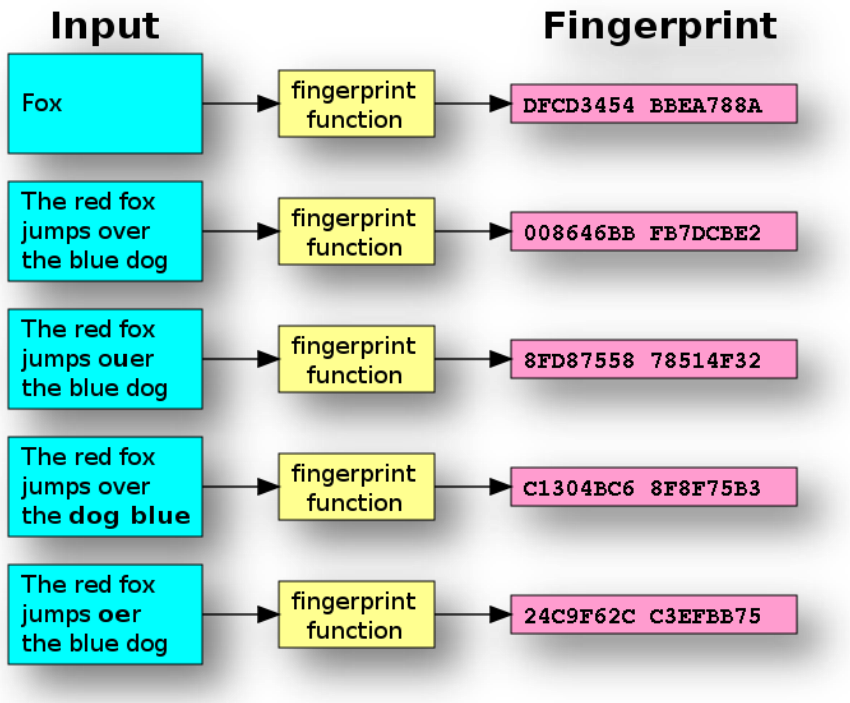
Μια εξίσου σημαντική μέθοδος για την Αποτροπή Απώλειας ευαίσθητων/ σημαντικών/ υψίστης σημασίας δεδομένων είναι η μέθοδος Αποτυπώματος Δεδομένων (Data Fingerprinting). Η μέθοδος Αποτυπώματος Δεδομένων πιο συγκεκριμένα υπολογίζει τη Συνάρτηση Κατακερματισμού (Hash Function) και των δυο αρχείων και ακολούθως τις συγκρίνει κομμάτι με κομμάτι (bit to bit).

Τα ωφελήματα της χρησιμοποίησης των κρυπτογραφικών συναρτήσεων κατακερματισμού (Cryptographic Hash Functions) είναι:

1**. Συναρτήσεις μιας κατεύθυνσης** (One way functions). Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις μιας κατεύθυνσης δηλαδή η τιμή της συνάρτησης για οποιοδήποτε είσοδο της υπολογίζεται εύκολα, όμως είναι μη αντιστρέψιμη ξέροντας κάποιος την έξοδο, δεν μπορεί να βρει την είσοδο. Για το λόγο αυτό εάν κάποιος επιτιθέμενος έχει πρόσβαση σε μια συνάρτηση κατακερματισμού δεν μπορεί να ανάκτηση οποιοδήποτε μέρος από το αρχείο μας.

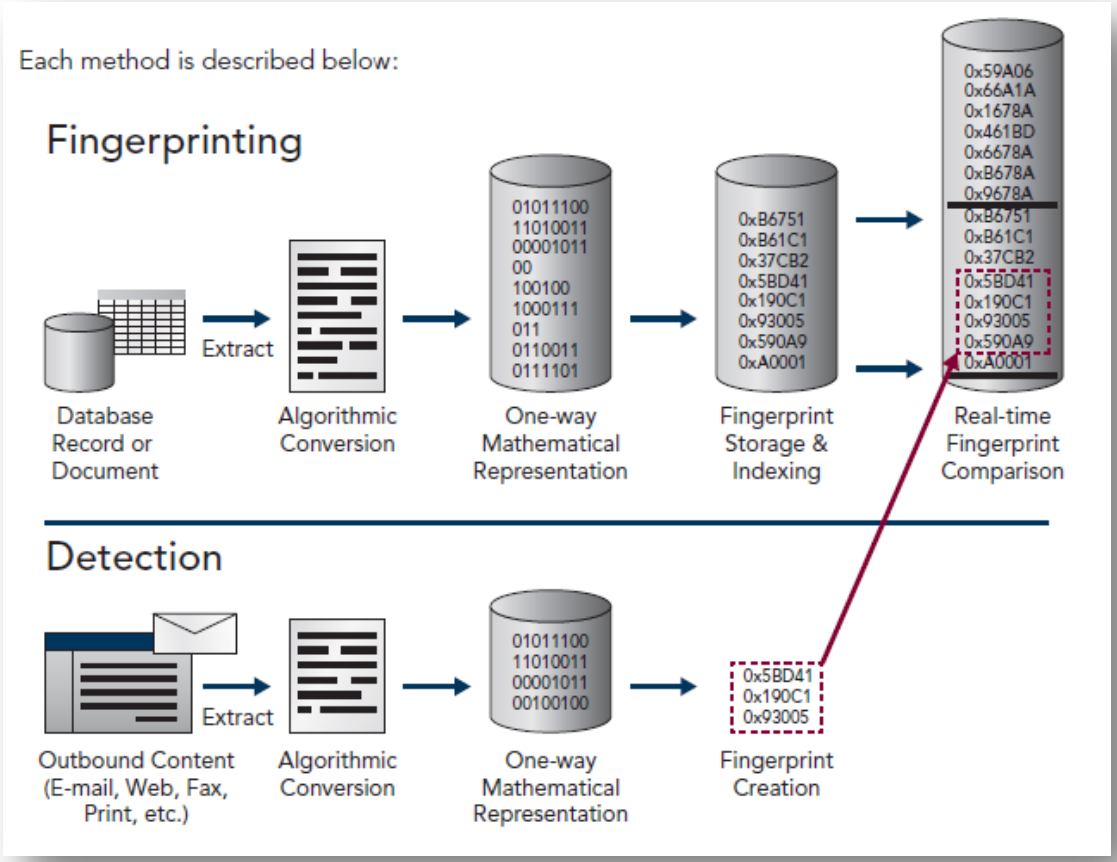
2. **Μέγεθος** (Size). Η συνάρτηση κατακερματισμού (Hash Function) καταλαμβάνει σημαντικά λιγότερο χώρο από το αρχείο μας. Συνεπώς η μεταφορά της μέσω δικτύου είναι γρήγορη και ταυτόχρονα έχει μικρή επιβάρυνση στο Δίκτυο μας. Επιπλέον, η αποθήκευση των Συναρτήσεων Κατακερματισμού είναι πιο εύκολη και αποτρέπει την αποθήκευση όλων των ευαίσθητων δεδομένων μας στο Διακομιστή Αποτροπής Απώλειας Δεδομένων (Data Loss Prevention Server).

3. **Μοναδική** (Unique). Κάθε συνάρτηση κατακερματισμού είναι μοναδική για κάθε αρχείο. Είναι πρακτικά ανέφικτο να βρεθούν δυο διαφορετικά αρχεία με το ίδιο αποτύπωμα (Fingerprint).



Εικόνα 3.2: Πως δουλεύει μια συνάρτηση κατακερματισμού.[110]

Η μέθοδος Αποτυπώματος Δεδομένων δουλεύει με όλους τους τύπους αρχείων. Επιπλέον έχει πολύ χαμηλό ποσοστό Ψευδώς Θετικών ειδοποιήσεων. [026, 042, 058, 061, 069, 075, 082, 088, 099, 109]



Εικόνα 3.3: Πως δουλεύει η μέθοδος αποτύπωμα αρχείου (Fingerprinting).[099]

3.4 Χαρακτηριστικά των Αρχείων

Τα Εργαλεία Αποτροπής Απώλειας Δεδομένων μπορούν να εντοπίζουν αρχεία με εμπιστευτικό περιεχόμενο με την τεχνική Χαρακτηριστικά των Αρχείων (File Attribute) όπως για παράδειγμα ο τύπος αρχείου (File Type) και το μέγεθος αρχείου (File Size). Τα Εργαλεία Αποτροπής Απώλειας Δεδομένων εκτελούν αληθινή ανίχνευση του τύπου του αρχείου, ακόμα κι αν η προέκταση του αρχείου (File Extension) έχει αλλάξει. [026, 061, 069]

3.5 Ανάλυση Βάσει Εννοιών

Η μέθοδος ανίχνευσης Ανάλυση Βάσει Εννοιών (Conceptual/Lexicon Analysis) συνδυάζει φράσεις και λέξεις που συνδέονται συνήθως με συγκεκριμένες έννοιες. Χρησιμοποιείται για να εντοπίσει εμπιστευτικές πληροφορίες ή ασυνήθιστη συμπεριφορά. Χρησιμοποιείται κυρίως σε

πιο σύνθετα Δομημένα Δεδομένα (Structured Data) τα οποία δεν μπορούν εύκολα να περιγραφούν και να εντοπιστούν με μεθόδους όπως είναι οι Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων και οι Κατηγορίες των απλών κανόνων. Για παράδειγμα, με τα εργαλεία αυτά μπορεί να γίνει εντοπισμός «ανάρμοστης» συμπεριφοράς των υπάλληλων, όπως η αναζήτηση νέας δουλειάς στο διαδίκτυο. [026, 042, 058, 069, 075, 088]

3.6 Κατηγορίες

Οι κατηγορίες (Categories) είναι προ-εγκατεστημένα πρότυπα με κανόνες και λεξικά από κοινούς τύπους εμπιστευτικών δεδομένων, όπως για παράδειγμα ο αριθμός της πιστωτικής κάρτας, PCI protection, HIPAA, IBAN, SWIFT/BIC.

Σημαντικό πλεονέκτημα των προ εγκατεστημένων κατηγοριών είναι ότι είναι εξαιρετικά άπλες στην ρύθμιση τους. Επιπλέον εξοικονομούν πολύτιμο χρόνο, αφού δεν χρειάζεται να κατασκευαστούν από τον οργανισμό. Για πολλούς οργανισμούς οι κατηγορίες μπορούν να καλύψουν ένα μεγάλο ποσοστό τους για τη προστασία των ευαίσθητων πληροφοριών που χρειάζεται.

Όμως είναι αυτονόητο ότι οι κατηγορίες που ταιριάζουν σε όλους του οργανισμούς ίσως να μην ανταποκρίνονται στις ιδιαιτερότητες που παρουσιάζει ένας οργανισμός. [042, 049, 069, 075, 088]

3.7 Αλγόριθμοι Μηχανικής Μάθησης

Η Μηχανική Μάθηση (Machine Learning) είναι μια περιοχή της τεχνητής νοημοσύνης (Artificial Intelligence) η οποία αφορά αλγορίθμους και μεθόδους που επιτρέπουν στους υπολογιστές να «μαθαίνουν» μέσα από παραδείγματα αντί να χρησιμοποιούν προκαθορισμένους κανόνες.

Σε ένα Εργαλείο Αποτροπής Απώλειας Δεδομένων το οποίο περιλαμβάνει σύστημα με μηχανική μάθηση, μπορείς κανείς να του παρέχει παραδείγματα (Examples) τα οποία θα εκπαιδεύουν (Train) το σύστημα για την προστασία των ευαίσθητων πληροφοριών του οργανισμού. Το σύστημα μετά την εκπαίδευση δημιουργεί ένα κατηγοριοποιητή (Classifier), ο οποίος κατηγοριοποιεί τα αρχεία ως προς την ομοιότητά τους σε σχέση με τα παραδείγματα.

Υπάρχουν δυο κατηγορίες Αλγορίθμων Μηχανικής Μάθησης, οι Αλγόριθμοι με επίβλεψη (Supervised learning algorithms) και οι αλγόριθμοι χωρίς επίβλεψη (Unsupervised learning algorithms).

Στους αλγορίθμους με επίβλεψη (Supervised learning), ο αλγόριθμος κατασκευάζει μια συνάρτηση που απεικονίζει δεδομένες εισόδους σε γνωστές, επιθυμητές εξόδους (σύνολο εκπαίδευσης), με απώτερο στόχο τη γενίκευση της συνάρτησης αυτής και για εισόδους με άγνωστη έξοδο (σύνολο ελέγχου).[111]

Στους αλγόριθμους χωρίς επίβλεψη (Unsupervised learning), ο αλγόριθμος κατασκευάζει ένα μοντέλο για κάποιο σύνολο εισόδων χωρίς να γνωρίζει επιθυμητές εξόδους για το σύνολο εκπαίδευσης.[111]

Τα περισσότερα Εργαλεία Αποτροπής Απώλειας Δεδομένων χρησιμοποιούν και τους δυο τύπους αλγορίθμων.

Τα Εργαλεία Αποτροπής Απώλειας Δεδομένων τα οποία χρησιμοποιούν Αλγορίθμους Μηχανικής Μάθησης δουλεύουν με τρόπο ανάλογο με αυτόν των συστημάτων φιλτραρίσματος των ανεπιθύμητων μηνυμάτων (filter / block Spam).

Στο παρακάτω σχήμα (Εικόνα: 3.4) αποτυπώνεται ο τρόπος λειτουργίας ενός αλγορίθμου Μηχανικής Μάθησης (Machine Learning Algorithm). Ο Αλγόριθμος Μηχανικής Μάθησης διεξάγεται σε δύο φάσεις. Τη φάση της εκπαίδευσης (**Training**) και τη φάση της εντόπισης (**Detection**). Κατά την διάρκεια της Εκπαίδευσης εξάγονται χαρακτηριστικά γνωρίσματα (Feature Extraction), προκειμένου να δημιουργηθεί ένα Προφίλ (Profile). Η εκπαίδευση βασίζεται στην κατηγορία των δεδομένων που πρέπει να προστατεύουμε .

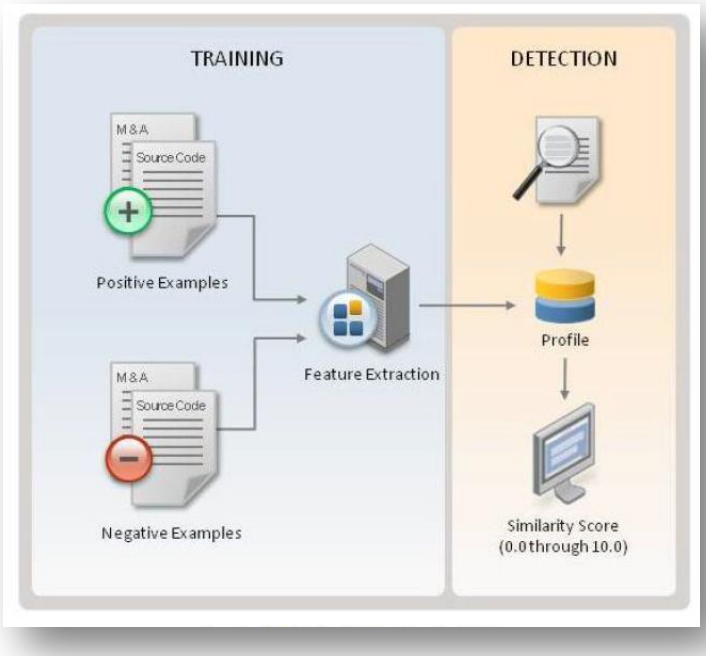
Πιο συγκεκριμένα, κατά την διάρκεια της εκπαίδευσης προβάλλονται Θετικά (Positive) και Αρνητικά (Negative) παραδείγματα. Και τα δυο σύνολα είναι απαραίτητα για να εξάγουμε το κατάλληλο Προφίλ (Profile). Μπορούν οι Διαχειριστές του Συστήματος να «ανεβάσουν» (uploading) θετικά (positive) και αρνητικά (negative) παραδείγματα αρχείων για την δημιουργία του Προφίλ (Profile). Ο αλγόριθμος χρησιμοποίει τα θετικά και αρνητικά παραδείγματα για να κτίσει το δικό του προφίλ.

Κατά την διάρκεια της εντόπισης (Detection) χρησιμοποιείται το προφίλ που δημιουργήθηκε έτσι ώστε να γίνει κατηγοριοποίηση των δεδομένων που εντοπίζονται.

Εάν τα δεδομένα είναι όμοια με τα Θετικά Παραδείγματα τότε παράγεται ένα ειδοποιητικό μήνυμα (Incident).

Κατά την διάρκεια της εντόπισης προσθέτεται ένας βαθμός ομοιότητας (Similarity Score) στα αρχεία που κατηγοριοποιήθηκαν. Ο βαθμός ομοιότητας δέκα δηλώνει πως τα δεδομένα είναι ακριβώς ίδια με αυτά που δόθηκαν στα παραδείγματα κατά την διάρκεια της εκπαίδευσης. Ενώ ένας βαθμός μηδέν δηλώνει ότι δεν μοιάζουν καθόλου τα δεδομένα με αυτά της εκπαίδευσης.

Στην περίπτωση που κάποια δεδομένα δεν μοιάζουν με αυτά που χρησιμοποιήθηκαν στην εκπαίδευση μας, τότε αυτά είναι Ψευδώς Θετικά (False Positive). Τα Ψευδώς Θετικά μπορούν να χρησιμοποιηθούν για Ανατροφοδότηση (Feedback) του Συνόλου Εκπαίδευσης έτσι ώστε με την πάροδο του χρόνου το προφίλ να τελειοποιηθεί.



Εικόνα3.4:Πως δουλεύει ο Αλγόριθμος Μηχανικής Μάθησης.[082]

Το κυρίως πρόβλημα των συστημάτων Αποτροπής Απώλειας Δεδομένων τα οποία χρησιμοποιούν αλγόριθμους μηχανικής μάθησης είναι το γεγονός πως μπορούν να φιλτράρουν

μόνο αρχεία κειμένου (text documents) και μπορεί να δώσουν ψηλό ποσοστό από Ψευδώς Θετικά και ψευδώς αρνητικά αποτελέσματα εάν τα συστήματα δεν εκπαιδευτούν καταλλήλως.

Επιπλέον κατά την διάρκεια της εκπαίδευσης προβάλλονται διάφορες γλώσσες με τις οποίες μπορεί ο αλγόριθμος να εντοπίσει εμπιστευτικά δεδομένα. Στην περίπτωση όμως που κάποια γλώσσα δεν συμπεριληφθεί στην εκπαίδευση τότε είναι δύσκολο να εντοπίσει τα εμπιστευτικά δεδομένα που υπάρχουν δημιουργημένα στην γλώσσα αυτή. [026, 042, 058, 069, 075, 082, 088, 107, 111]

Οι επτά τεχνικές ανίχνευσης ευαίσθητων πληροφοριών συμπεριλαμβάνονται στα περισσότερα προϊόντα Αποτροπής Απώλειας Δεδομένων στην αγορά. Δεν συμπεριλαμβάνουν όλα τα προϊόντα όλες τις τεχνικές, όμως μπορούν να χρησιμοποιούν συνδυασμούς από τεχνικές για την ανάλυση των δεδομένων με αποτέλεσμα την Αποτροπή Απώλειας εμπιστευτικών πληροφοριών.

Κεφάλαιο 4
Σύγχρονες Τεχνολογίες Αποτροπής Απώλειας Δεδομένων

Στην αγορά σήμερα υπάρχουν διάφορες τεχνολογίες Αποτροπής Απώλειας Δεδομένων που είτε προσφέρουν ένα ολοκληρωμένο πακέτο προστασίας των δεδομένων που βρίσκονται σε αδράνεια (Data at Rest- DAR), σε κίνηση (Data in Motion-DIM) και σε καταληκτικό σημείο (Data at the Endpoint-DAE), είτε προσφέρουν ένα περιορισμένο πακέτο σε μια από τις τρεις περιοχές.

Το καταλληλότερο εργαλείο Αποτροπής Απώλειας Δεδομένων για ένα οργανισμό πρέπει να προσαρμόζεται ανάλογα με τις απαιτήσεις και το εύρος των εργασιών του οργανισμού. Συνεπώς μπορεί να ειπωθεί ότι ένα εργαλείο Αποτροπής Απώλειας Δεδομένων με συγκεκριμένες, όχι πολλές, δυνατότητες μπορεί να είναι το κατάλληλο για ένα μικρό οργανισμό και, αντίστοιχα, ένα ισχυρό εργαλείο Αποτροπής Απώλειας Δεδομένων να είναι κατάλληλο για ένα μεγάλης εμβέλειας οργανισμό. Το αντίθετο όμως θα μπορούσε να ήταν καταστροφικό.

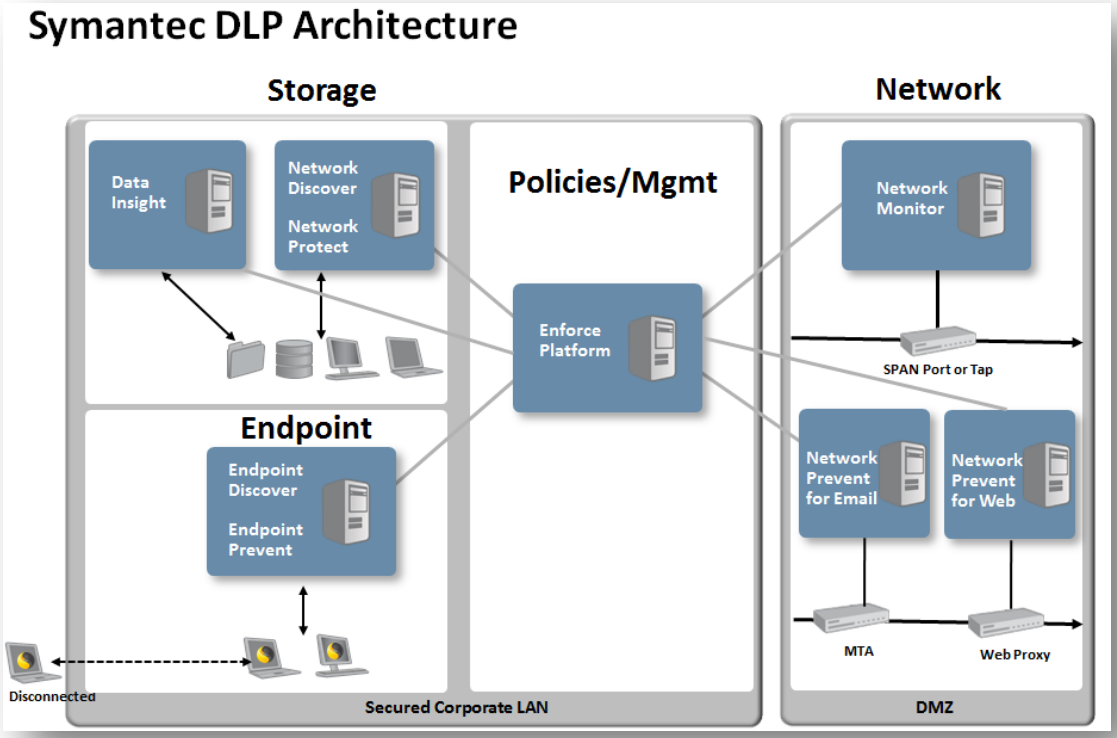
Σύμφωνα με την Αμερικανική εταιρεία Gartner (η οποία ασχολείται με την έρευνα σε θέματα τεχνολογιών πληροφορικής και έχει ένα συμβουλευτικό ρόλο στις εταιρείες και στους οργανισμούς στην αγορά), η εταιρεία Symantec κατατάσσεται ως ο κορυφαίος Ηγέτης (Leader) στην αγορά Εργαλείων Αποτροπής Απώλειας Δεδομένων. Η έρευνα έχει γίνει το Δεκέμβριο του 2013. Μεταξύ άλλων στις ηγετικές θέσεις (**Leaders**) συνυπάρχουν οι εταιρείες Symantec, EMC (RSA), McAfee, Verdasys και Websense. Στην θέση των διεκδικητών **(Challengers)** βρίσκονται οι εταιρείες Trustwave και CA Technologies. Στη θέση των εξειδικευμένων παικτών (**Niche Players)** βρίσκονται οι εταιρείες Code Green Networks, Absolute Software, InfoWatch και Zecurion. Και στη θέση των Οραματιστών **(Visionaries)** βρίσκονται General Dynamics Fidelis Cybersecurity Solutions και GTB Technologies. όπου θα γίνει μια σύντομη περιγραφή τους στο κεφάλαιο αυτό. [070]

Εικόνα 4.1: Magic Quadrant for Content-Aware Data Loss Prevention 12 December 2013.[070]

Στις θέσεις που χαρακτηρίζονται ως ηγετικές (leaders) περιλαμβάνονται οι τεχνολογικές λύσεις των εταιρειών Symantec, MacAfee, EMC (RSA), Verdasys και Websense.

4.1 Symantec

Το εργαλείο Symantec Data Loss Prevention είναι μια ολοκληρωμένη λύση περί ασφάλειας δεδομένων (Data Security Solution) η οποία ανακαλύπτει (Discovers), παρακολουθεί (Monitors), διαχειρίζεται (Manages) και προστατεύει (Protects) εμπιστευτικά και ευαίσθητα δεδομένα τα οποία είναι αποθηκευμένα (Stored) ή χρησιμοποιούνται (Used). Το εργαλείο Symantec Data Loss Prevention συμμορφώνεται με την παγκόσμια νομοθεσία περί προστασίας προσωπικών δεδομένων και επιτρέπει ταυτόχρονα στους οργανισμούς να διασφαλίζουν την φήμη και την αξιοπιστία τους. [001, 082-086]



Εικόνα4.2: Symantec DLP Αρχιτεκτονική.[083]

4.1.1 Αρχιτεκτονική

Η Αρχιτεκτονική του Εργαλείου DLP της εταιρείας Symantec περιλαμβάνει τα παρακάτω προϊόντα:

- **Symantec DLP Enforce Platform**. Είναι η κεντρική πλατφόρμα στην όποια γίνεται διαχείριση της ροής των εργασιών, των πολιτικών (Policies) και γίνεται προβολή εκθέσεων/αναφορών (Reports).

- **Symantec DLP for Network**. παρακολουθεί και αποτρέπει την απώλεια ευαίσθητων πληροφοριών μέσω ηλεκτρονικού ταχυδρομικού (Email) και μέσω ιστού (Web).

- **Symantec DLP for Storage** σαρώνει τα δεδομένα σε αδράνεια όπως κοινόχρηστα αρχεία (Share Files), Διακομιστές Ιστού (Web Servers), Βάσεις Δεδομένων (Database).

- **Symantec DLP for Endpoint** σαρώνει και ανακαλύπτει ευαίσθητα και εμπιστευτικά δεδομένα που βρίσκονται σε αδράνεια (at Rest) και δεδομένα που χρησιμοποιούνται (in Use) σε τελικό σημείο (Endpoint)

- **Symantec DLP for Mobile** παρακολουθεί το δίκτυο και γίνεται αποτροπή κυκλοφορίας ευαίσθητης πληροφορίας μέσω ηλεκτρονικού ταχυδρομείου (email), ιστού (web) και εφαρμογών (Applications) σε IPads και IPhones. [001, 082-086]

4.1.2 Χρησιμοποιούμενες μέθοδοι

Η σουίτα της εταιρείας Symantec για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: Αποτύπωμα δεδομένων (data fingerprinting), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching), αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), Χαρακτηριστικά των αρχείων (file attribute), ανάλυση βάσει εννοιών (conceptual/Lexicon analysis) και Αλγόριθμοι Μηχανικής Μάθησης (Machine learning Algorithm).[001, 022, 082-086]

4.2 Websense

Η εταιρεία Websense προσφέρει την τεχνολογική λύση με ονομασία Websense Data Security Suite DLP (DSS). Η συγκεκριμένη σουίτα εργαλείων προσφέρει προστασία και στις τρεις περιοχές (δεδομένα σε κίνηση, δεδομένα σε αδράνεια και δεδομένα που χρησιμοποιούνται). Προσφέρει προστασία σε πύλες δικτύου (Gateways), τερματικά (endpoints), ηλεκτρονικό ταχυδρομείο (web email), δεδομένα στο νέφος (data cloud). [001, 104-107]

4.2.1 Αρχιτεκτονική

Η τεχνολογική λύση Websense Data Security Suite DLP (DSS) περιλαμβάνει τα παρακάτω προϊόντα:

- **Websense Data Security Gateway:** Παρακολουθεί τα κοινά κανάλια επικοινωνίας δικτύου (common network communications channels), όπως για παράδειγμα τον ιστό (web) και το ηλεκτρονικό ταχυδρομείο (email), το πρωτόκολλο μεταφοράς αρχείων (FTP File Transfer Protocol), συνδέσεις ActiveSync για κινητές συσκευές (κινητό ηλεκτρονικό ταχυδρομείο) και άλλα. Όταν εντοπιστούν κρίσιμα δεδομένα, το προϊόν εμποδίζει τη διαβίβασή του, καταγράφονται τα συμβάντα αυτόματα και εκτελείται μια ενέργεια αποκατάστασης τους.

- **Websense Data Endpoint:** Παρακολουθεί την κίνηση σε πραγματικό χρόνο και ελέγχει πού μπορούν να μετακινηθούν τα εμπιστευτικά δεδομένα, ποιος τα χρησιμοποιεί, και ποιες ενέργειες γίνονται σε πραγματικό χρόνο έτσι ώστε να γίνει η πρόληψη της απώλειας των δεδομένων στο τελικό σημείο (Endpoint).

- **Websense Data Discovery:** Προσδιορίζει με ακρίβεια τα εμπιστευτικά δεδομένα με τη χρήση της μηχανής εντοπισμού και κατηγοριοποίησης δεδομένων της εταιρείας Websense (Data identification and Classification engine), που αποτελείται από το σύνολο τριών περιοχών κατηγοροποιητών δεδομένων (data classifiers) (περιγραφική described, καταχωρημένα registered και εκπαιδευμένα learned). [001, 104-107]

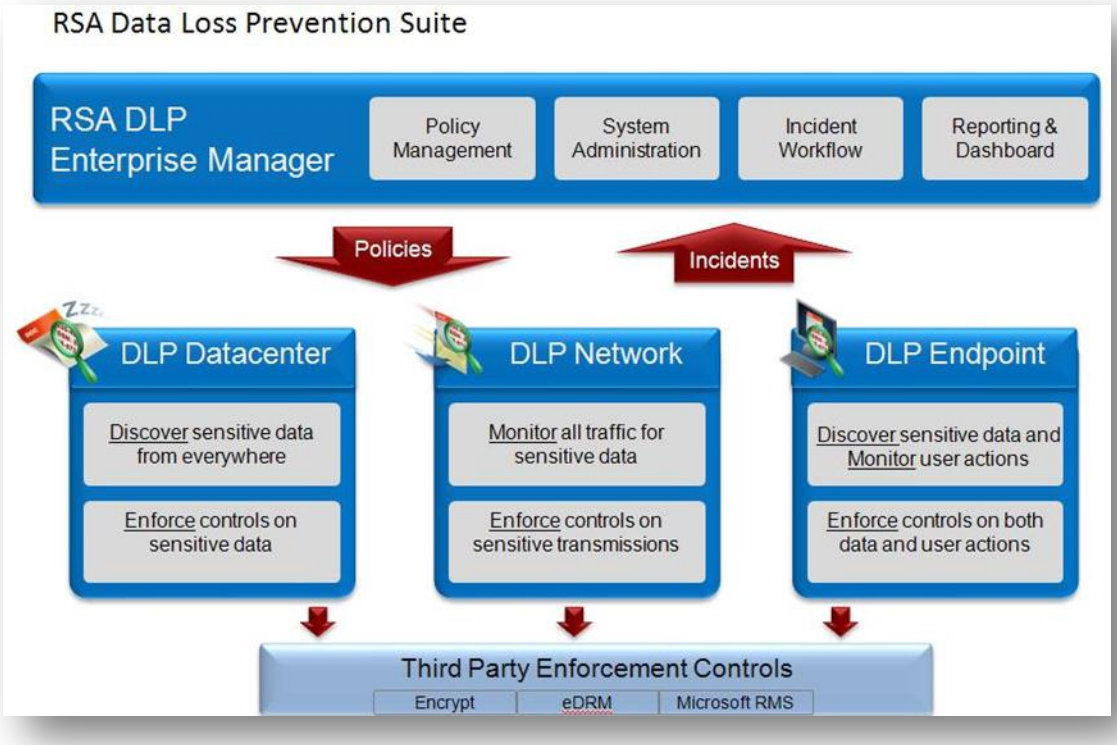
4.2.2 Χρησιμοποιούμενες μέθοδοι

Η τεχνολογική λύση Websense DLP tools για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), Αποτύπωμα δεδομένων (Data Fingerprinting), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching), Χαρακτηριστικά των αρχείων (file attribute), ανάλυση βάσει εννοιών (Conceptual/Lexicon analysis), Κατηγορίες (Categories) και Αλγόριθμοι Μηχανικής Μάθησης (Machine Learning Algorithm). [001, 022, 104-107]

4.3 EMC RSA

Η εταιρεία EMC προσφέρει την τεχνολογική λύση RSA Data Loss Prevention Suite. Η τεχνολογική λύση βοηθά τους οργανισμούς να αντιμετωπίσουν τις προκλήσεις της εξασφάλισης των δεδομένων σε κατάσταση ηρεμίας (Data at Rest), σε κίνηση (Data in Motion) και κατά τη χρήση (Data in Use). [001, 071-074]

4.3.1 Αρχιτεκτονική



Εικόνα 3.3: RSA DLP Αρχιτεκτονική. [071]

Η τεχνολογική λύση RSA Data Loss Prevention Suite περιλαμβάνει τα παρακάτω προϊόντα:

- **RSA DLP Network**: Είναι μια συσκευή δικτύου βασισμένη σε Linux, η οποία παρακολουθεί (monitor) όλη την κίνηση (monitor) των εμπιστευτικών και ευαίσθητων δεδομένων.

- **RSA DLP Endpoint**: Είναι λογισμικό πράκτορας (software agent) για windows το οποίο ανακαλύπτει εμπιστευτικά και ευαίσθητα δεδομένα και παρακολουθεί τις ενέργειες των χρηστών.

- **RSA DLP Data center**: Είναι Windows software crawling agents, grid-based software ή agentless scanning software τα οποία ανακαλύπτουν εμπιστευτικά και ευαίσθητα δεδομένα από παντού.

- **RSA DLP Enterprise Manager**: είναι μια εφαρμογή ιστού (Web Application) με την οποίαν ο Διαχειριστής (Administrator) ρυθμίζει και διαχειρίζεται τα πιο πάνω προϊόντα DLP. [001, 071-074]

4.3.2 Χρησιμοποιούμενες μέθοδοι

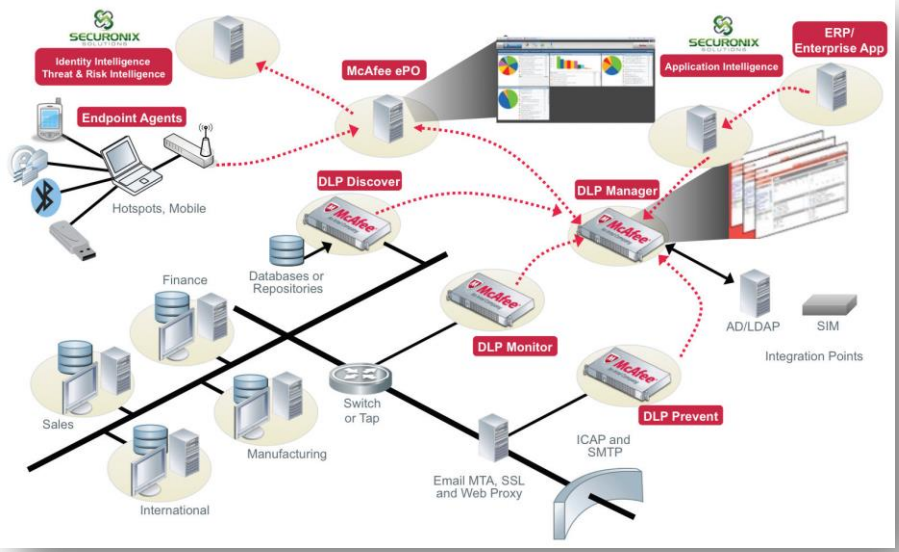
Η σουίτα της εταιρείας RSA για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: Αποτύπωμα δεδομένων (data fingerprinting), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching), Κατηγορίες (Categories), αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), Χαρακτηριστικά των αρχείων (file attribute) και ανάλυση βάσει εννοιών (conceptual/Lexicon analysis). [001, 022, 071-074]

4.4 McAfee

Η τεχνολογική λύση της εταιρείας McAfee Data Loss Prevention προστατεύει ευαίσθητα και εμπιστευτικά δεδομένα που είναι σε κίνηση, σε αδράνεια ή χρησιμοποιούνται. Αποτρέπει την απώλεια δεδομένων μέσω USB, mp3 players, CD, DVD, φορητά αποθηκευτικά μέσα, φορητούς υπολογιστές (Laptops), διακομιστές αρχείων (file servers) καθώς και αποθηκευτικά μέσα νέφους (cloud).[001, 059]

4.4.1 Αρχιτεκτονική

Η τεχνολογική λύση McAfee Data Loss Prevention Suite περιλαμβάνει τα παρακάτω προϊόντα:



Εικόνα 4.4: McAfee DLP Αρχιτεκτονική.[059]

- **McAfee DLP Monitor:** επιτρέπει την εύρεση, παρακολούθηση, καθώς και την προστασία των κρίσιμων πληροφοριών από οποιοδήποτε εφαρμογή (application) ή τοποθεσία (location) σε οποιοδήποτε μορφή (format), σε οποιοδήποτε πρωτόκολλο (protocol) ή θύρα (port).

- **McAfee DLP Discover**: βρίσκει εμπιστευτικές και ευαίσθητες πληροφορίες ακόμη και αν η τοποθεσία είναι άγνωστη. Χρησιμοποιεί προηγμένη τεχνολογία σάρωσης δικτύου και εκτελεί προγραμματισμένες σαρώσεις.

- **McAfee DLP Prevent:** βοηθά να εφαρμοστούν πολιτικές ασφαλείας για τις πληροφορίες που φεύγουν έξω από τα όρια του δικτύου (boundaries of your network). Εφαρμόζει τις τεχνολογίες ασφαλείας για ηλεκτρονικό ταχυδρομείο (email), ιστό (web), άμεσα μηνύματα (IM) και άλλες εφαρμογές δικτύου (Network Applications).

- **McAfee DLP Endpoint:** προσφέρει προστασία κατά της κλοπής (theft) και τυχαίας αποκάλυψης των εμπιστευτικών δεδομένων. Η προστασία λειτουργεί σε όλα τα δίκτυα, μέσω των εφαρμογών, καθώς και μέσω αφαιρούμενων συσκευών αποθήκευσης (removable storage devices).

- **McAfee DLP Manager:** παρέχει εντατικοποιημένο έλεγχο για τα υπόλοιπα DLP προϊόντα.

- **McAfee ePO:** είναι πλατφόρμα για κεντρική διαχείριση και έχει την ικανότητα υποβολής εκθέσεων (report).[001, 059]

4.4.2 Χρησιμοποιούμενες Μέθοδοι

Η σουίτα της εταιρείας McAfee για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: Αποτύπωμα δεδομένων (data fingerprinting), αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching). Τα ψευδώς θετικά (False Positives) ελαχιστοποιούνται μέσω αλγόριθμων επικύρωσης (validation algorithms), εξαιρέσεων (exceptions) και τον κανόνα συντονισμού (rule tuning) από καταγεγραμμένα δεδομένα.[001, 022, 059]

4.5 Verdasys

Η τεχνολογική λύση της εταιρείας Verdasys προσφέρει το προϊόν με ονομασία Digital Guardian. Το εργαλείο αποτροπής απώλειας δεδομένων Digital Guardian είναι μια τεχνολογική λύση για προστασία των δεδομένων που βρίσκονται στο τελικό σημείο (endpoint). Η εταιρεία περιγράφει το προϊόν της ως να παρέχει πλήρη προστασία δια το λόγο ότι συνδυάζει το τελικό σημείο (endpoint), τους διακομιστές (servers) και το DLP δικτύου (Network DLP) με δυνατότητες ανεύρεσης δεδομένων σε αδράνεια (Data at Rest), σήμανσης δεδομένων (Data tagging), προστασίας της ηλεκτρονικής αλληλογραφίας(email protection), προστασίας των αρχείων (File protection), προστασίας της κίνησης των δεδομένων στο δίκτυο, έλεγχο των αφαιρούμενων συσκευών (removable media), κρυπτογράφηση (encryption), ανίχνευση και άμυνα από κακόβουλο λογισμικό (Malware) (όλα βασισμένα σε τελικό σημείο).

Η εταιρεία συνεργάζεται με τη Fidelis XPS που τώρα ανήκει στην General Dynamics οι οποίες προσφέρουν ένα ενιαίο περιβάλλον εργασίας το οποίο προσφέρει προστασία στο δίκτυο και στο τελικό σημείο.[099-102]

4.5.1 Αρχιτεκτονική

Η τεχνολογική λύση Digital Guardian προσφέρει τα παρακάτω προϊόντα.

- **Verdasys Host agents:** είναι πράκτορες όπου σαρώνουν υπολογιστές και διακομιστές σε περιβάλλον Windows και Linux.

- **Verdasys Discovery:** Σάρωση από τον πράκτορα eDiscovery ή εικονική συσκευή (SUSE)

- **Digital Guardian management Console (windows server)**: Παρέχει τη διαχείριση για τα άλλα DLP προϊόντα.

DLP Network: (χτίστηκε από Fidelis, που τώρα ανήκει στην General Dynamics) είναι ενσωματωμένος με την πλευρά του τελικού σημείου και μπορεί να πωληθεί και να χρησιμοποιηθεί, επίσης από την Verdasys. [022, 099-102]

4.5.2 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση Verdasys DLP tools για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: η αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching), η αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), το Αποτύπωμα δεδομένων (data fingerprinting) και τα Χαρακτηριστικά των αρχείων (file attribute).[099-102]

Στις θέσεις των challengers περιλαμβάνονται οι τεχνολογικές λύσεις των εταιρειών CA Technologies, Trustwave.

4.6 CA Technologies

Η τεχνολογική λύση της εταιρείας CA Technologies με ονομασία CA DataMinder επιτρέπει στους οργανισμούς να ελέγχουν τις πληροφορίες οι οποίες χρησιμοποιούνται (In use), είναι σε κίνηση (in motion), σε αδράνεια (at rest) και σε πρόσβαση (at access). Η λύση CA DataMinder παρέχει αυτές τις δυνατότητες μέσων των προϊόντων CA DataMinder Endpoint, CA DataMinder Network, CA DataMinder Email, CA DataMinder Stored Data τα οποία προϊόντα ενσωματώνονται μέσω του προϊόντος CA Identity & Access Management. [011-016]

4.6.1 Αρχιτεκτονική

- **Ca DataMinder Management Platform:** Παρέχει μια κεντρική διαχείριση των προϊόντων μέσα από ένα εκτελεστικό ταμπλό (dashboard). Με την Ca DataMinder Management Platform εκτελείτε λεπτομερή προσαρμογή των εκθέσεων.

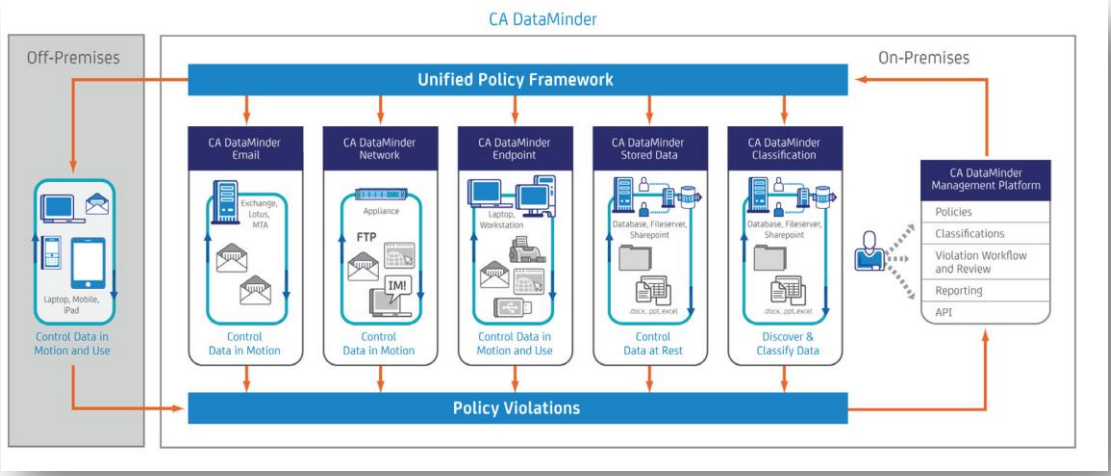
- **Ca DataMinder Email:** Ελέγχει και δίνει αναφορές σχετικά με ηλεκτρονική αλληλογραφία που είναι σε κίνηση ή σε αδράνεια.

- **CA DataMinder Network:** Προστατεύει και ελέγχει δεδομένα σε κίνηση.

- **CA DataMinder Endpoint:** Προστατεύει και ελέγχει δεδομένα που χρησιμοποιούνται.

- **CA DataMinder Stored Data:** Προσφέρει προστασία και έλεγχο των πληροφοριών οι οποίες αποθηκεύονται σε κοινόχρηστους φάκελους (share folders), αρχεία και έγγραφα αποθετήρια (file and document repositories), δημοσίους φακέλους (public folders), ODBC πηγές και άλλα εργαλεία συνεργασίας, όπως Microsoft SharePoint. Μέσα από προκαθορισμένες αλλά και διαμορφώσιμες πολιτικές (policies) ο CA DataMinder Stored Data μπορεί να εντοπίζει, να κατηγοριοποιεί και να ελέγχει εμπιστευτικές πληροφορίες ελαχιστοποιώντας έτσι το ρίσκο κινδύνου της επιχείρησης.

- **CA DataMinder Classification:** Ανακαλύπτει και κατηγοριοποιεί ευαίσθητο δομημένο και μη δομημένο περιεχόμενο που είναι αποθηκευμένο σε διακομιστές αρχείων (file servers), βάσεις δεδομένων (databases), εργαλεία συνεργασίας (collaboration tools) και αποθετήρια αποθήκευσης (storage repositories). [011-016]



Εικόνα 4.5: CA DataMinder DLP Αρχιτεκτονική.[013]

4.6.2 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση CA DataMinder για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: Αποτύπωμα δεδομένων (data fingerprinting). [011-016]

4.7 Trustwave

Η τεχνολογική λύση Trustwave Data Loss Prevention (DLP) Solution είναι λύση έλεγχου του περιεχομένου και σχεδιάστηκε για την παρακολούθηση και αποτροπή της απώλειας των δεδομένων που κυκλοφορούν στο δίκτυο.

Είναι σχεδιασμένο για οργανισμούς από όλους τους κλάδους με απώτερο σκοπό την διασφάλιση της πνευματικής ιδιοκτησίας και των δεδομένων είτε αυτά είναι των πελατών είτε του οργανισμού τα οποία είναι σε κίνηση (data in motion), σε κατάσταση ηρεμίας (data at rest) και κατά την χρήση τους (data in use). [090-095]

4.7.1 Αρχιτεκτονική

- **Trustwave DLP Discover:** Ερευνά τα δεδομένα σε αδράνεια (data at rest) για να εντοπίσει και να προστατεύσει ευαίσθητες πληροφορίες που εμπεριέχονται σε αποθηκευμένα δεδομένα χρησιμοποιώντας μεθόδους ανίχνευσης (detection) και κατηγοριοποίησης (Classification).

- **Trustwave DLP Monitor:** Αναλύει όλες τις επικοινωνίες που βασίζονται στο διαδίκτυο, συμπεριλαμβανομένων των συνημμένων του ηλεκτρονικού ταχυδρομείου (email), άμεσα μηνύματα (IM), ανταλλαγή αρχείων P2P file sharing, δωμάτια συνομιλίας (chat rooms), ιστολογία (blogs), δημοσιεύσεις ιστού (web postings), Πρωτόκολλο μεταφοράς Αρχείου (FTP) και Telnet.

- **Trustwave DLP Protect:** Αμύνεται έναντι της ακούσιας απώλειας δεδομένων μέσω ηλεκτρονικής αλληλογραφίας (email) και συνημμένων (attachment) αρχείων. [090-095]

4.7.2 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση Trustwave DLP Solution για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), Αποτύπωμα δεδομένων (data fingerprinting), ανάλυση βάσει εννοιών (conceptual/Lexicon analysis), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching) και Αλγόριθμοι Μηχανικής Μάθησης (Machine learning Algorithm). [090-095]

Στις θέσεις των Visionaries περιλαμβάνονται οι τεχνολογικές λύσεις των εταιρειών General Dynamics Fidelis Cybersecurity Solutions και GTB Technologies.

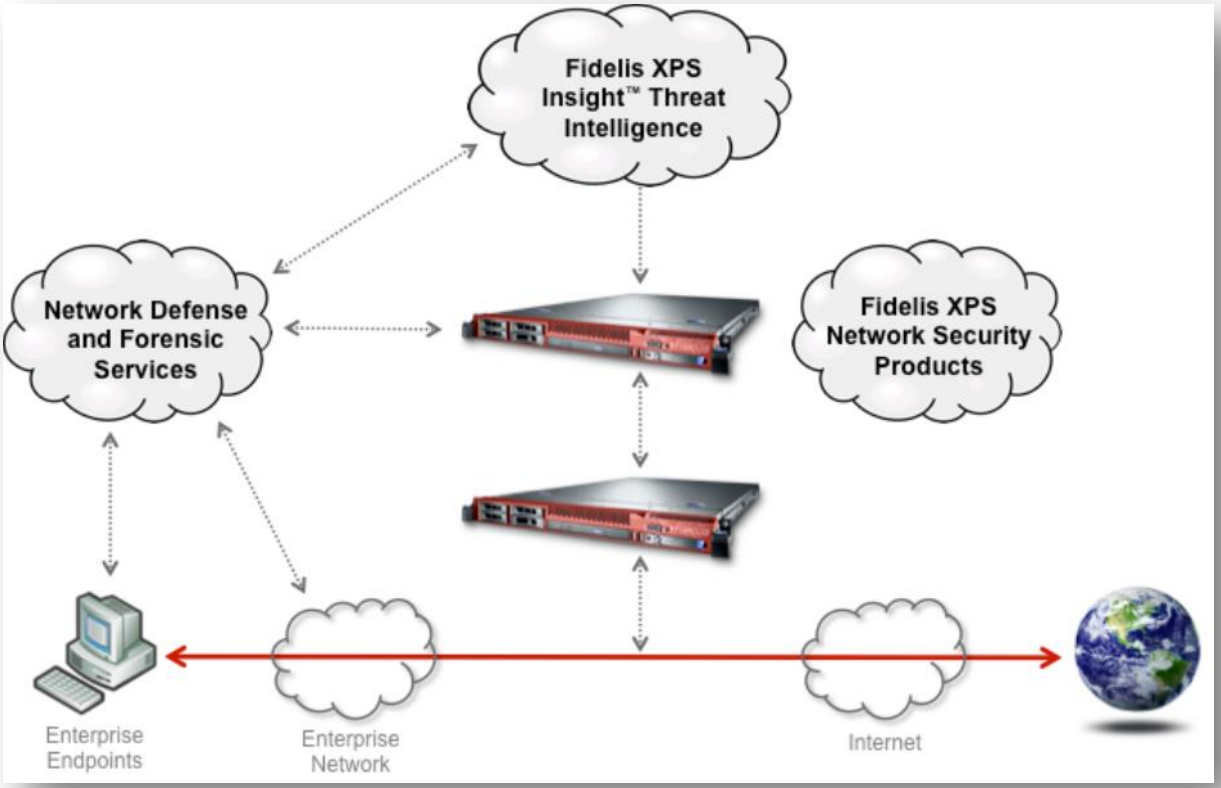
4.8 General Dynamics Fidelis Cybersecurity Solutions

Η General Dynamics Fidelis Cybersecurity Solutions παρέχει στους οργανισμούς ένα ισχυρό, ολοκληρωμένο χαρτοφυλάκιο προϊόντων, υπηρεσιών και τεχνογνωσίας για την καταπολέμηση εξελιγμένων απειλών και την πρόληψη της διαρροής δεδομένων. Επιχειρήσεις και οργανισμοί μπορούν να αντιμετωπίσουν προηγμένες απειλές με την χρήση του προϊόντος Network Defense

and Forensics Services, επιπλέον έχουν το έλεγχο μέσω του βραβευμένου προϊόντος Fidelis XPS™ Advanced Threat Defense Products.[034-038]

4.8.1 Αρχιτεκτονική

Η τεχνολογική λύση της εταιρείας General Dynamics Fidelis Cybersecurity Solutions αποτελείτε από τα παρακάτω προϊόντα:



Εικόνα 4.6: Αρχιτεκτονική της Fidelis XPS.[038]

- **Fidelis XPS Insight Treat Intelligence** είναι προϊόν βασισμένο στην τεχνολογία νέφους (Cloud). Το προϊόν Fidelis XPS Insight Treat Intelligence είναι βασικό στοιχείο της τεχνολογίας. Εντοπίζει αυτόματα ύποπτες και κακόβουλες δραστηριότητες που διεξάγονται στο δίκτυο.

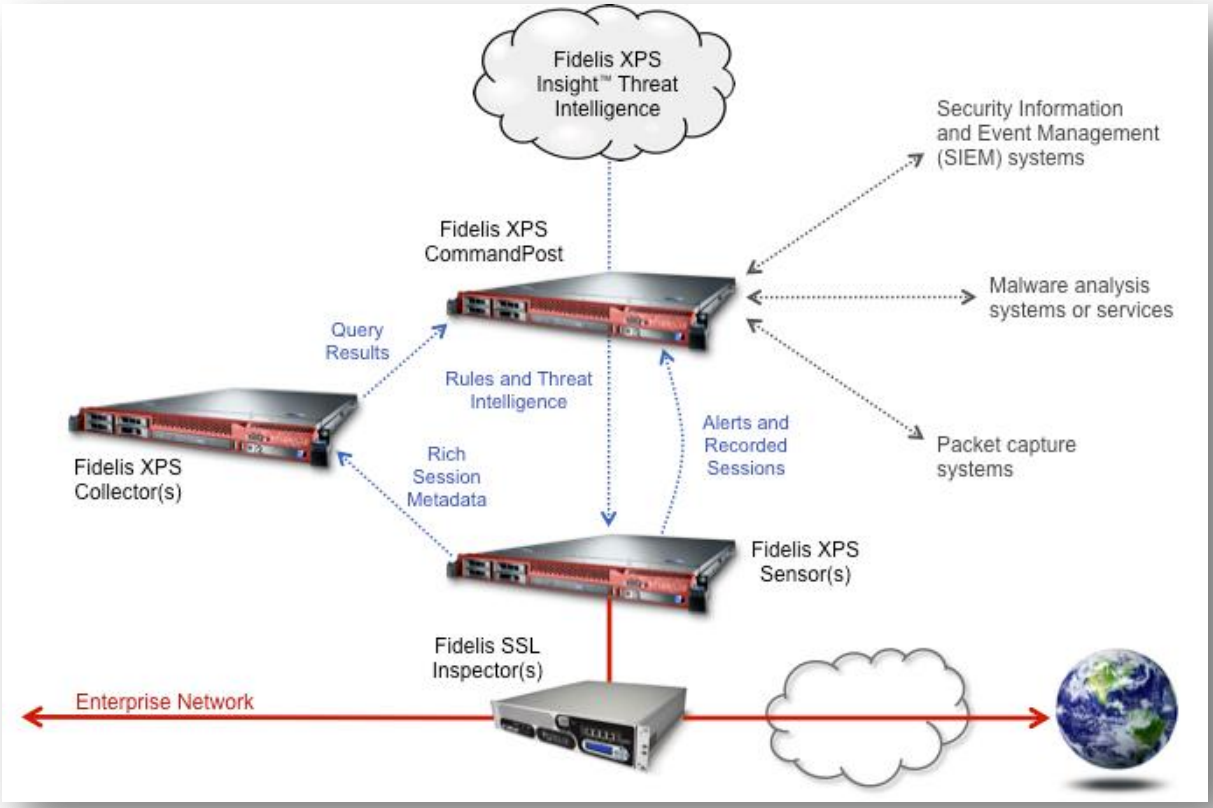
- **Fidelis XPS Network Security Products** όπως διακρίνουμε στο παρακάτω σχήμα η ανάπτυξη της τεχνολογίας περιλαμβάνει το συνδυασμών το πιο κάτω προϊόντων.

- **Fidelis XPS CommandPost (management console):** είναι το σύστημα διαχείρισης του Fidelis XPS Network Security Products.

- **Fidelis XPS Sensors:** συνήθως αναπτύσσονται σε όλα τα σημεία πρόσβασης στο διαδίκτυο, και στα συστήματα ασφαλείας του δικτύου όπως αναχώματα ασφαλείας (firewalls) και συστήματα πρόληψης και ανίχνευσης εισβολής (intrusion detection & prevention systems) τα οποία παρακολουθούν την κίνηση ανάμεσα στο εταιρικό δίκτυο και το διαδίκτυο.

- **Fidelis XPS Collector:** είναι μια βάση δεδομένων όπου συλλέγει τα μετά δεδομένα τα οποία εξάγονται από τις συνόδους δικτύου από τα Fidelis XPS Sensors.

- **Fidelis SSL Inspector:** το προϊόν δίνει την δυνατότητα στην λύση Fidelis XPS ορατότητα στην κρυπτογραφημένη κίνηση του πρωτοκόλλου SSL



Εικόνα 4.7: Fidelis XPS Network Security προϊόντα.[038]

- **Network Defense and Forensic Services:** είναι σχεδιασμένο για να προσφέρει στους οργανισμούς άμυνα από προηγμένες απειλές. [034-038]

4.8.2 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση της εταιρείας General Dynamics Fidelis Cybersecurity Solutions για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching), Αποτύπωμα δεδομένων (data fingerprinting) και Αλγόριθμοι Μηχανικής Μάθησης (Machine learning Algorithm). [034-038]

4.9 GTB Technologies

Η τεχνολογική λύση της εταιρείας GTB Technologies με ονομασία GTB's Complete Extrusion / Data Loss Prevention Platform προσφέρει προστασία από την απώλεια δεδομένων στα δεδομένα εν κίνηση (Data in Motion), δεδομένα κατά την χρήση (Data in Use) και δεδομένα σε αδράνεια (Data at Rest). Επιτρέπει στους οργανισμούς να διασφαλίσουν τα κρίσιμα δεδομένα τους και να επιβάλουν τις πολιτικές ασφαλείας για τα δεδομένα.[041]

4.9.1 Αρχιτεκτονική

Η τεχνολογική λύση GTB's Complete Extrusion / Data Loss Prevention Platform προσφέρει τα παρακάτω προϊόντα.

- **GTB Inspector:** παρακολουθεί, μπλοκάρει κίνηση του δικτύου. Ο GTB Inspector αναλύει και σαρώνει όλα τα επικοινωνιακά κανάλια όπως ηλεκτρονική αλληλογραφία και άμεσα μηνύματα.

- **GTB Endpoint** Protection: σαρώνει τα δεδομένα με κρίσιμο περιεχόμενο πριν να αποθηκευτούν σε καταληκτικά σημεία όπως αφαιρούμενες μνήμες και μπλοκάρει την μην εξουσιοδοτημένη μεταφορά τους.

- **GTB Data at Rest Manager:** σαρώνει τους διακομιστές (Servers) και αναγνωρίζει κρίσιμα δεδομένα τα οποία αποθηκεύονται σε τοποθεσίες οι οποίες δεν επιτρέπεται.[041]

4.9.2 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση GTB's Complete Extrusion / Data Loss Prevention Platform για τον εντοπισμό των ευαίσθητων δεδομένων χρησιμοποιεί διάφορες τεχνικές εντοπισμού όπως είναι: αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching), ανάλυση βάσει εννοιών (conceptual/Lexicon analysis), Αποτύπωμα δεδομένων (data fingerprinting) και αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression matching). [041]

Στις θέσεις των Niche players περιλαμβάνονται οι τεχνολογικές λύσεις των εταιρειών Code Green Networks, Absolute Software, InfoWatch και Zecurion.

4.10 Code Green Networks

Code Green Networks TrueDLP είναι μια ολοκληρωμένη λύση Data Loss Prevention (DLP) που επιτρέπει στις εταιρείες αποτελεσματικά, να παρακολουθούν και να ελέγχουν την διασφάλιση εμπιστευτικών και ευαίσθητων δεδομένων και πληροφοριών, οι οποίες είναι σε κίνηση είτε σε αδράνεια είτε σε τελικό σημείο. [001, 024-025]

4.10.1 Αρχιτεκτονική

- **Code Green Networks Network DLP:** παρέχει το τρόπο για παρακολούθηση και έλεγχο των δικτυακών επικοινωνιών για να αποτρέπουν τις ευαίσθητες πληροφορίες να διαφεύγουν από το δίκτυο.

- **Code Green Networks Discovery DLP:** Εντοπίζει και εξασφαλίζει τα ευαίσθητα δεδομένα σε όλο το δίκτυο.

- **Code Green Networks Endpoint DLP:** παρέχει προστασία από τη απώλεια δεδομένων σε προσωπικούς υπολογιστές, φορητούς υπολογιστές και παρέχει έλεγχο των

ευαίσθητων πληροφοριών που αντιγράφονται σε αφαιρούμενα μέσα ή αποστέλλονται μέσω ασύρματων συνδέσεων.

- **Code Green Networks Centralized Management System:** είναι το προϊόν που χρησιμοποιείται προκειμένου να ενσωματωθούν όλα τα προϊόντα μαζί. Μέσα από αυτό το κεντρικό σύστημα παρέχεται η διαμόρφωση και η συντήρηση των υπόλοιπων προϊόντων. Καθώς επίσης γίνεται η διαχείριση των πολιτικών του οργανισμού και η διαχείριση των αναφορών (reports) σε συμβάντα (events). [001, 024-025]

4.10.2 Χρησιμοποιούμενες Μέθοδοι

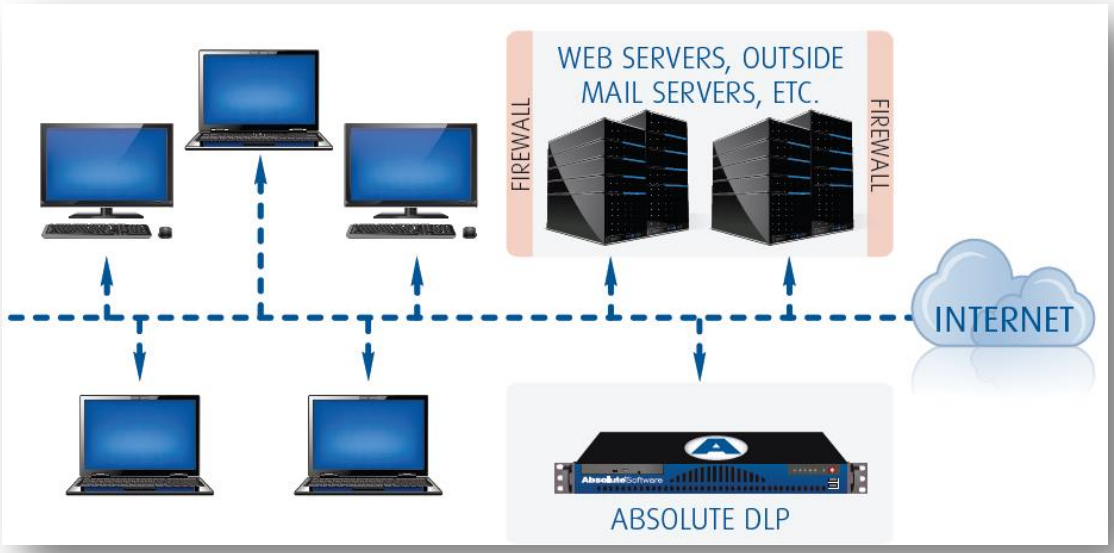
Η τεχνολογική λύση TrueDLP της εταιρείας Code Green Networks για τον εντοπισμών των ευαίσθητων και εμπιστευτικών δεδομένων χρησιμοποίει τεχνικές όπως: Αποτύπωμα δεδομένων (Data Fingerprinting), Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων (Rule και Regular Expression Matching), Ανάλυση Βάσει Εννοιών (Conceptual/Lexicon analysis), Κατηγορίες (Categories) και Αλγόριθμοι Μηχανικής Μάθησης (Machine Learning Algorithm). [001, 024-025]

4.11 Absolute Software

Η τεχνολογική λύση Absolute DLP επιτρέπει στο να παρακολουθείται και να εμποδίζεται η κυκλοφορία ευαίσθητων και εμπιστευτικών αρχείων να φύγουν από το δίκτυο της επιχείρησης σας ή του οργανισμού συμπεριλαμβανομένων των δεδομένων που χρησιμοποιούνται (Data in Use), δεδομένων σε κίνηση (Data in Motion), ή δεδομένων σε αδράνεια (Data at Rest). Παρέχει την δυνατότητα ανάλυσης των δεδομένων που διακινούνται μέσω του δικτύου σε πραγματικό χρόνο και σε όλα τα πρωτόκολλα δικτύου (Web Protocols) συμπεριλαμβανομένου της ηλεκτρονικής αλληλογραφίας (Email), μέσων κοινωνικής δικτύωσης(Social Media), κίνηση ιστού(Web Traffic) και μεταφορά αρχείων(File Transfers). [004-006]

4.11.1 Αρχιτεκτονική

Η τεχνολογική λύση της εταιρείας Absolute παρέχει ένα προϊόν το οποίο περιέχει όλα σε ένα (All in One) δηλαδή περιέχει τα προϊόντα δικτύου(Network), αποθήκευσης (Storage) και τελικού σημείου (Endpoint) σε ένα μηχάνημα. [004-006]



Εικόνα 4.8: Αρχιτεκτονική Absolute DLP.[004]

4.11.2 Χρησιμοποιούμενες Μέθοδοι

Το προϊόν Absolute DLP εκτελεί φιλτράρισμα σε τρία επίπεδα φιλτράρισμα πρωτοκόλλου (Protocol Filtering), φιλτράρισμα ιστού (Web Filtering) και ανάλυση περιεχομένου (Content Analysis). Επιπλέον χρησιμοποίει τεχνικές ανάλυσης περιεχομένου όπως: Αποτύπωμα δεδομένων (Data Fingerprinting), αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule και Regular Expression Matching), ανάλυση βάσει εννοιών (Conceptual/Lexicon Analysis) και Αλγόριθμοι Μηχανικής Μάθησης (Machine Learning Algorithm). [004-006]

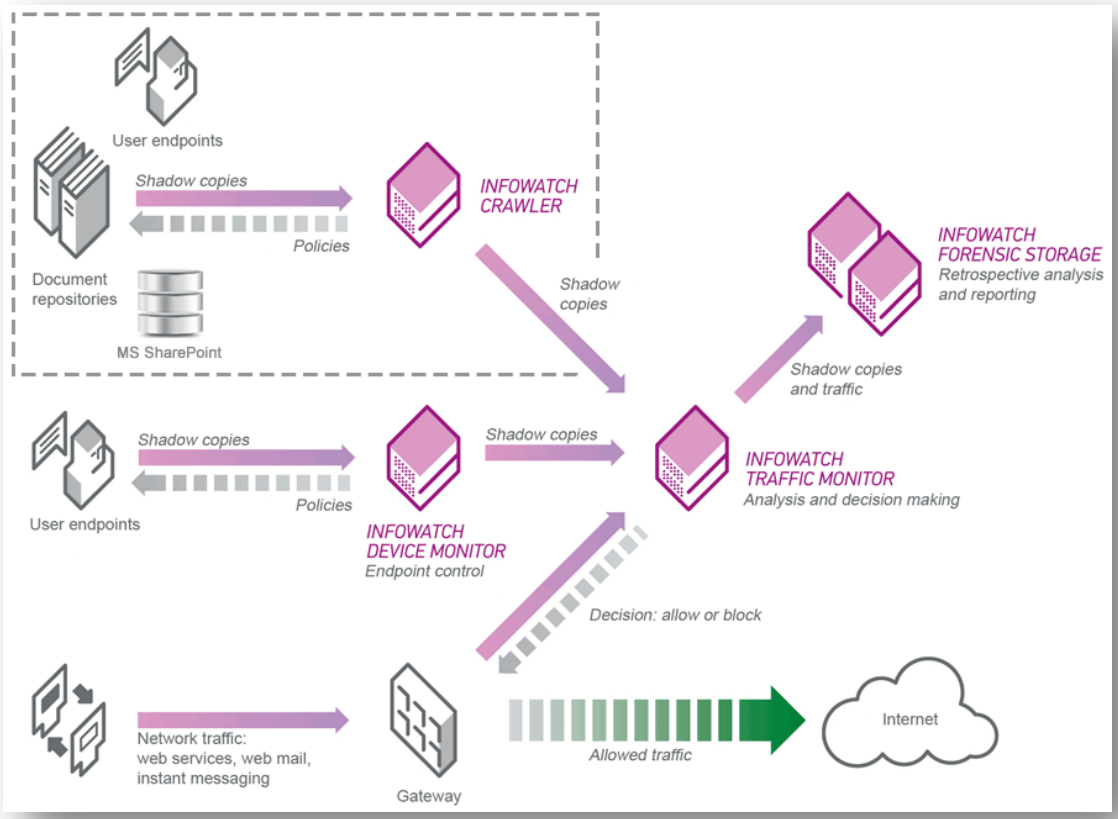
4.12 InfoWatch

Η εταιρεία InfoWatch δημιούργησε μια ολοκληρωμένη λύση για παρακολούθηση της ροής των πληροφοριών, σχεδιασμένη για εταιρείες που επιδιώκουν να προστατεύσουν τα ευαίσθητα δεδομένα τους. Η ολοκληρωμένη αυτή λύση ονομάζεται InfoWatch Traffic Monitor Enterprise. Η λύση αυτή επιτρέπει στις εταιρείες και οργανισμούς να προσδιορίζουν το ποιος χρησιμοποίει ευαίσθητες πληροφορίες, πως τις διαβιβάζει και ποιος έχει πρόσβαση σε αυτές. Το σύστημα αυτόματα ταξινομεί τις πληροφορίες που διαβιβάζονται, αξιολογεί το επίπεδο που προαπαιτείται να προστατεύεται και παρακολουθεί δυναμικά το ρίσκο των ευαίσθητων πληροφοριών που θα διαρρεύσουν.

Η τεχνολογική λύση **InfoWatch Traffic Monitor Enterprise** παρακολουθεί και αναλύει τα δεδομένα τα οποία στέλνονται έξω από το εταιρικό δίκτυο μέσω ηλεκτρονικού ταχυδρομείου (email), μέσω ιστού (web), ή συστήματα ανταλλαγής μηνυμάτων, εκτύπωσης από δικτυακούς και τοπικούς εκτυπωτές ή αντιγραφές αρχείων σε αφαιρούμενα μέσα. Το προϊόν εκτελεί αυτόματη ταξινόμηση των πληροφοριών που μεταδίδονται και επιπλέον γίνεται πρόληψη διαρροής των ευαίσθητων δεδομένων μπλοκάροντας την μεταφορά εάν εντοπιστεί παραβίαση της πολίτικης ασφαλείας. Η τεχνολογική λύση InfoWatch Traffic Monitor Enterprise παρέχει ασφαλή αποθήκευση των δεδομένων για σκοπούς ανάλυσης και έρευνας. [046-047]

4.12.1 Αρχιτεκτονική

Η τεχνολογική λύση της εταιρείας Info Watch αποτελείται από τα παρακάτω προϊόντα:



Εικόνα 4.9: InfoWatch Traffic Monitor Enterprise DLP Αρχιτεκτονική.[046]

1. **InfoWatch Traffic Monitor:** υπεύθυνο για την περιμετρική ασφάλεια του δικτύου.

- **InfoWatch Traffic Monitor for Web:** παρακολουθεί δεδομένα τα οποία μεταφέρονται μέσω webmail, ιστολογία (blogs), φόρουμ (forums) και άλλες ιστοσελίδες διαδικτύου(internet sites).

- **InfoWatch Traffic Monitor for HTTPS:** παρακολουθεί τα δεδομένα που μεταφέρονται μέσω του κρυπτογραφημένου πρωτόκολλου του διαδικτύου HTTPS.

- **InfoWatch Traffic Monitor for Mail:** παρακολουθεί τις πληροφορίες που στέλνονται μέσω του εταιρικού ηλεκτρονικού ταχυδρομείου.

- **InfoWatch Traffic Monitor for IM:** παρακολουθεί συστήματα ανταλλαγής μηνυμάτων άμεσης αποστολής (instant messaging systems) συμπεριλαμβανομένων της παρακολούθησης των αρχείων και SMS (Υπηρεσία Σύντομων Μηνυμάτων short Message Service).

2. **InfoWatch Device Monitor:** προστατεύει τους σταθμούς εργασίας (Workstation).

- **InfoWatch Device Monitor for Devices:** παρακολουθεί την πρόσβαση και την αντιγραφή των πληροφοριών στις αφαιρούμενες συσκευές (removable media) (including flash drives, CD/DVD). Παρακολουθεί τις συσκευές που συνδέονται στις θήρες (ports) COM, LPT και USB.

- **InfoWatch Device Monitor for Print:** παρακολουθεί την εκτύπωση αρχείων μέσω δικτυακών και τοπικών εκτυπωτών.

- **InfoWatch Device Monitor for Skype** παρακολουθεί τα άμεσα μηνύματα, την κίνηση φωνής, την μεταφορά αρχείων και γραπτών μηνυμάτων (SMS) μέσω Skype.

- **InfoWatch Device Monitor for XMPP:** παρακολουθεί τα άμεσα μηνύματα, την κίνηση φωνής, την μεταφορά αρχείων και γραπτών μηνυμάτων (SMS) μέσω XMPP (GTalk, QIP).

- **InfoWatch Device Monitor for Mail.ru Agent:** παρακολουθεί τα άμεσα μηνύματα, την κίνηση φωνής, την μεταφορά αρχείων και γραπτών μηνυμάτων (SMS) μέσω Mail.ru Agent.

- **InfoWatch Device Monitor for FTP:** παρακολουθεί την μεταφορά δεδομένων μέσω του πρωτοκόλλου μεταφοράς αρχείων FTP (File Transfer Protocol).

- **InfoWatch Device Monitor for Network:** παρακολουθεί τις συνδέσεις δικτύου, εξασφαλίζει ότι οι συνδέσεις (connections) γίνονται μόνο σε επιτρεπτά δίκτυα.

3. **InfoWatch Crawler:** είναι προϊόν που παρέχει παρακολούθηση των πληροφοριών, οι οποίες βρίσκονται σε αποθήκες δεδομένων του δικτύου (corporate network data repositories) και συστήματα διαχείρισης εγγράφων (document management systems).

Το προϊόν σαρώνει και εφαρμόζει πολιτικές στα δεδομένα που βρίσκονται σε αδράνεια (at rest).

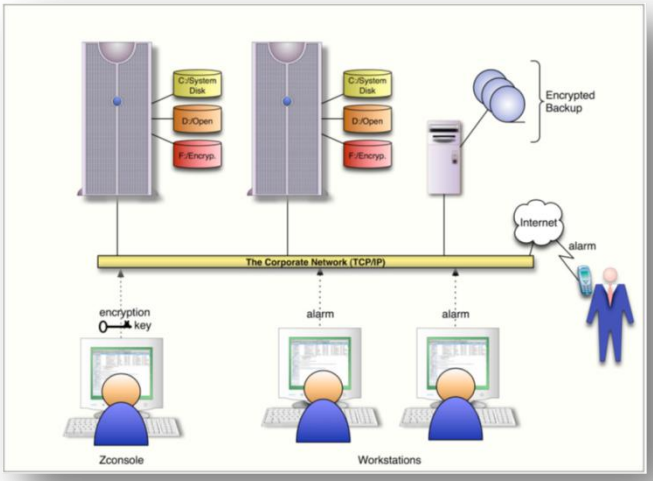
4. **InfoWatch Forensic Storage:** σε αυτό το προϊόν γίνεται μια κεντρικοποιημένη αρχειοθέτηση όλων των πληροφοριών που έχουν υποκλαπεί με σκοπό την περαιτέρω διερεύνηση των παραβάσεων (breaches) και για προετοιμασία των αναλυτικών εκθέσεων. [046-047]

4.12.1 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση InfoWatch Traffic Monitor Enterprise παρέχει ένα έξυπνο σύστημα ανάλυσης περιεχομένου το οποίο συνδυάζει διάφορές τεχνικές που του επιτρέπουν να κατηγοριοποίηση τις πληροφορίες με υψηλό δίκτυ ακρίβειας. Η τεχνολογική λύση της εταιρείας InfoWatch χρησιμοποίει συνδυασμό των τεχνικών Linguistic analysis, object detection και digital fingerprints. [046-047]

4.13 Zecurion

Η τεχνολογική λύση Zecurion Data Loss Prevention συμπεριλαμβάνει ένα ευρύ φάσμα τεχνολογιών με σκοπό να μείωση το ρίσκο της διαρροής ευαίσθητων δεδομένων εκτός οργανισμού. Παρέχει προστασία σε δεδομένα που είναι σε αδράνεια (Data at Rest), δεδομένα που χρησιμοποιούνται (Data in Use) και δεδομένα σε κίνηση (Data in Motion).[116-122]

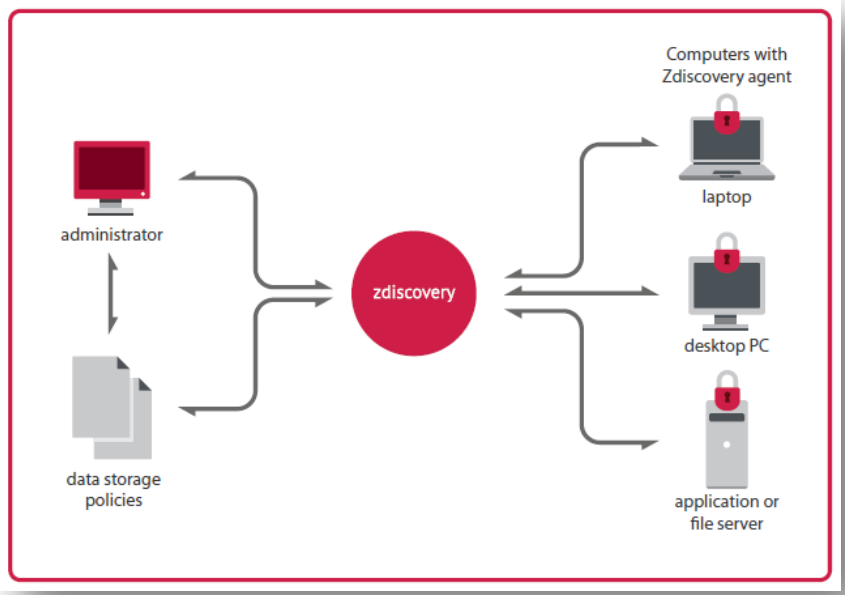


Εικόνα 4.10: Zecurion Data Loss Prevention Αρχιτεκτονική.[122]

4.13.1 Αρχιτεκτονική

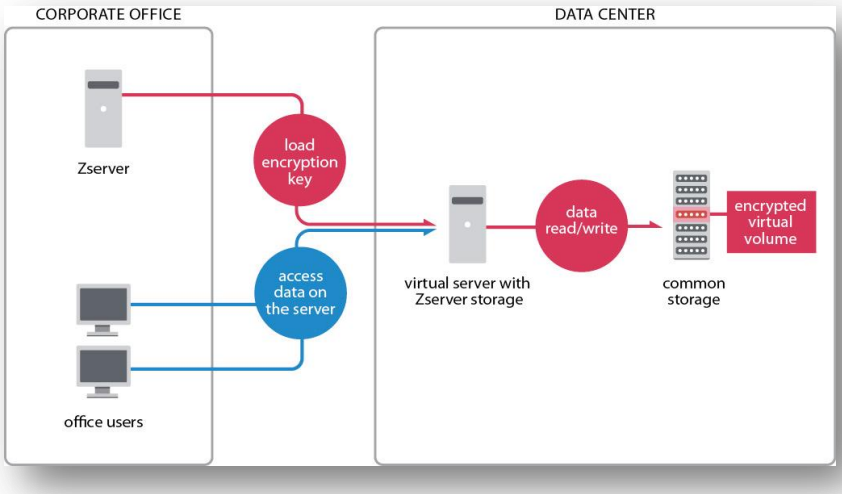
Η τεχνολογική λύση της εταιρείας Zecurion αποτελείται από τα παρακάτω προϊόντα:

- **Zecurion Zdiscovery:** το προϊόν σαρώνει όλα τα αποθηκευμένα δεδομένα στο δίκτυο του οργανισμού, αποκαλύπτει τα «ανάρμοστα» αποθηκευμένα ευαίσθητα δεδομένα και προσδιορίζει τις παραβιάσεις των πολιτικών ασφαλείας. Το Zecurion Zdiscovery χρησιμοποίει υβριδική ανάλυση (hybrid analysis) που μπορεί να καθορίσει με ακρίβεια την κατηγορία των πληροφοριών και να αποφασίσει εάν είναι αποθηκευμένα στην κατάλληλη θέση, με βάση την εταιρική πολιτική και τα πρότυπα της βιομηχανίας. Η εφαρμογή της υβριδικής ανάλυσης βελτιώνει την ανίχνευση των εμπιστευτικών πληροφοριών έως και 95% σε σύγκριση με τα συστήματα που χρησιμοποιούν λιγότερο εξελιγμένες τεχνολογίες ανίχνευσης. [116-122]



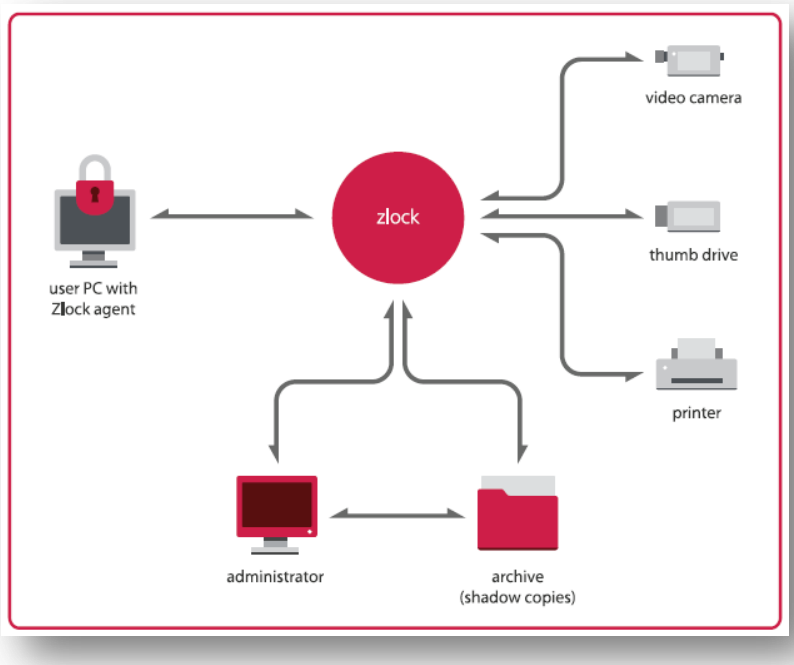
Εικόνα 4.11: •Zecurion Zdiscovery.[118]

- **Zecurion Zserver:** είναι σχεδιασμένο για να προστατεύει τα δεδομένα που είναι αποθηκευμένα σε διακομιστές (Servers) και συσκευές εφεδρικής αποθήκευσης (Backup media). Το σύστημα κρυπτογραφεί τις πληροφορίες όπου περιέχουν οι σκληροί δίσκοι (hard drives), disk arrays και SAN storage χρησιμοποιώντας εξελιγμένη μέθοδο κρυπτογράφησης. Η κρυπτογράφηση με το Zserver προϊόν προστατεύει τις αποθηκευμένες πληροφορίες για το λόγο ότι ο φυσικός έλεγχος είναι αδύνατο να εφαρμοστεί στις συσκευές. Για παράδειγμα, μπορεί να μετακινηθούν τα δεδομένα στο cloud ή ένας σκληρός δίσκος να χαθεί. Για την κρυπτογράφηση του ο Zserver χρησιμοποίει κρυπτογραφικούς αλγορίθμους με μήκος κλειδιού πάνω από 512 bits (AES, XTS-AES). [116-122]



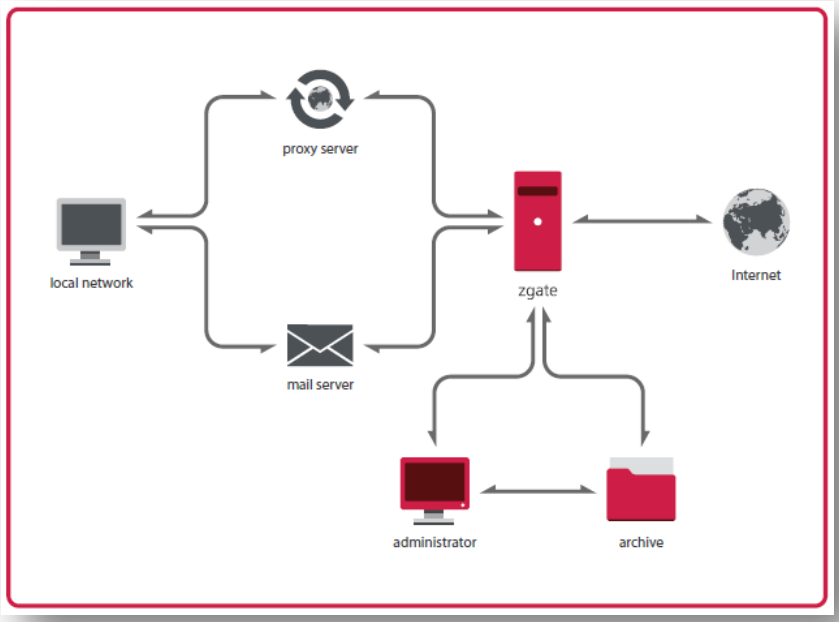
Εικόνα 4.12: •Zecurion Zserver.[121]

- **Zecurion Zlock:** είναι σχεδιασμένο για να προστατεύει από την διαρροή των ευαίσθητων πληροφοριών στα τελικά σημεία (Endpoints) του δικτύου. Το Zecurion Zlock επιτρέπει να ελέγχεται η χρήση των συσκευών που είναι συνδεδεμένες στις θύρες (ports) συμπεριλαμβανόμενου USB, LPT, COM, IrDA, IEEE 1394, PCMCIA και εσωτερικών συσκευών όπως προ-εγκατεστημένες κάρτες δικτύου (network cards), modems, Bluetooth, Wi-Fi, CD/DVD–drives καθώς και τοπικούς και δικτυακούς εκτυπωτές (Network printers). [116-122]



Εικόνα 4.13: Zecurion Zlock.[120]

- **Zecurion Zgate:** Το Zecurion Zgate προϊόν επιτρέπει στους οργανισμούς να παρακολουθούν την κίνηση του δικτύου προς τα έξω καθώς και τις online επικοινωνίες εντοπίζοντας τις ευαίσθητες πληροφορίες και αποτρέποντας τις να φύγουν από το δίκτυο του οργανισμού. Το προϊόν Zgate παρακολουθεί το ηλεκτρονικό ταχυδρομείο (email), τα κοινωνικά δίκτυα (social networks) και τα άμεσα μηνύματα (instant messages). [116-122]



Εικόνα 4.14: Zecurion Zgate.[119]

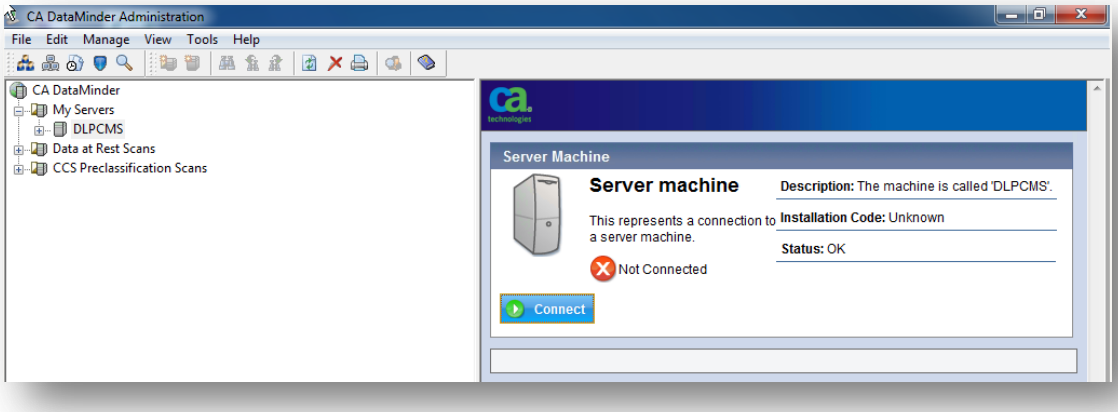
4.13.2 Χρησιμοποιούμενες Μέθοδοι

Η τεχνολογική λύση της εταιρείας Zecurion για να επιτύχει την αποτροπή απώλειας δεδομένων χρησιμοποιεί τις ακόλουθες τεχνικές ανάλυσης δεδομένων: Αντιστοίχηση Λέξεων Κλειδιών (Keyword Matching), Χαρακτηριστικά των αρχείων (File Attribute), ανάλυση βάσει εννοιών (Conceptual/Lexicon Analysis), Κατηγορίες (Categories), Αποτύπωμα Δεδομένων (Data Fingerprinting),, Αλγόριθμοι Μηχανικής Μάθησης (Machine Learning Algorithms).[116-122]

4.14 Εργαλεία Αποτροπής Απώλειας Δεδομένων στην πράξη

Στο παρόν κεφάλαιο θα περιγράψουμε αναλυτικά το πώς λειτουργεί το εργαλείο αποτροπής απώλειας δεδομένων CA DataMinder της εταιρείας CA Technologies. [012]

Το εργαλείο CA DataMinder δίνει την δυνατότητα στους Διαχειριστές (Administrators), μέσω κεντρικής κονσόλας (console), να διαχειρίζονται τα εργαλεία (components) και τις πολιτικές ασφαλείας του συστήματος. Τέτοιες πολιτικές είναι για παράδειγμα: πολιτικές για τα αρχεία (Files), την ηλεκτρονική αλληλογραφία (E-mail), την κίνηση στο ιστό (web traffic), την επιφάνεια εργασίας (Desktop), τους Διακομιστές (servers) και τα όρια του Δικτύου (Network Boundary). Με αυτόν τον τρόπο παρέχεται προστασία στα δεδομένα που βρίσκονται σε καταληκτικό σημείο (Data at Endpoint), στα δεδομένα σε κίνηση (Data in Motion) αλλά και στα δεδομένα σε αδράνεια (Data at Rest).

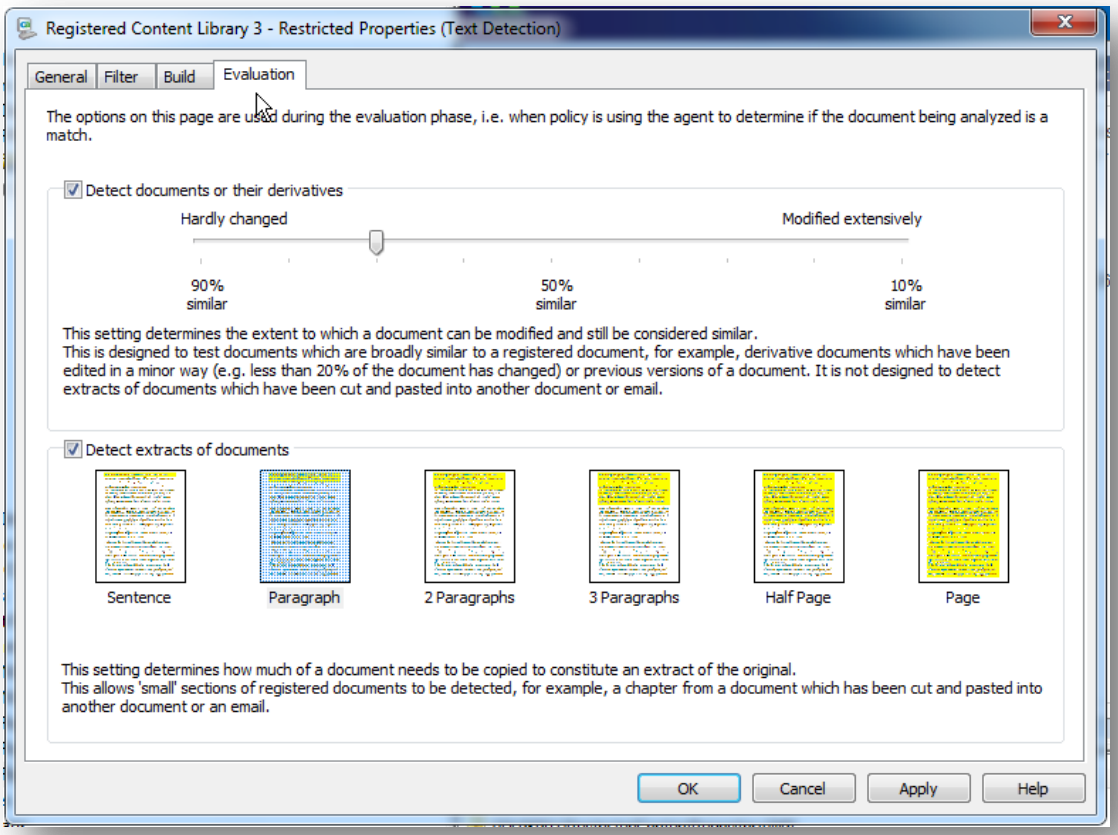


Εικόνα 4.15: CA DataMinder Administration Console. [012]

Η κονσόλα παρέχει γρήγορους συνδέσμους στον διαχειριστή όπως για επεξεργασία και δημιουργία των πολιτικών, προσφέρει αναζητήσεις για τους χρήστες και για την μηχανή. Επίσης μπορεί να δει τα αρχεία καταγραφής (Log files) για τις ενέργειες των χρηστών και του συστήματος.

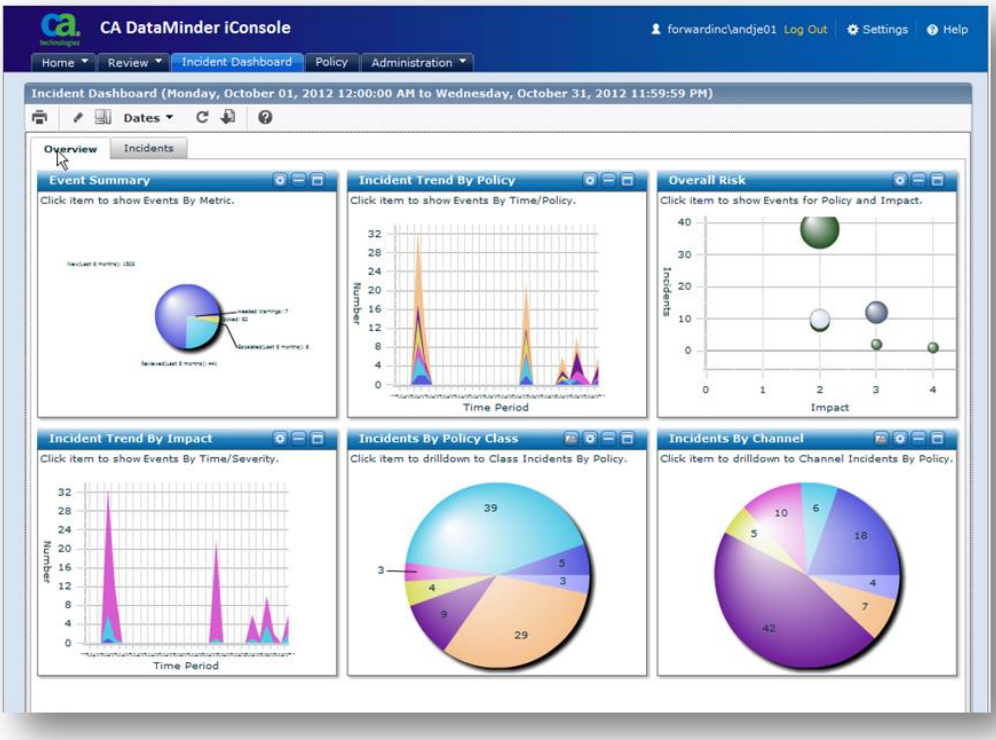
Επιπλέον, παρέχει την ευελιξία στους Διαχειριστές του Συστήματος να θέσουν τα δικά τους κριτήρια για συγκεκριμένους τύπους αρχείων προσαρμοσμένους στις απαιτήσεις του εκάστοτε

οργανισμού. Παρέχει την δυνατότητα προσαρμογής του Συστήματος στην εκάστοτε ροη δεδομένων έτσι ώστε το σύστημα να επιστρέφει όσο το δυνατό χαμηλό βαθμό από ψευδώς θετικές ειδοποιήσεις.



Εικόνα 4.16: CA DataMinder Administration Console. [012]

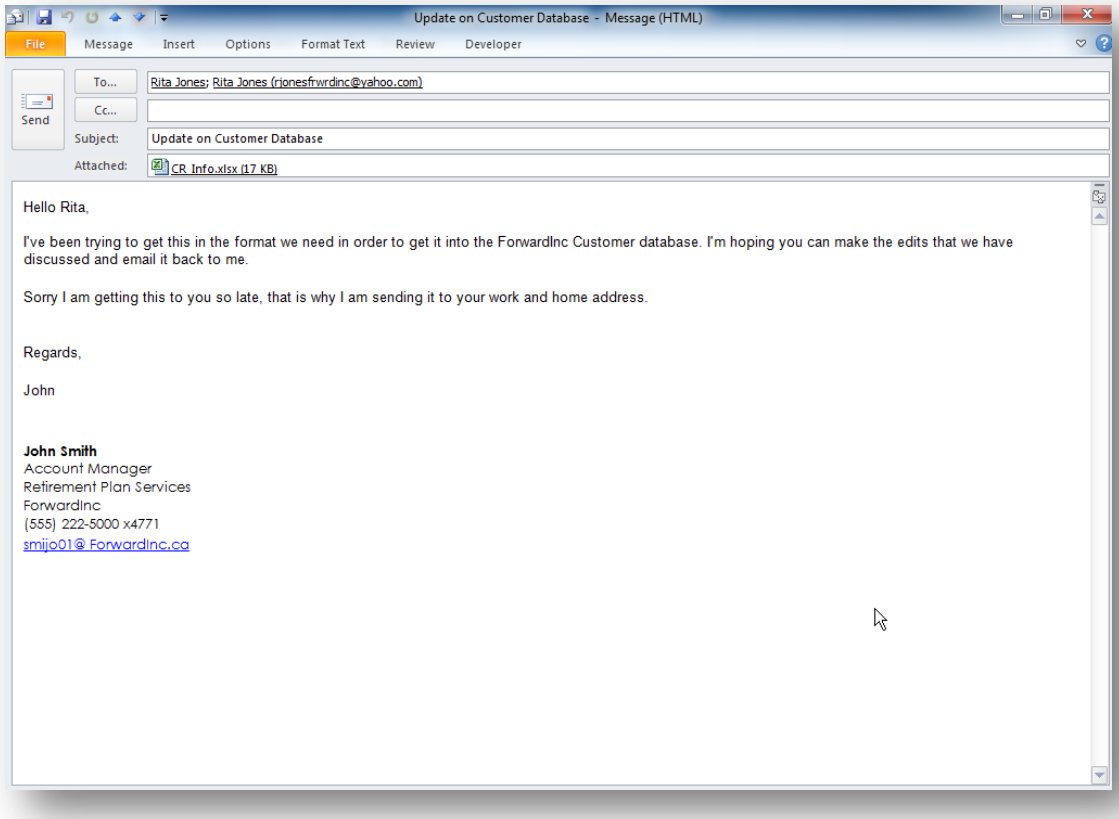
Επιπλέον, το εργαλείο CA DataMinder δίνει την δυνατότητα στους Διαχειριστές (Administrators) μέσω της κεντρικής κονσόλας (console) να βλέπει αναφορές του συστήματος και να επιστρέφει διάφορα στατιστικά στοιχεία. Τα οποία μπορούν να εκμεταλλευτούν οι Διαχειριστές του συστήματος έτσι ώστε να το προσαρμόσουν πιο κοντά στις απαιτήσεις του οργανισμού και το σύστημα να λειτούργει με ακρίβεια και να επιστρέφει χαμηλό ποσοστό από ψευδώς θετικές ειδοποιήσεις. [012]



Εικόνα 4.17: Αναφορές του συστήματος. [012]

4.14.1 Δεδομένα σε Καταληκτικό Σημείο.

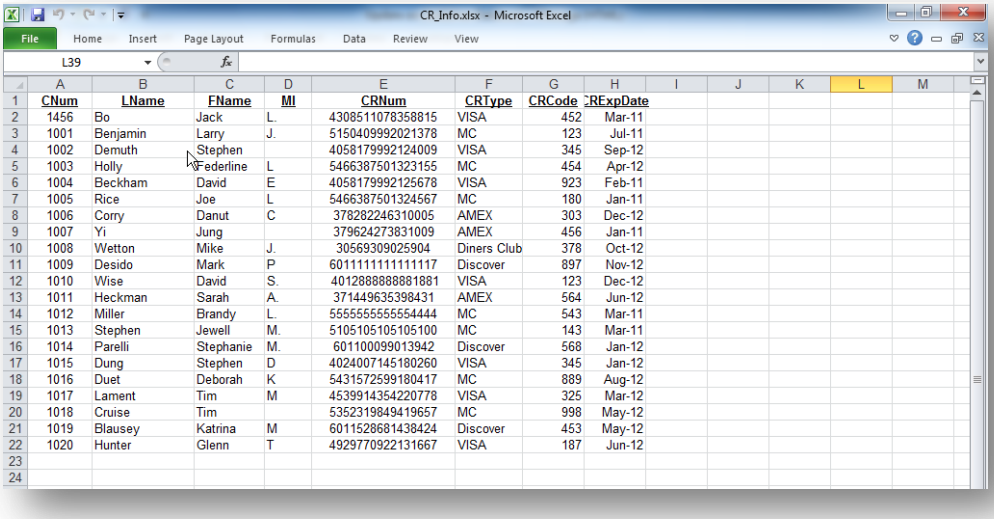
Σε αυτή την ενότητα συμπεριλαμβάνονται η ηλεκτρονική αλληλογραφία (email), τα κοινωνικά δίκτυα (social media), τα αφαιρούμενα μέσα (removable media) και οι εκτυπώσεις (printing)



Εικόνα 4.18:Ηλεκτρονικο ταχυδρομείο με επισυναπτόμενο το αρχείο CR_Info.xlsx.[012]

Σεναριο 1ο

Στο πιο πάνω σενάριο ο John Smith επιχειρεί να στείλει ηλεκτρονικό ταχυδρομείο (email) σε μια εσωτερική και μια εξωτερική ηλεκτρονική διεύθυνση με επισυναπτόμενο (attachment) το αρχείο CR_Info.xlsx το οποίο περιέχει στοιχεία πιστωτικών καρτών από το πελατολόγιο του οργανισμού του.



CR_Info.xlsx - Microsoft Excel

File Home Insert Page Layout Formulas Data Review View

L39

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	CNum	LName	FName	MI	CRNum	CRType	CRCode	CRExpDate					
2	1456	Bo	Jack	L.	4308511078358815	VISA	452	Mar-11					
3	1001	Benjamin	Larry	J.	5150409992021378	MC	123	Jul-11					
4	1002	Demuth	Stephen		4058179992124009	VISA	345	Sep-12					
5	1003	Holly	Federline	L	5466387501323155	MC	454	Apr-12					
6	1004	Beckham	David	E	4058179992125678	VISA	923	Feb-11					
7	1005	Rice	Joe	L	5466387501324567	MC	180	Jan-11					
8	1006	Corry	Danut	C	378282246310005	AMEX	303	Dec-12					
9	1007	Yi	Jung		379624273831009	AMEX	456	Jan-11					
10	1008	Wetton	Mike	J.	30569309025904	Diners Club	378	Oct-12					
11	1009	Desido	Mark	P	6011111111111117	Discover	897	Nov-12					
12	1010	Wise	David	S.	4012888888881881	VISA	123	Dec-12					
13	1011	Heckman	Sarah	A.	371449635398431	AMEX	564	Jun-12					
14	1012	Miller	Brandy	L.	5555555555554444	MC	543	Mar-11					
15	1013	Stephen	Jewell	M.	5105105105105100	MC	143	Mar-11					
16	1014	Parelli	Stephanie	M.	601100099013942	Discover	568	Jan-12					
17	1015	Dung	Stephen	D	4024007145180260	VISA	345	Jan-12					
18	1016	Duet	Deborah	K	5431572599180417	MC	889	Aug-12					
19	1017	Lament	Tim	M	4539914354220778	VISA	325	Mar-12					
20	1018	Cruise	Tim		5352319849419657	MC	998	May-12					
21	1019	Blausey	Katrina	M	6011528681438424	Discover	453	May-12					
22	1020	Hunter	Glenn	T	4929770922131667	VISA	187	Jun-12					
23													
24													

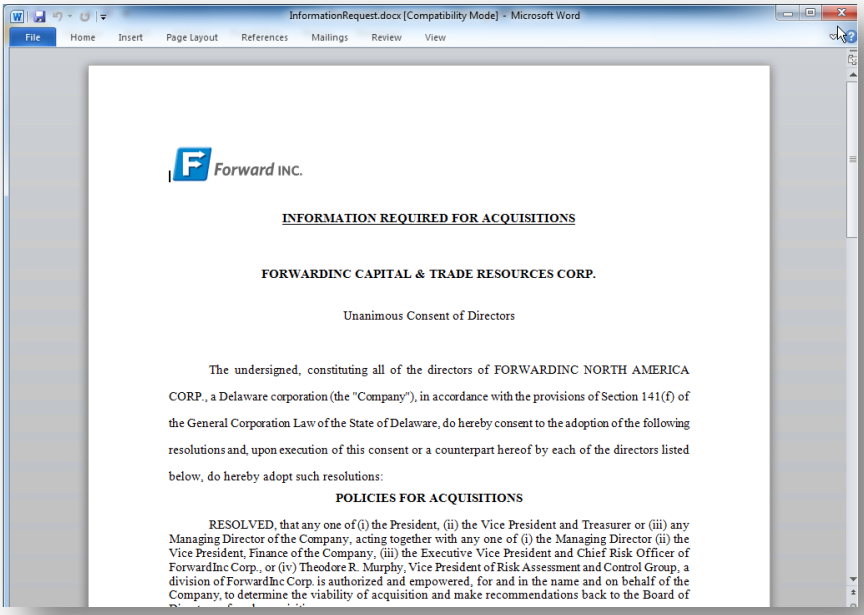
Εικόνα 4.19: Το αρχείο CR_Info.xlsx το οποίο περιέχει πληροφορίες για πιστωτικές κάρτες πελατών. [012]

Οι πληροφορίες αυτές δεν επιτρέπεται να σταλούν . Στην προσπάθεια του χρήστη να πατήσει το κουμπί «αποστολή» (send) το εργαλείο μας CA DataMinder αναλύει το περιεχόμενο του αρχείου εντοπίζοντας κρίσιμες πληροφορίες και ειδοποιεί ότι το περιεχόμενο του μηνύματος δεν μπορεί να σταλεί σε ένα εξωτερικό παραλήπτη.

Εικόνα 4.20: Ειδοποιητικό μήνυμα από εργαλείο CA DataMinder. [012]

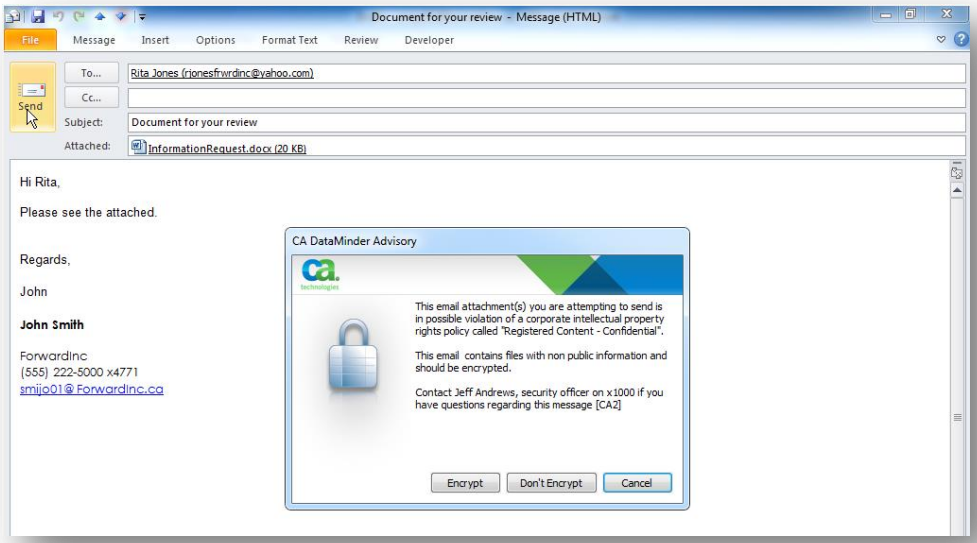
Σενάριο 2ο

Σε αυτό το σενάριο ο John Smith θέλει να στείλει ένα ηλεκτρονικό μήνυμα επισυνάπτοντας αρχείο κείμενου με όνομα InformationRequest.docx σε εξωτερική και εσωτερική ηλεκτρονική διεύθυνση. Το συγκεκριμένο αρχείο είχε προηγουμένως καθοριστεί βάσει της μεθόδου αποτυπώματος αρχείων (Fingerprinting) ως κρίσιμο δεδομένο.



Εικόνα 4.21: Το αρχείο InformationRequest.docx. [012]

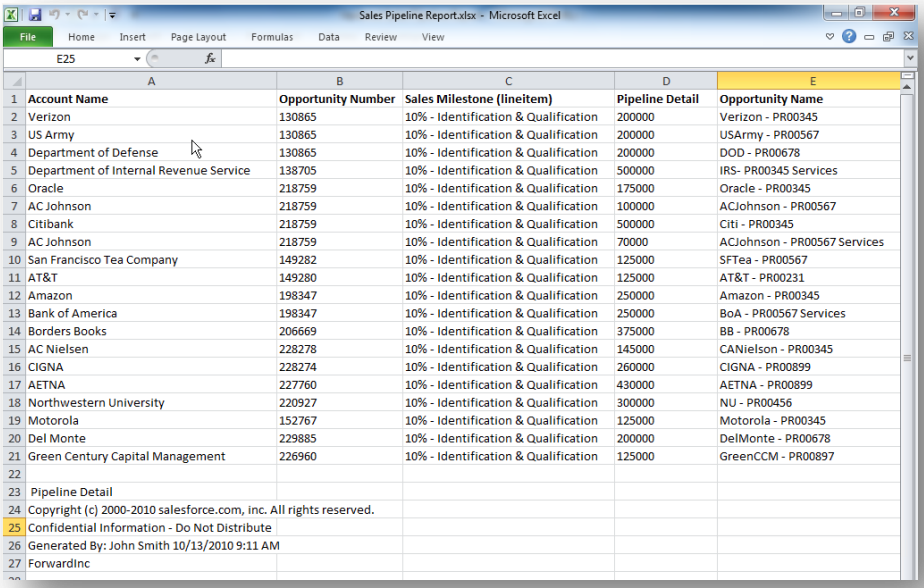
Συμφώνα με τις πολιτικές της εταιρείας έχει καθοριστεί ότι το συγκεκριμένο αρχείο χρειάζεται κρυπτογράφηση για να μετακινηθεί. Έτσι, πατώντας ο John το κουμπί «αποστολή» (send), το εργαλείο μας εντοπίζει την παραβίαση και δίνει τις επιλογές για κρυπτογράφηση (encrypt), ή όχι.



Εικόνα 4.22:Ειδοποιητικό μήνυμα. [012]

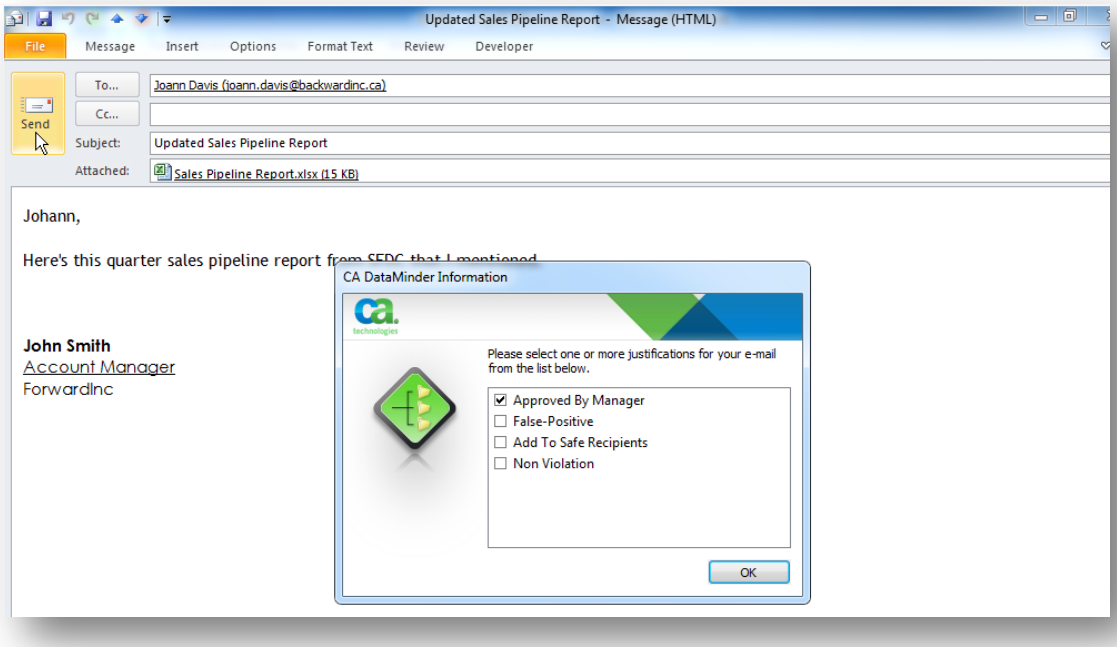
Σενάριο 3ο

Σε αυτό το σενάριο ο John Smith θέλει να στείλει ένα ηλεκτρονικό μήνυμα επισυνάπτοντας αρχείο επεξεργασίας υπολογιστικών φύλων με όνομα Sales Pipeline Report.xlsx σε εσωτερική ηλεκτρονική διεύθυνση. Το συγκεκριμένο αρχείο είχε προηγουμένως καθοριστεί βάσει της μεθόδου αποτυπώματος αρχείων (Fingerprinting) ως κρίσιμο δεδομένο.



	A	B	C	D	E
1	**Account Name**	**Opportunity Number**	**Sales Milestone (lineitem)**	**Pipeline Detail**	**Opportunity Name**
2	Verizon	130865	10% - Identification & Qualification	200000	Verizon - PR00345
3	US Army	130865	10% - Identification & Qualification	200000	USArmy - PR00567
4	Department of Defense	130865	10% - Identification & Qualification	200000	DOD - PR00678
5	Department of Internal Revenue Service	138705	10% - Identification & Qualification	500000	IRS- PR00345 Services
6	Oracle	218759	10% - Identification & Qualification	175000	Oracle - PR00345
7	AC Johnson	218759	10% - Identification & Qualification	100000	ACJohnson - PR00567
8	Citibank	218759	10% - Identification & Qualification	500000	Citi - PR00345
9	AC Johnson	218759	10% - Identification & Qualification	70000	ACJohnson - PR00567 Services
10	San Francisco Tea Company	149282	10% - Identification & Qualification	125000	SFTea - PR00567
11	AT&T	149280	10% - Identification & Qualification	125000	AT&T - PR00231
12	Amazon	198347	10% - Identification & Qualification	250000	Amazon - PR00345
13	Bank of America	198347	10% - Identification & Qualification	250000	BoA - PR00567 Services
14	Borders Books	206669	10% - Identification & Qualification	375000	BB - PR00678
15	AC Nielsen	228278	10% - Identification & Qualification	145000	CANielson - PR00345
16	CIGNA	228274	10% - Identification & Qualification	260000	CIGNA - PR00899
17	AETNA	227760	10% - Identification & Qualification	430000	AETNA - PR00899
18	Northwestern University	220927	10% - Identification & Qualification	300000	NU - PR00456
19	Motorola	152767	10% - Identification & Qualification	125000	Motorola - PR00345
20	Del Monte	229885	10% - Identification & Qualification	200000	DelMonte - PR00678
21	Green Century Capital Management	226960	10% - Identification & Qualification	125000	GreenCCM - PR00897
22					
23	Pipeline Detail				
24	Copyright (c) 2000-2010 salesforce.com, inc. All rights reserved.				
25	Confidential Information - Do Not Distribute				
26	Generated By: John Smith 10/13/2010 9:11 AM				
27	ForwardInc				

Εικόνα 4.23: Το αρχείο Sales Pipeline Report.xlsx. [012]



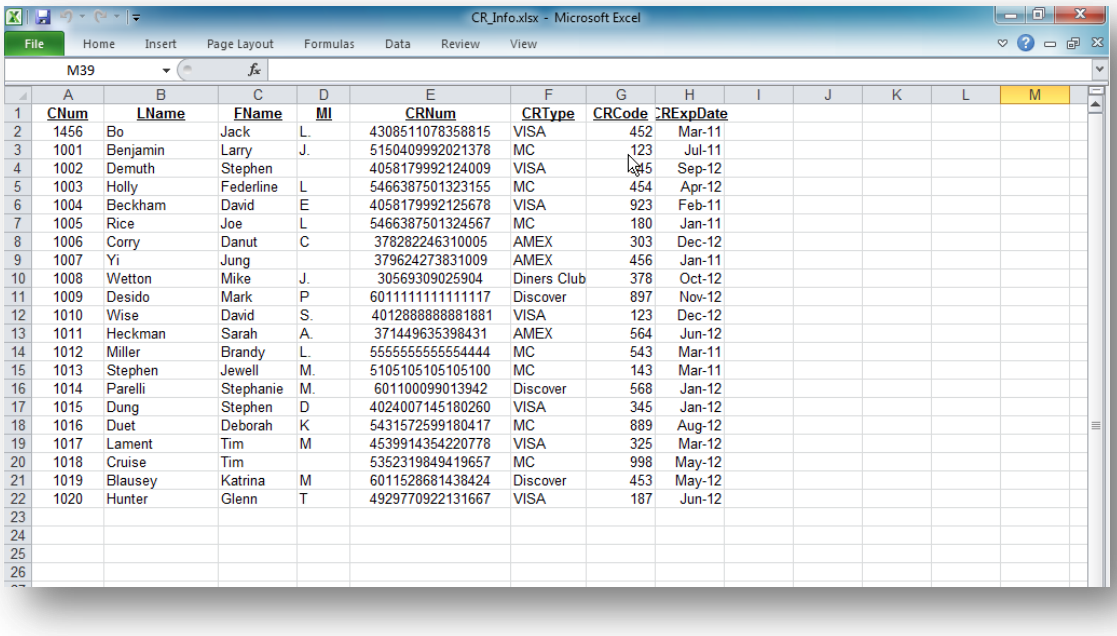
Εικόνα 4.24: Ειδοποιητικό μήνυμα.. [012]

Έτσι πατώντας ο John Smith το κουμπί «αποστολή» (send). Το εργαλείο μας εμφανίζει ένα παράθυρο με αιτιολογήσεις: στην πρώτη επιλογή το αρχείο χρειάζεται αποδοχή από τον

διευθυντή, στη δεύτερη το αρχείο ορίζεται ως ψευδώς θετικό, στην τρίτη προσθέτει τις διεύθυνσεις στους ασφαλείς παραλήπτες και στην τέταρτη δηλώνει ότι δεν υπάρχει παραβίαση. Πριν φτάσει στο παραλήπτη το μήνυμα θα έχει την δυνατότητα ο Διαχειριστής του συστήματος να επεξεργαστεί την πληροφορία και αυτός θα έχει το τελικό λόγο εάν θα ταξιδέψει το ηλεκτρονικό μήνυμα.

Σενάριο 4ο

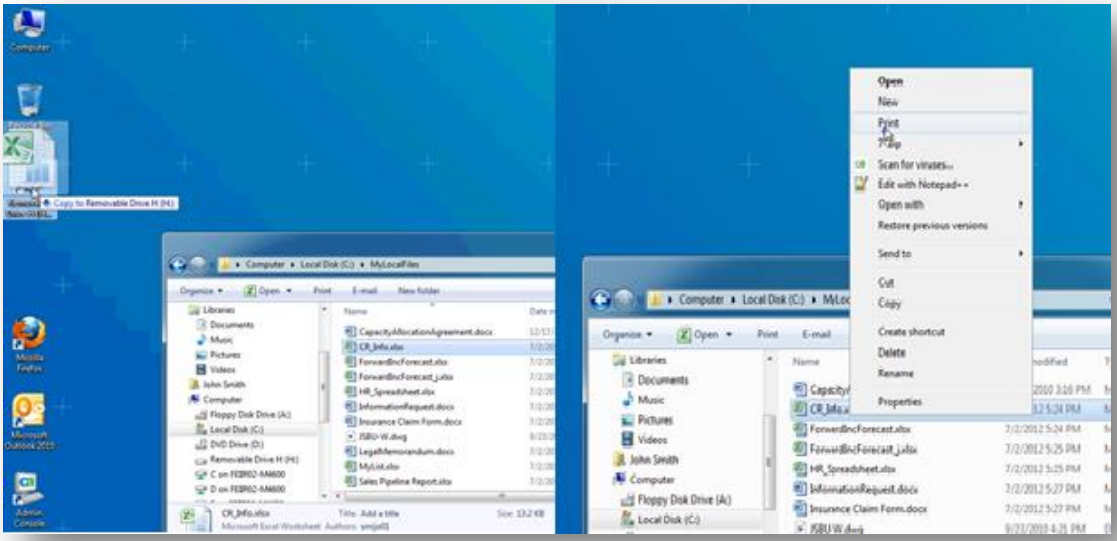
Σε αυτό το σενάριο ο χρήστης John Smith προσπαθεί να αντιγράψει δεδομένα σε μια μνήμη usb ή να εκτυπώσει το αρχείο σε ένα εκτυπωτή. Το αρχείο που επιχειρεί να αντιγράψει ή να εκτυπώσει είναι το αρχείο υπολογιστικών φύλλων excel με όνομα CR_Info.xlsx το οποίο περιέχει στοιχεία των πιστωτικών καρτών (visa card) των πελατών του οργανισμού. Το περιεχόμενο του αρχείου διακρίνεται στην εικόνα: 4.25.



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	CNum	LName	FName	MI	CRNum	CRType	CRCode	CRExpDate					
2	1456	Bo	Jack	L.	4308511078358815	VISA	452	Mar-11					
3	1001	Benjamin	Larry	J.	5150409992021378	MC	123	Jul-11					
4	1002	Demuth	Stephen		4058179992124009	VISA	345	Sep-12					
5	1003	Holly	Federline	L	5466387501323155	MC	454	Apr-12					
6	1004	Beckham	David	E	4058179992125678	VISA	923	Feb-11					
7	1005	Rice	Joe	L	5466387501324567	MC	180	Jan-11					
8	1006	Corry	Danut	C	378282246310005	AMEX	303	Dec-12					
9	1007	Yi	Jung		379624273831009	AMEX	456	Jan-11					
10	1008	Wetton	Mike	J.	30569309025904	Diners Club	378	Oct-12					
11	1009	Desido	Mark	P	6011111111111117	Discover	897	Nov-12					
12	1010	Wise	David	S.	4012888888881881	VISA	123	Dec-12					
13	1011	Heckman	Sarah	A.	371449635398431	AMEX	564	Jun-12					
14	1012	Miller	Brandy	L.	5555555555554444	MC	543	Mar-11					
15	1013	Stephen	Jewell	M.	5105105105105100	MC	143	Mar-11					
16	1014	Parelli	Stephanie	M.	601100099013942	Discover	568	Jan-12					
17	1015	Dung	Stephen	D	4024007145180260	VISA	345	Jan-12					
18	1016	Duet	Deborah	K	5431572599180417	MC	889	Aug-12					
19	1017	Lament	Tim	M	4539914354220778	VISA	325	Mar-12					
20	1018	Cruise	Tim		5352319849419657	MC	998	May-12					
21	1019	Blausey	Katrina	M	6011528681438424	Discover	453	May-12					
22	1020	Hunter	Glenn	T	4929770922131667	VISA	187	Jun-12					

Εικόνα 4.25: Το αρχείο CR_Info.xlsx. [012]

Όταν ο χρήστης προσπαθήσει να μεταφέρει το αρχείο σε USB ή να εκτυπώσει,



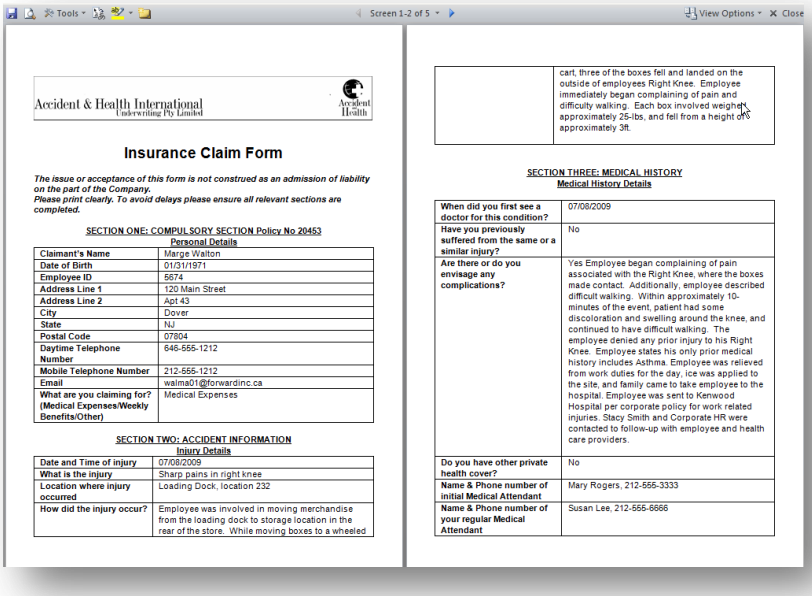
Εικόνα 4.26: Μεταφορά αρχείου σε αφαιρούμενη μνήμη (USB) ή εκτύπωση αρχείου. [012]

Τότε εμφανίζεται ένα προειδοποιητικό μήνυμα πως δεν μπορεί το συγκεκριμένο αρχείο να μετακινηθεί ή να εκτυπωθεί.

Εικόνα 4.27: Ειδοποιητικό μήνυμα. [012]

Σενάριο 5ο

Σε αυτό το σενάριο ο χρήστης John Smith προσπαθεί να αντιγράψει δεδομένα σε μια μνήμη usb ή να εκτυπώσει το αρχείο σε ένα εκτυπωτή. Το αρχείο που επιχειρεί να αντιγράψει ή να εκτυπώσει είναι το αρχείο επεξεργασίας κειμένου με όνομα Insurance Claim Form.docx το οποίο περιέχει προστατευμένες πληροφορίες για την υγεία (Protected health information- PHI) ενός πελάτη του οργανισμού. Το περιεχόμενο του αρχείου διακρίνεται στην εικόνα 4.28.



Accident & Health International Underwriting Pty Limited

Insurance Claim Form

The issue or acceptance of this form is not construed as an admission of liability on the part of the Company.
Please print clearly. To avoid delays please ensure all relevant sections are completed.

SECTION ONE: COMPULSORY SECTION Policy No 20453
Personal Details

Claimant's Name	Marge Walton
Date of Birth	01/31/1971
Employee ID	5674
Address Line 1	120 Main Street
Address Line 2	Apt 43
City	Dover
State	NJ
Postal Code	07804
Daytime Telephone Number	646-555-1212
Mobile Telephone Number	212-555-1212
Email	walma01@forwardinc.ca
What are you claiming for? (Medical Expenses/Weekly Benefits/Other)	Medical Expenses

SECTION TWO: ACCIDENT INFORMATION
Injury Details

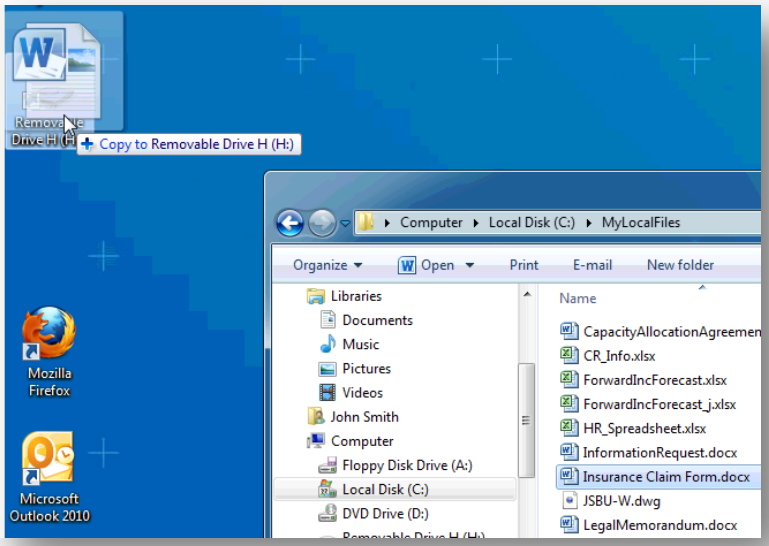
Date and Time of injury	07/08/2009
What is the injury	Sharp pains in right knee
Location where injury occurred	Loading Dock, location 232
How did the injury occur?	Employee was involved in moving merchandise from the loading dock to storage location in the rear of the store. While moving boxes to a wheeled cart, three of the boxes fell and landed on the outside of employees Right Knee. Employee immediately began complaining of pain and difficulty walking. Each box involved weighed approximately 25-lbs, and fell from a height of approximately 3ft.

SECTION THREE: MEDICAL HISTORY
Medical History Details

When did you first see a doctor for this condition?	07/08/2009
Have you previously suffered from the same or a similar injury?	No
Are there or do you envisage any complications?	Yes Employee began complaining of pain associated with the Right Knee, where the boxes made contact. Additionally, employee described difficult walking. Within approximately 10-minutes of the event, patient had some discoloration and swelling around the knee, and continued to have difficult walking. The employee denied any prior injury to his Right Knee. Employee states his only prior medical history includes Asthma. Employee was relieved from work duties for the day, ice was applied to the site, and family came to take employee to the hospital. Employee was sent to Kenwood Hospital per corporate policy for work related injuries. Stacy Smith and Corporate HR were contacted to follow-up with employee and health care providers.
Do you have other private health cover?	No
Name & Phone number of initial Medical Attendant	Mary Rogers, 212-555-3333
Name & Phone number of your regular Medical Attendant	Susan Lee, 212-555-6666

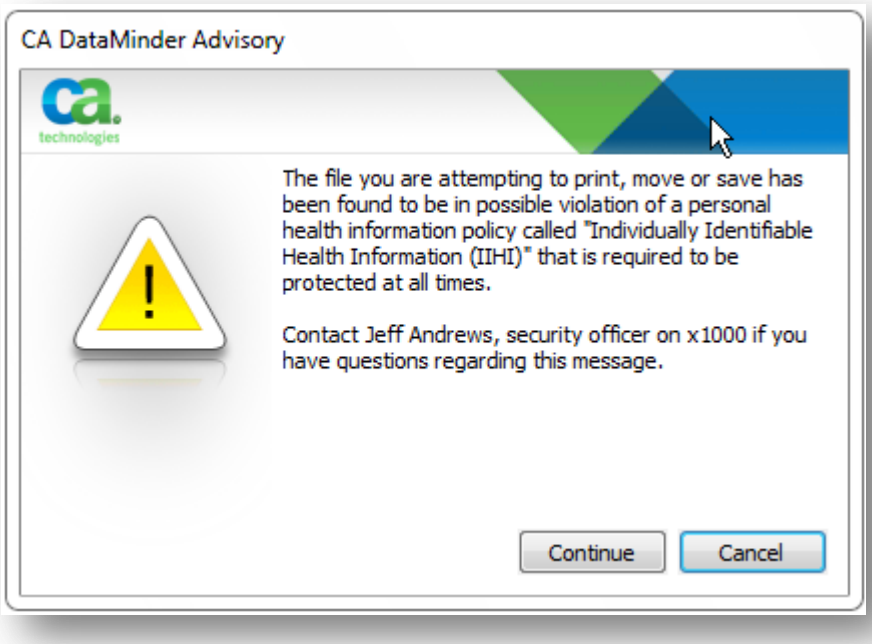
Εικόνα 4.28: Το αρχείο Insurance Claim form.docx. [012]

Όταν ο χρήστης προσπαθήσει να μεταφέρει το αρχείο σε USB ή να εκτυπώσει (εικόνα 4.29),



Εικόνα 4.29: Μεταφορά αρχείου σε αφαιρούμενη συσκευή. [012]

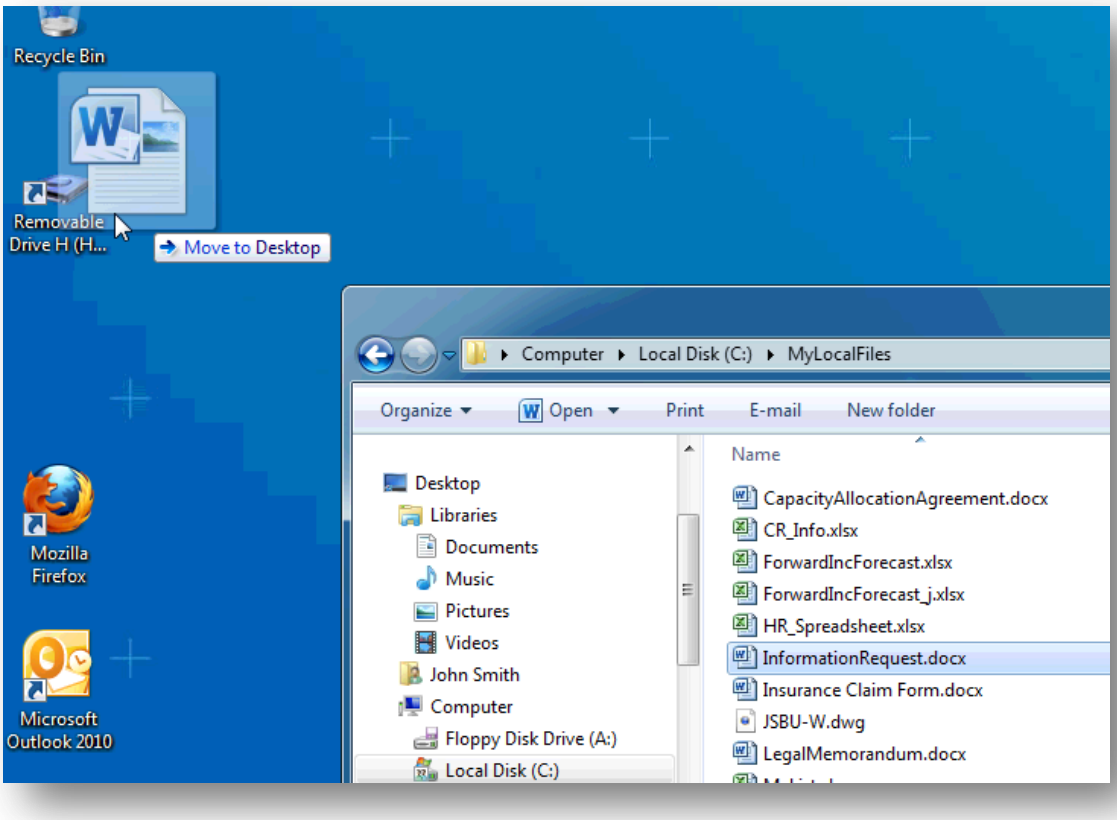
Τότε εμφανίζεται ένα προειδοποιητικό μήνυμα ότι το αρχείο όταν αντιγράφει ή εκτυπωθεί παραβιάζει τις πολιτικές του οργανισμού (εικόνα: 4.30).



Εικόνα 4.30: Προειδοποιητικό Μήνυμα

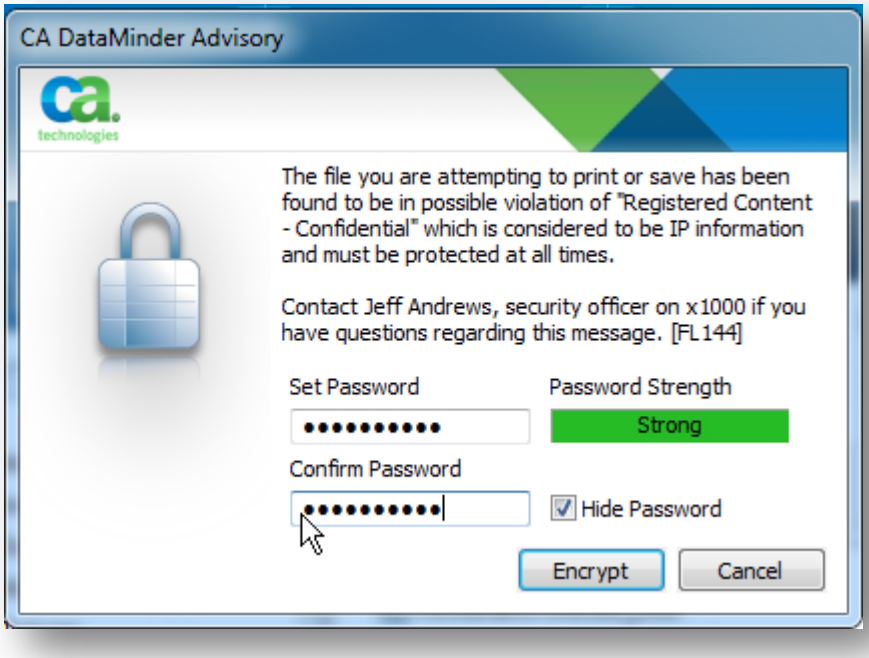
Σενάριο 6ο

Το αρχείο InformationRequest.docx έχει οριστεί με την μέθοδο του αποτυπώματος αρχείου ως κρίσιμο. Όταν ο χρήστης προσπαθήσει να μεταφέρει το αρχείο σε USB ή να εκτυπώσει (εικόνα: 4.31) το συγκεκριμένο αρχείο, εμφανίζεται ένα μήνυμα σχετικά με το ότι το αρχείο θα πρέπει να κρυπτογραφηθεί. (εικόνα: 4.32).



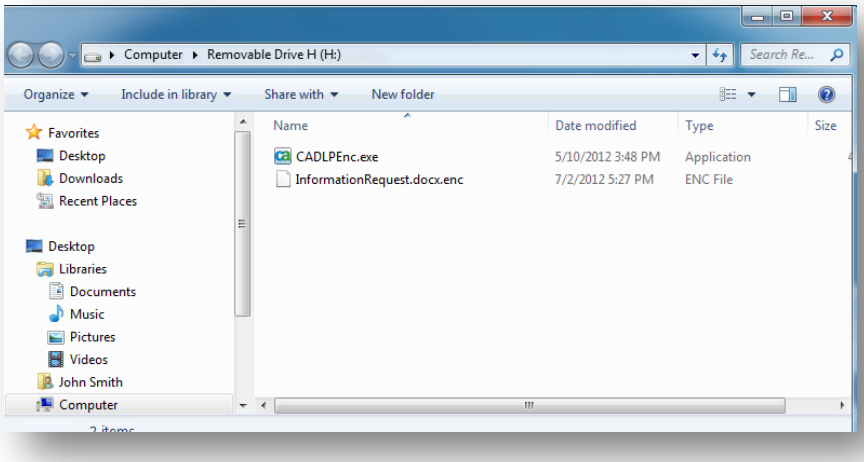
Εικόνα 4.32: Μεταφορά αρχείου σε αφαιρούμενη συσκευή. [012]

Ο χρήστης δίνει στο αρχείο κωδικό και πατώντας το κουμπί «encrypt» το αρχείο κρυπτογραφείται.

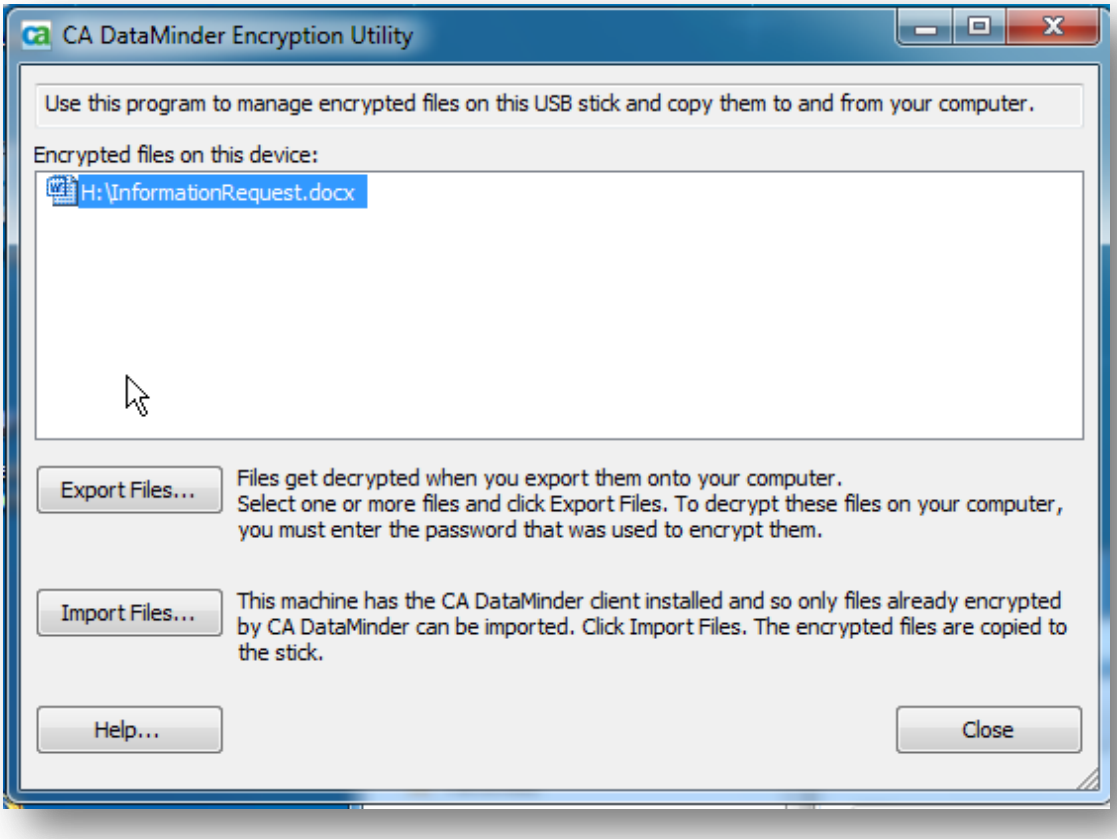


Εικόνα 4.33: Κρυπτογράφηση Αρχείου. [012]

Στο USB τώρα υπάρχει το κρυπτογραφημένο αρχείο και ένα βοηθητικό πρόγραμμα (CADLPEnc.exe), με το οποίο μπορεί κάποιος να διαχειριστεί το κρυπτογραφημένο αρχείο στο Usb stick. (εικόνα: 4.33).



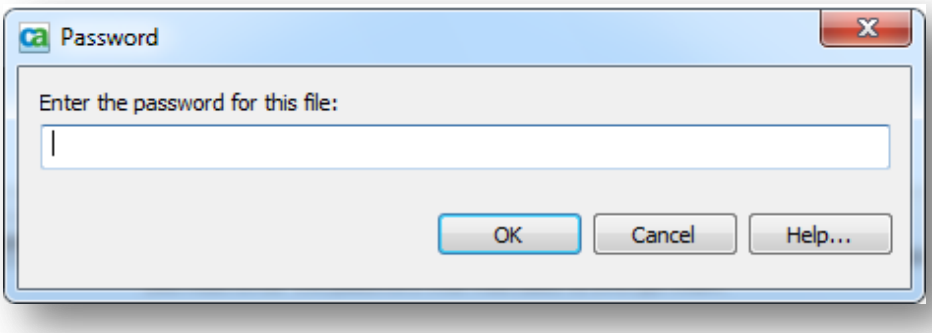
Εικόνα 4.34: Κρυπτογραφημένο Αρχείο. [012]



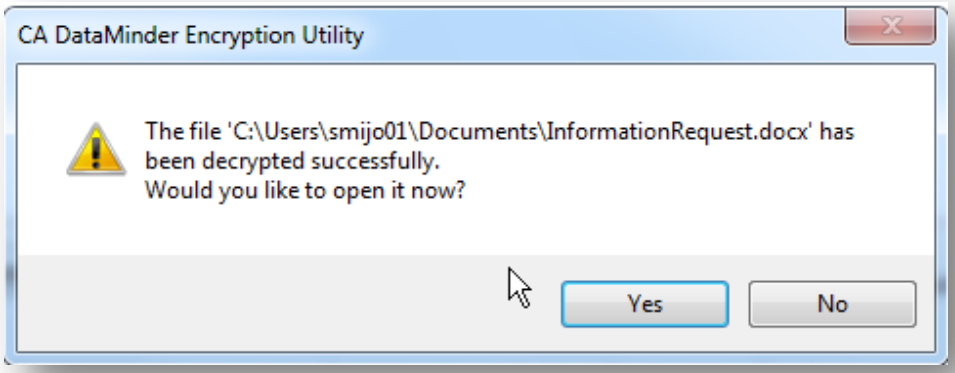
Εικόνα 4.35: Αποκρυπτογράφηση Αρχείου. [012]

Για να αποκρυπτογραφήσει κάποιος το αρχείο, επιλέγει το βοηθητικό πρόγραμμα και εμφανίζεται η πιο πάνω εικόνα. Πατώντας το κουμπί «εξαγωγή αρχείων» (export files) και

διαλέγοντας το χώρο που θέλουμε να αποκρυπτογραφήσουμε το αρχείο μας, ζητείται να προσθέσουμε το κωδικό με το οποίο κρυπτογραφήθηκε το αρχείο έτσι ώστε να γίνει με επιτυχία η αποκρυπτογράφηση.



Εικόνα 4.36: Αποκρυπτογράφηση Αρχείου. [012]

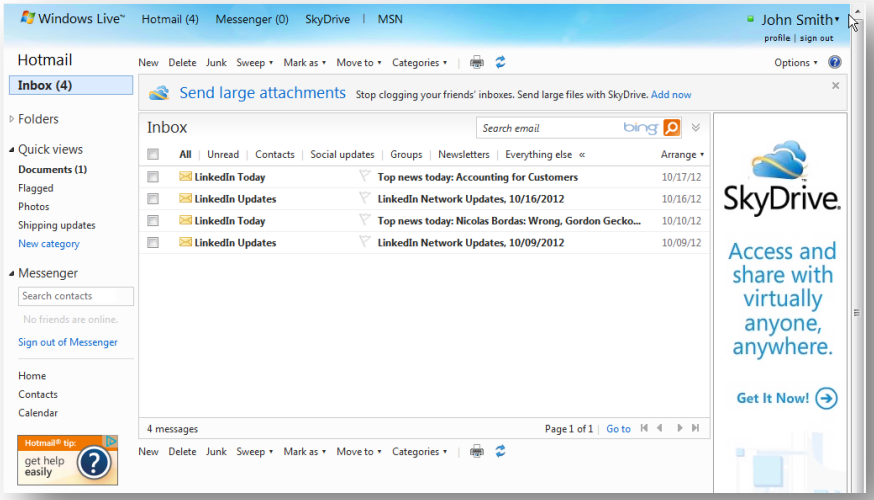


Εικόνα 4.37: Αποκρυπτογράφηση Αρχείου. [012]

Στην συνέχεια εμφανίζεται το μήνυμα ότι το αρχείο έχει αποκρυπτογραφηθεί με επιτυχία. (εικόνα: 4.37).

Σενάριο 7ο

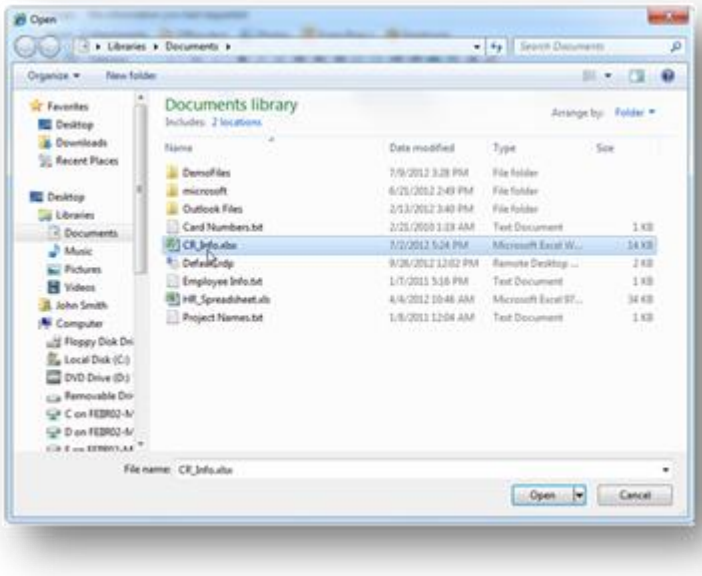
Σε αυτό το σενάριο ο χρήστης John Smith θα χρησιμοποιήσει την υπηρεσία hotmail για στείλει δεδομένα σε ένα εξωτερικό παραλήπτη.



Εικόνα 4.38: Υπηρεσία ηλεκτρονικού ταχυδρομείου Hotmail. [012]

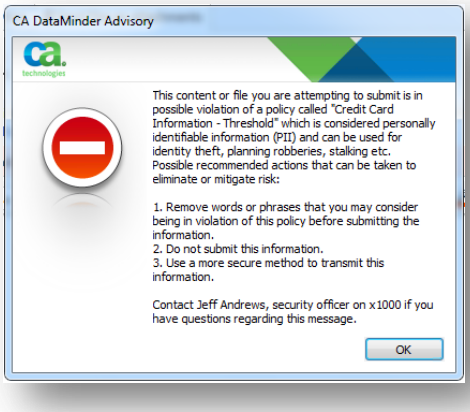
Ο John Smith θα στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στην Rita Jones η οποία χρησιμοποίει και αυτή την υπηρεσία Hotmail, δηλαδή με όνομα περιοχής live.com.

Ο John Smith θα επισυνάψει το αρχείο CR_Info.xlsx το οποίο περιέχει πληροφορίες σχετικά με τις πιστωτικές κάρτες των πελατών (Customers credit card information).



Εικόνα 4.39: Ανέβασμα αρχείου CR_Info.xlsx. [012]

Όταν ο John Smith πατήσει το κουμπί «Open» τότε εμφανίζεται ένα μήνυμα παρεμπόδισης της διαδικασίας από το εργαλείο αποτροπής απώλειας δεδομένων. Το μόνο που μπορεί να κάνει είναι να πατήσει το κουμπί «OK» και να συνεχίσει χωρίς να επισυνάψει το αρχείο. [012]



Εικόνα 4.40: Ειδοποιητικό μήνυμα. [012]

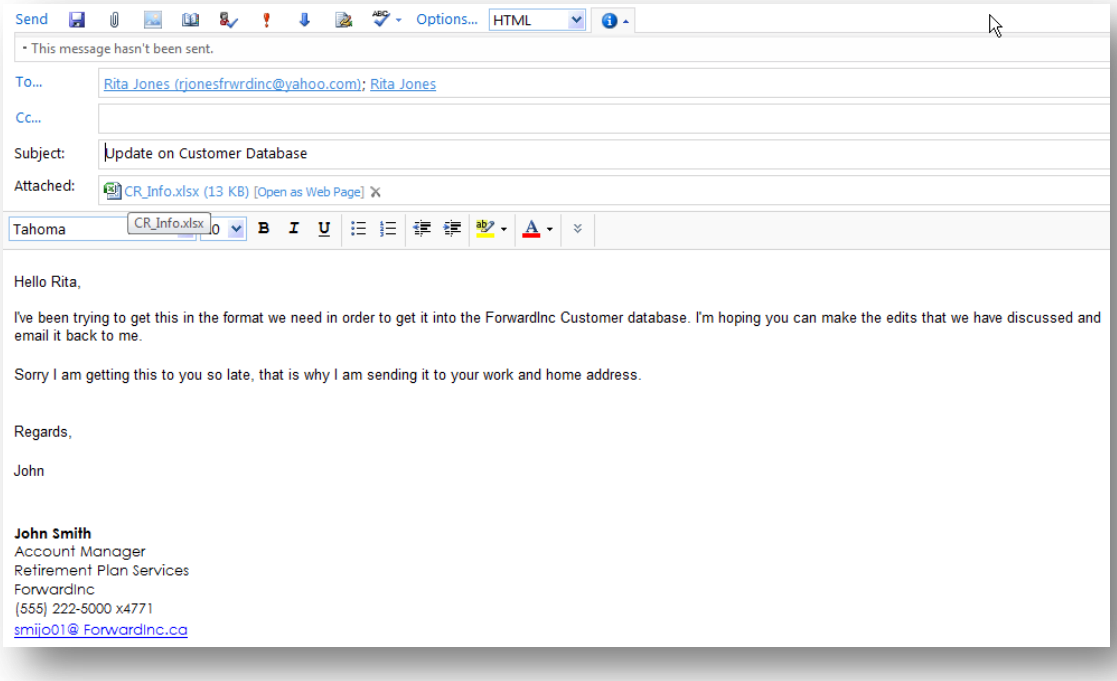
4.14.2 Δεδομένα σε κίνηση

Με τον όρο Δεδομένα σε Κίνηση (Data in Motion) αναφερόμαστε στη χρήση του Outlook Web Application-OWA, τη χρήση του Ιστού (Web), τη χρήση του πρωτοκόλλου μεταφοράς αρχείων (File Transfer Protocol- FTP) και τη χρήση των άμεσων μηνυμάτων (Instant Message- IM).

Σεναριο 1ο

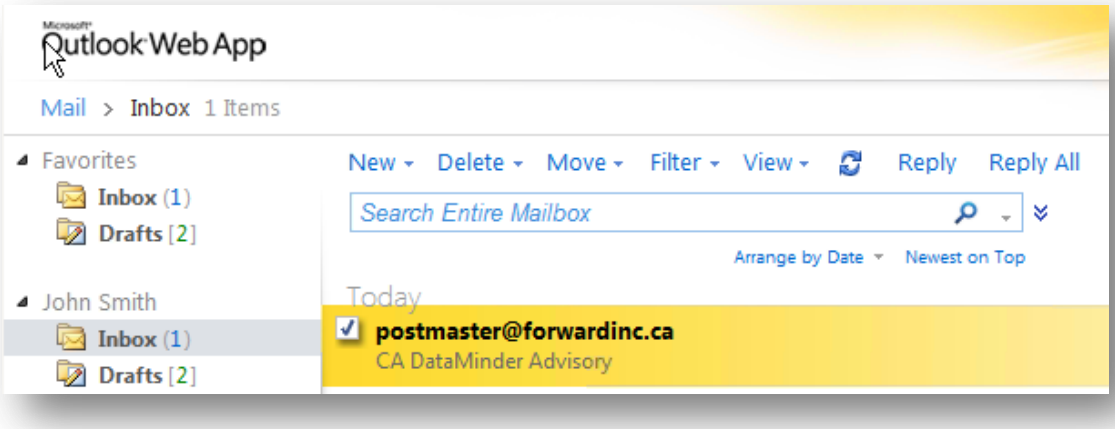
Σε αυτό το σεναριο θα χρησημοποιησουμε το Outlook Web Application για να διαπιστώσουμε πως προστατεύονται τα εμπιστευτικά δεδομενα της επιχείρησης.

Ο υπάλληλος John Smith θα επιχειρήσει να στείλει το αρχείο CR_Info.xlsx σε μια εξωτερική διεύθυνση ηλεκτρονικού ταχυδρομείου και σε μια εσωτερική διεύθυνση ηλεκτρονικού ταχυδρομείου. Το επισυναπτόμενο αρχείο περιέχει αριθμούς πιστωτικών καρτών των πελατών της επιχείρησης.



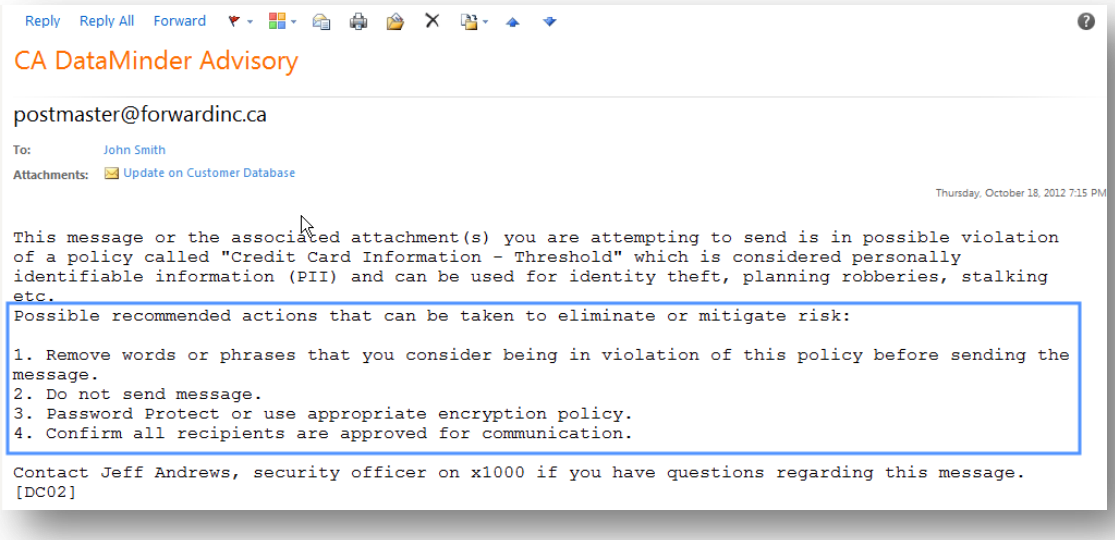
Εικόνα 4.41: Ηλεκτρονικό ταχυδρομείο με επισυναπτόμενο το αρχείο CR_Info.xlsx. [012]

Πατώντας το κουμπί «αποστολή» (send) ο John Smith στέλνει το μήνυμα όμως αμέσως έρχεται ένα ειδοποιητικό μήνυμα στη εισερχόμενη αλληλογραφία (Inbox) του ηλεκτρονικού ταχυδρομείου όπου αναφέρει ότι παραβιάζονται οι πολιτικές της εταιρείας.



Εικόνα 4.42: Η εισερχόμενη αλληλογραφία (inbox). [012]

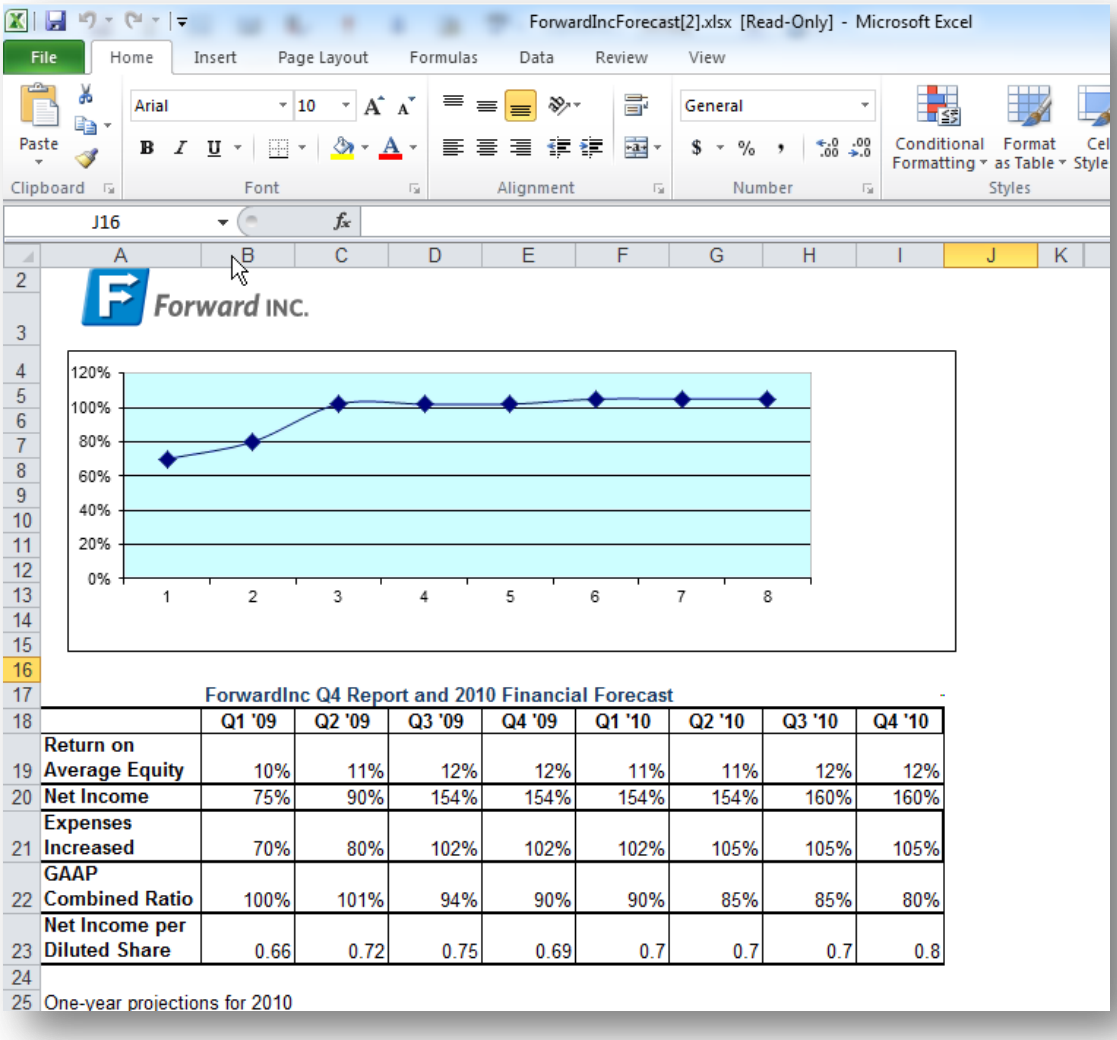
Το μήνυμα εξηγεί με λεπτομερείς πληροφορίες πώς θα αντιμετωπίσει το πρόβλημα αυτό, και επισυνάπτει ταυτόχρονα και το αρχικό ηλεκτρονικό μήνυμα.



Εικόνα 4.43: Ειδοποιητικό μήνυμα. [012]

Σεναριο 2ο

Σε αυτό το σενάριο ο υπάλληλος προσπαθεί να στείλει μήνυμα με το ηλεκτρονικό ταχυδρομείο με επισυναπτόμενο αρχείο στο οποίο περιέχονται οικονομικά δεδομένα.

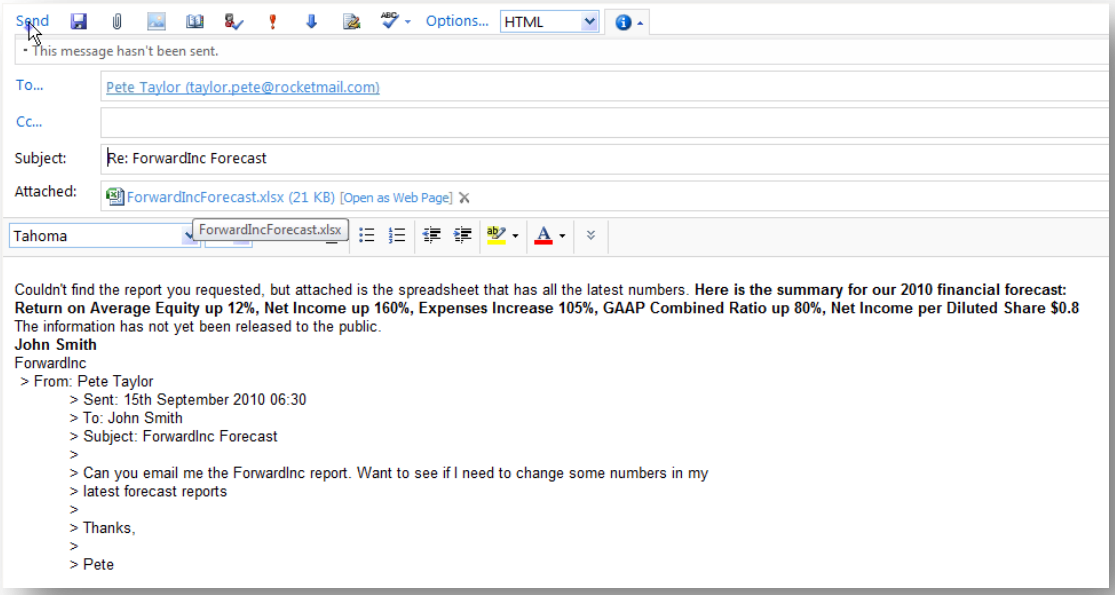


ForwardInc Q4 Report and 2010 Financial Forecast

	Q1 '09	Q2 '09	Q3 '09	Q4 '09	Q1 '10	Q2 '10	Q3 '10	Q4 '10
Return on Average Equity	10%	11%	12%	12%	11%	11%	12%	12%
Net Income	75%	90%	154%	154%	154%	154%	160%	160%
Expenses Increased	70%	80%	102%	102%	102%	105%	105%	105%
GAAP Combined Ratio	100%	101%	94%	90%	90%	85%	85%	80%
Net Income per Diluted Share	0.66	0.72	0.75	0.69	0.7	0.7	0.7	0.8

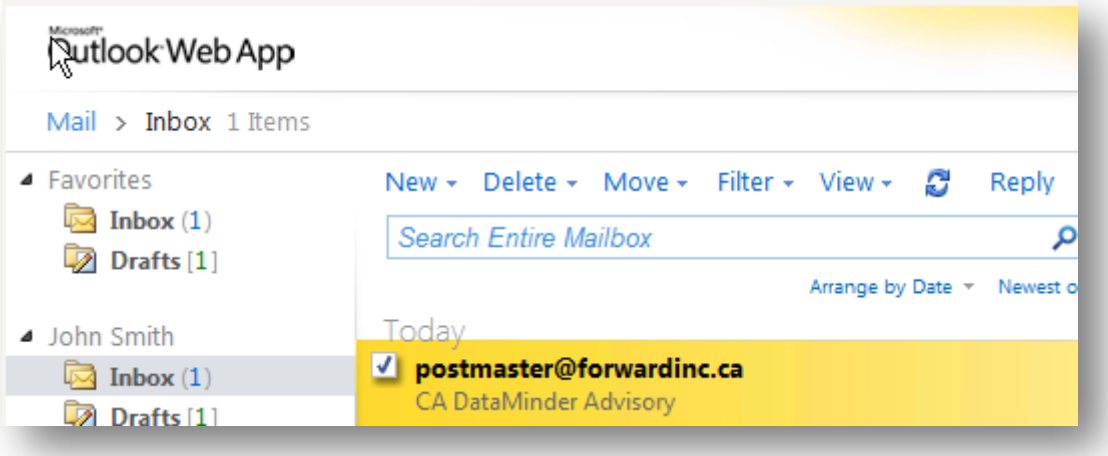
One-year projections for 2010

Εικόνα 4.44: Το αρχείο ForwardIncForecast.xlsx.[012]



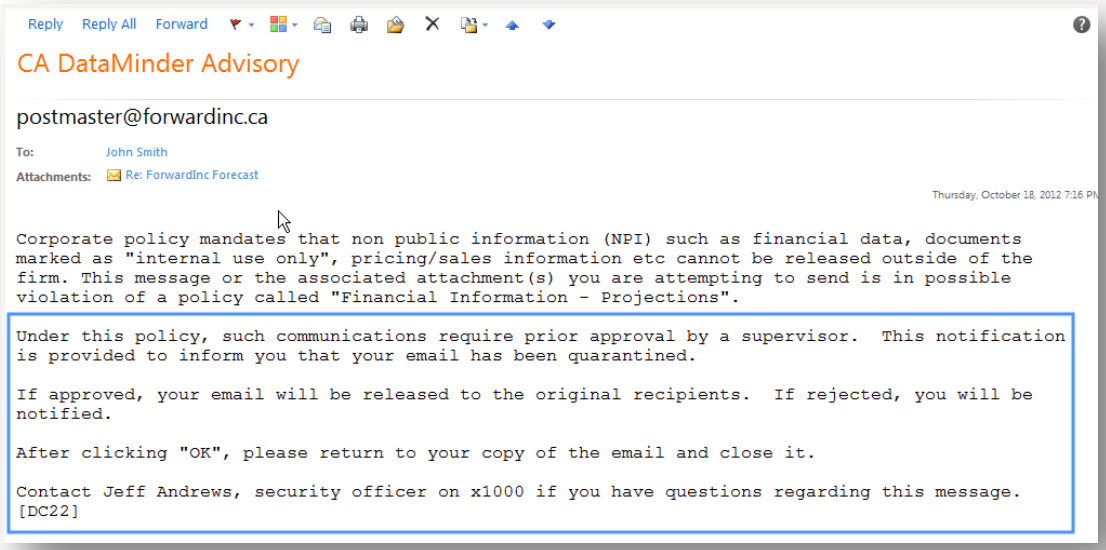
Εικόνα 4.45: Ηλεκτρονικό ταχυδρομείο με επισυναπτόμενο το αρχείο ForwardIncForecast.xlsx. [012]

Πατώντας το κουμπί «αποστολή» (send) ο John Smith στέλνει το μήνυμα όμως αμέσως έρχεται ένα ειδοποιητικό μήνυμα στη εισερχόμενη αλληλογραφία (Inbox) του ηλεκτρονικού ταχυδρομείου.



Εικόνα 4.46: Η εισερχόμενη αλληλογραφία (inbox). [012]

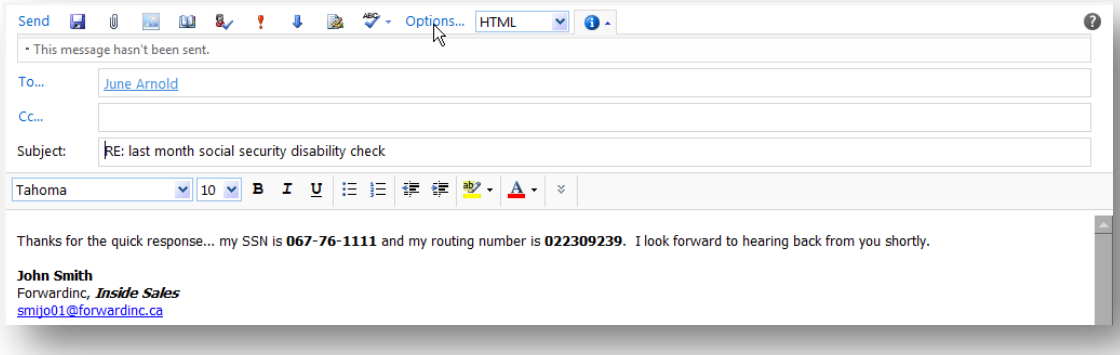
Το ειδοποιητικό μήνυμα εξηγεί ότι το ηλεκτρονικό μήνυμα έχει μπει σε καραντίνα (quarantine) και περιμένει τον διαχειριστή να το αποδεχτεί ή να το απορρίψει.



Εικόνα 4.47: Ειδοποιητικό μήνυμα. [012]

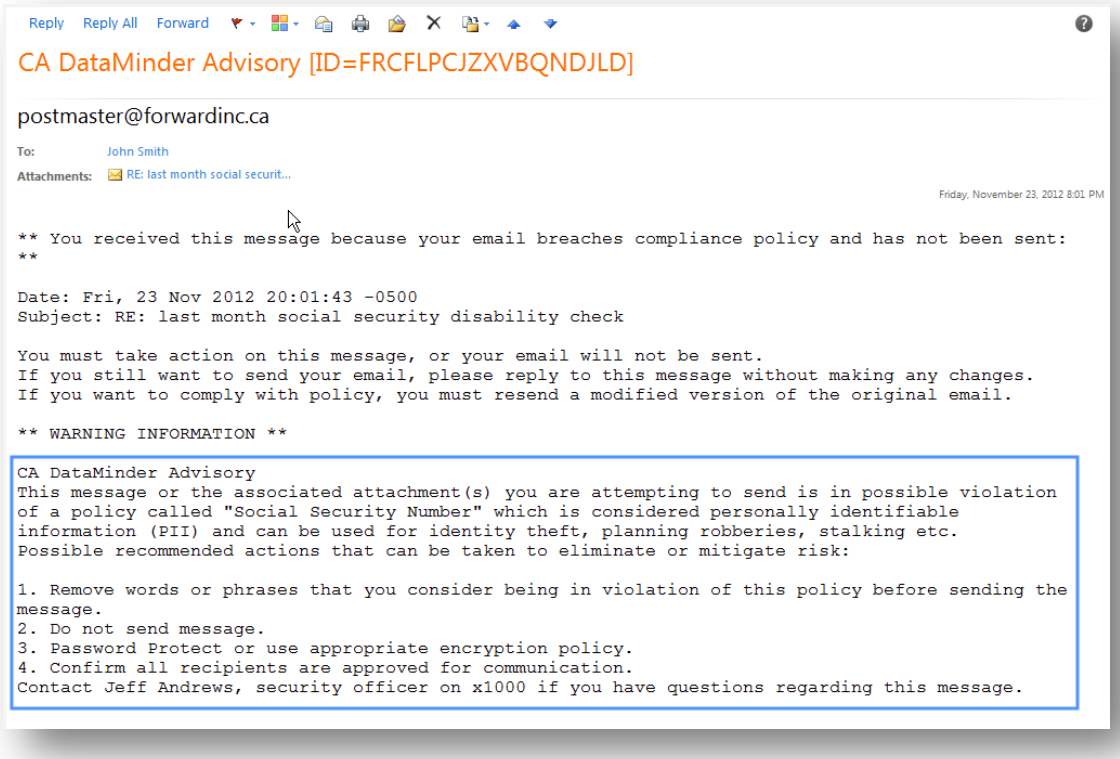
Σεναριο 3ο

Στο σενάριο αυτό ο υπαλληλος θα επιχειρήσει να στείλει σε μια εσωτερική ηλεκτρονική διεύθυνση προσωπικά δεδομένα που αφορούν υπαλλήλους.

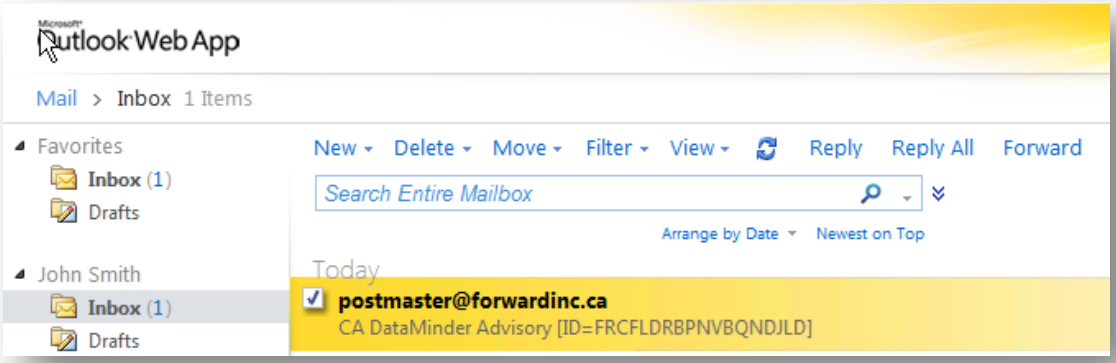


Εικόνα 4.48: Ηλεκτρονικό ταχυδρομείο να συμπεριλαμβάνει προσωπικά δεδομένα υπαλλήλων. [012]

Πατώντας το κουμπί «αποστολή» (send) ο John Smith στέλνει το μήνυμα όμως αμέσως έρχεται ένα ειδοποιητικό μήνυμα στη εισερχόμενη αλληλογραφία (Inbox) του ηλεκτρονικού ταχυδρομείου.



Εικόνα 4.49 Η εισερχόμενη αλληλογραφία (inbox). [012]

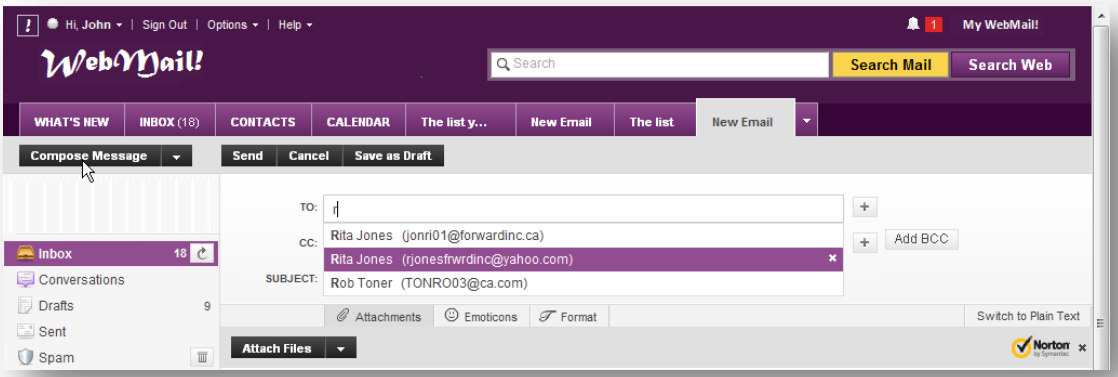


Εικόνα 4.50: Ειδοποιητικό μήνυμα.[012]

Το ειδοποιητικό μήνυμα με λεπτομερή τρόπο εξηγεί πώς παράγεται αυτό το αίτημα και επεξηγεί σε ποιες ενέργειες μπορεί να προβεί ο αποστολέας (π.χ. να στείλει το αρχικό κείμενο χωρίς να κάνει καμιά αλλαγή εφόσον απευθύνεται σε συγκεκριμένα εγκεκριμένα άτομα ή να στείλει το μήνυμα ξανά χωρίς να περιέχει πληροφορίες οι οποίες πλήττουν τις πολιτικές της εταιρείας).

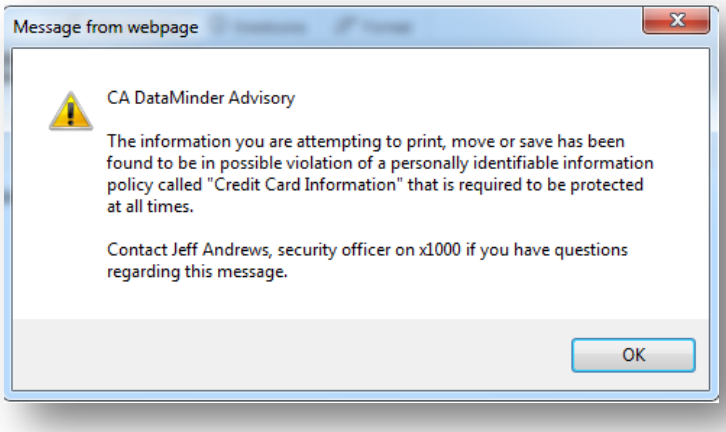
Σενάριο 4ο

Σε αυτό το σενάριο ο υπάλληλος John Smith θα επιχειρήσει να στείλει μέσω webmail (και συγκεκριμένα με hotmail) επισυναπτόμενο αρχείο (με το όνομα card numbers.txt) το οποίο περιέχει στοιχεία από πιστωτικές κάρτες πελατών, οι οποίες έγιναν εξαγωγή από βάση δεδομένων.



Εικόνα 4.51: Ηλεκτρονικό ταχυδρομείο Hotmail. [012]

Το αρχείο ονομάζεται card numbers.txt το οποίο θα στείλει σε μια άλλη διεύθυνση hotmail. Στην προσπάθεια να επισυναφθεί το αρχείο εμφανίζεται ένα προειδοποιητικό μήνυμα από το CA Dataminder δίκτυο περί φραγμού (block) της εν λόγω επισύναψης.

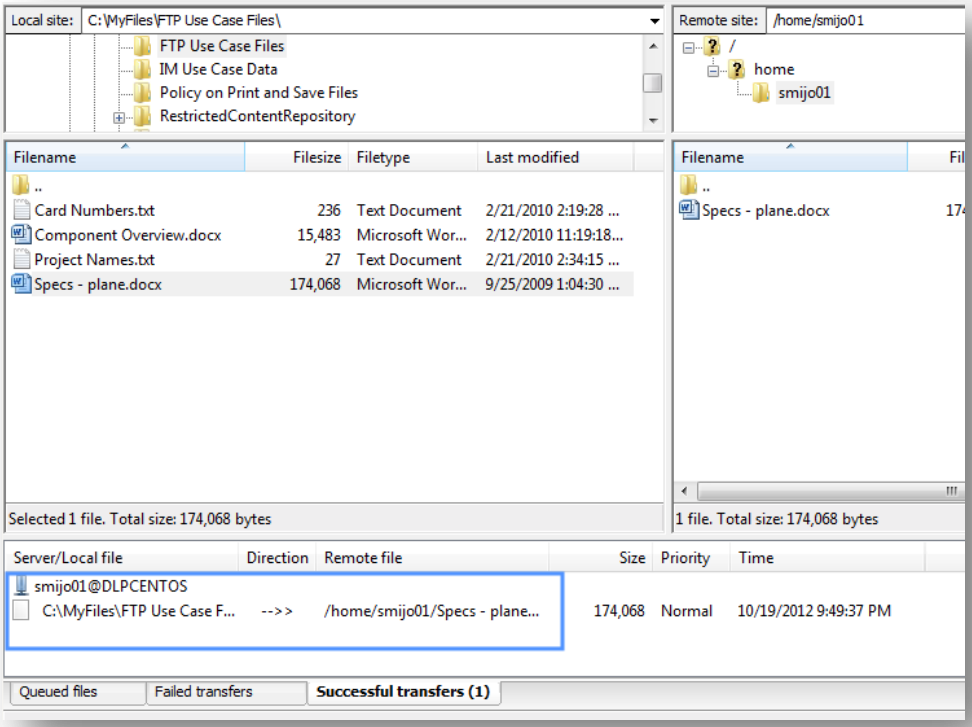


Εικόνα 4.52: Ειδοποιητικό μήνυμα. [012]

Το μήνυμα αναφέρει ότι το περιεχόμενο πλήττει τις πολιτικές της εταιρείας.

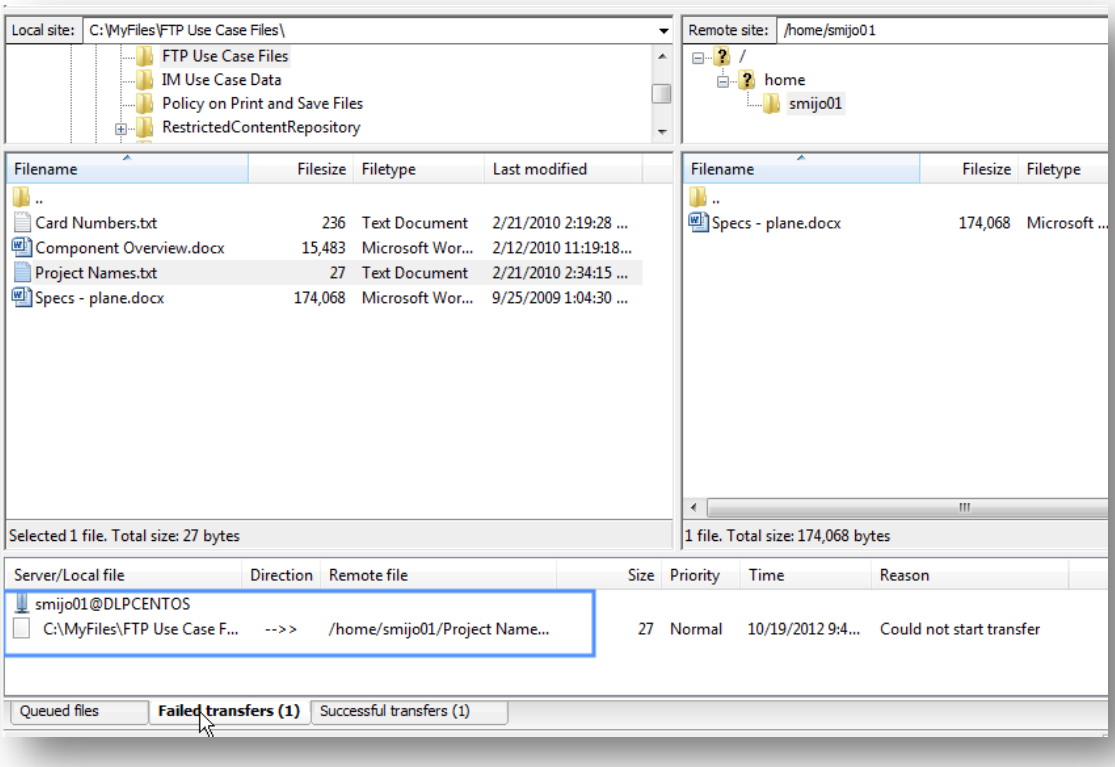
Σεναριο 5ο

Σε αυτό το σενάριο ο John Smith χρησιμοποιεί το πρωτόκολλο μεταφοράς αρχείων FTP (File Transfer Protocol) για να μεταφέρει αρχεία σε ένα εξωτερικό Διακομιστή μεταφοράς Αρχείων (FTP Server). Στην πρώτη εικόνα ο John Smith μεταφέρει το αρχείο Specs–plane.docx το οποίο περιέχει τεχνικές προδιαγραφές. Η συγκεκριμένη δραστηριότητα είναι σύμφωνη με τις ισχύουσες πολιτικές.



Εικόνα 4.53: Μεταφορά μέσω διακομιστή μεταφοράς αρχείων (FTP Server). [012]

Στο επόμενο σενάριο ο John Smith μεταφέρει το αρχείο Project Names.txt το οποίο περιέχει εμπιστευτικές πληροφορίες της εταιρείας (Company Confidential Information), οι οποίες δεν πρέπει να φύγουν εκτός οργανισμού. Το αρχείο μπλοκάρεται από τις πολιτικές που εμπεριέχονται στο εργαλείο μας CA DataMinder.



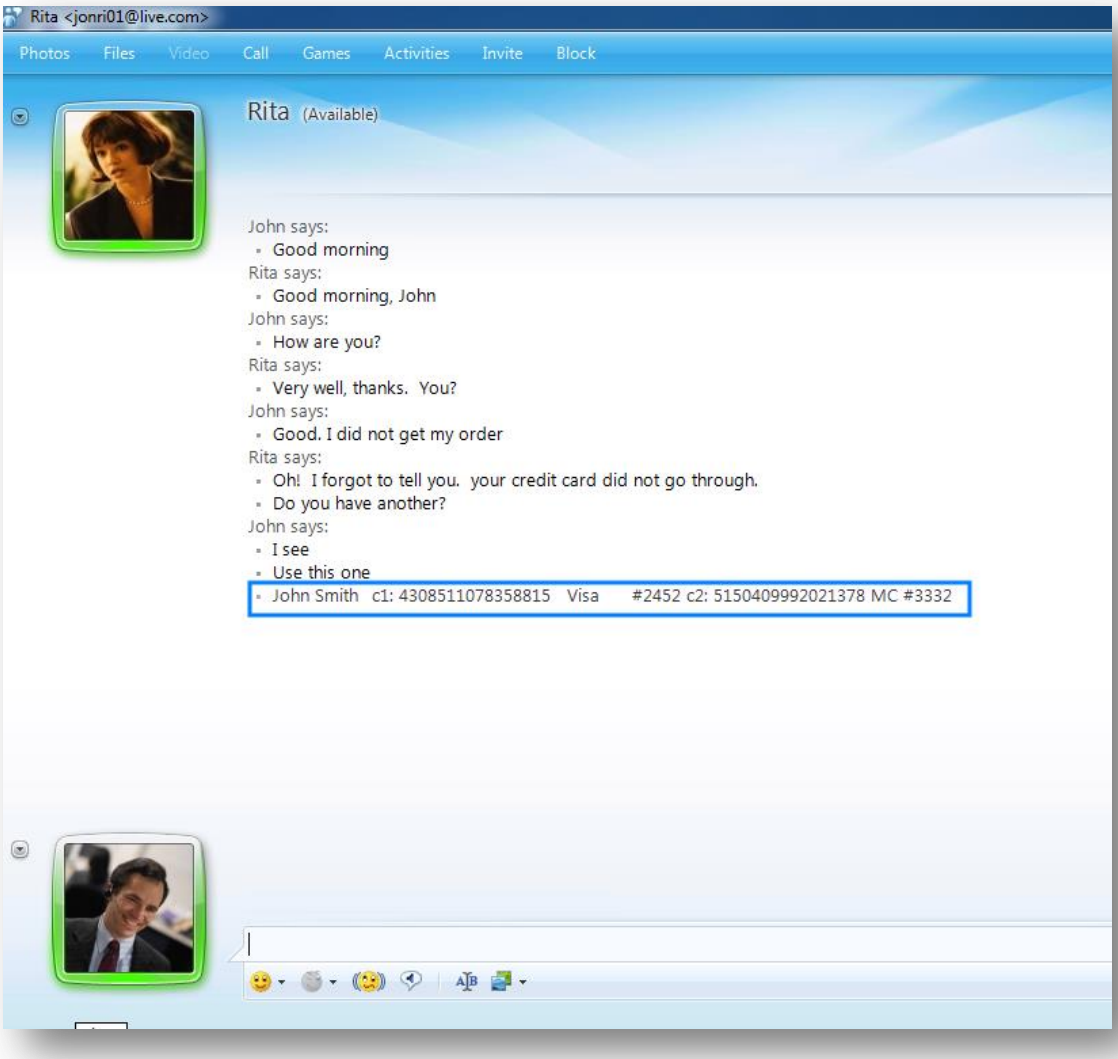
Εικόνα 4.54: Μεταφορά μέσω διακομιστή μεταφοράς αρχείων (FTP Server). [012]

Σεναριο 6ο

Σε αυτό το σενάριο περιγράφεται πώς το CA DataMinder εντοπίζει ευαίσθητα δεδομένα που πλήττουν τις πολιτικές της επιχείρησης μέσω αμέσων μηνυμάτων (Instant Message).

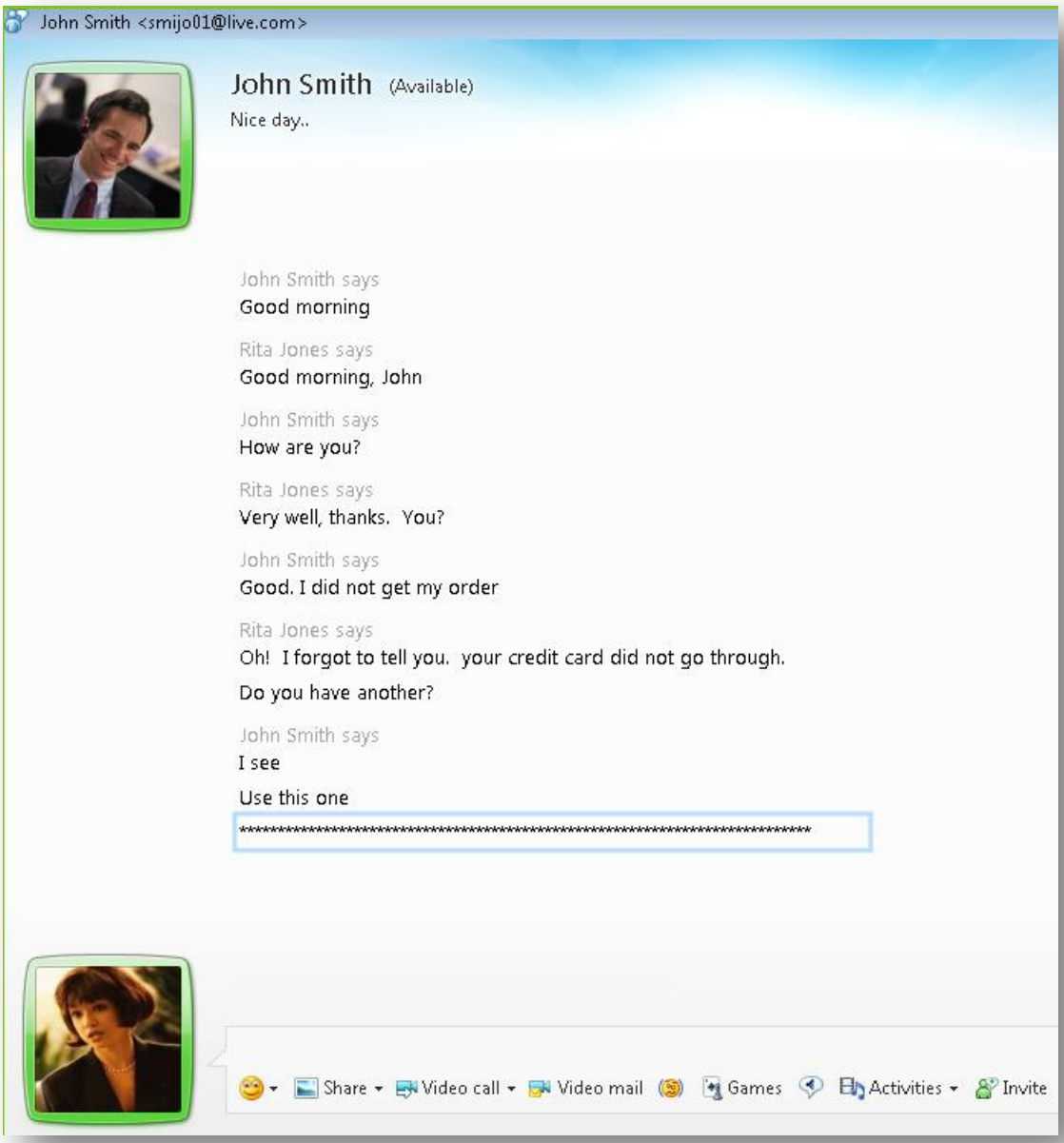
Πιο συγκεκριμένα ο υπάλληλος της εταιρείας John Smith που βρίσκεται στο δίκτυο της εταιρείας προσπαθεί να επικοινωνήσει με την Rita που βρίσκετε στο σπίτι της μέσω άμεσων μηνυμάτων (Instant Message-IM).

Η συνομιλία διεξάγεται κανονικά. Στην προσπάθεια του να στείλει αριθμούς πιστωτικών καρτών ή άλλες εμπιστευτικές πληροφορίες μέσω άμεσων μηνυμάτων, δεν διαπιστώνει κάποιο πρόβλημα και θεωρεί πως στάλθηκαν.



Εικόνα 4.55: Συνομιλία μέσω άμεσων μηνυμάτων. [012]

Όμως, το εργαλείο CA DataMinder εντόπισε ότι ο υπάλληλος επιχειρεί να στείλει εμπιστευτικές πληροφορίες. Έτσι, παρόλο που στην οθόνη συνομιλίας του υπαλλήλου φαίνεται ότι το μήνυμα έχει σταλεί κανονικά (Εικόνα 4.55), εν τούτοις ο παραλήπτης του μηνύματος δεν βλέπει τις εμπιστευτικές αυτές πληροφορίες αλλά αστερίσκους (Εικόνα 4.56).



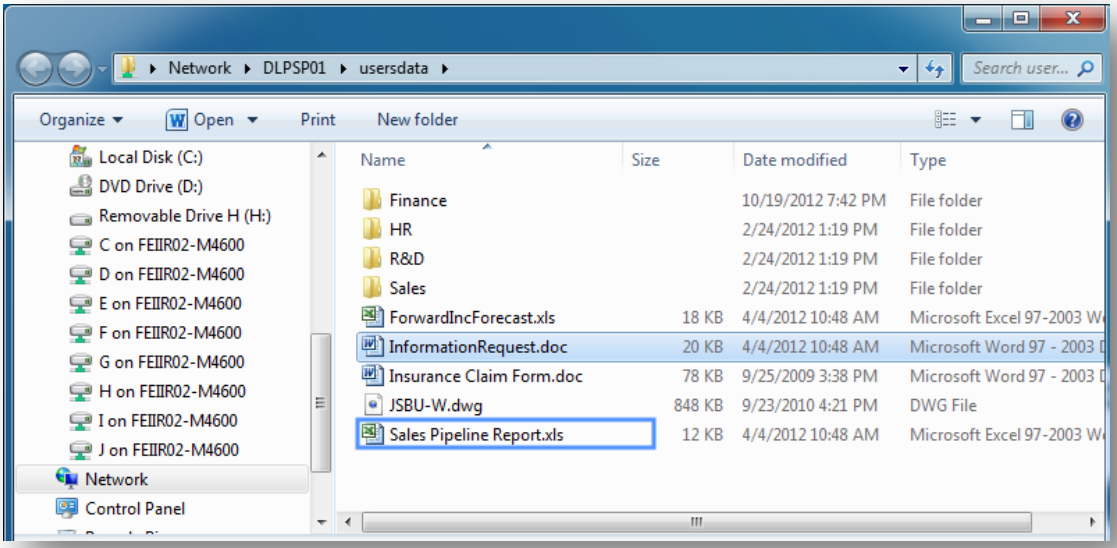
Εικόνα 4.56: Συνομιλία μέσω άμεσων μηνυμάτων. [012]

4.14.3 Δεδομένα σε Αδράνεια.

Με το όρο δεδομένα σε αδράνεια (Data at Rest) εννοούμε τοπικά αρχεία και φακέλους (Local files and folders), απομακρυσμένες συνδέσεις (remote locations) και το SharePoint .

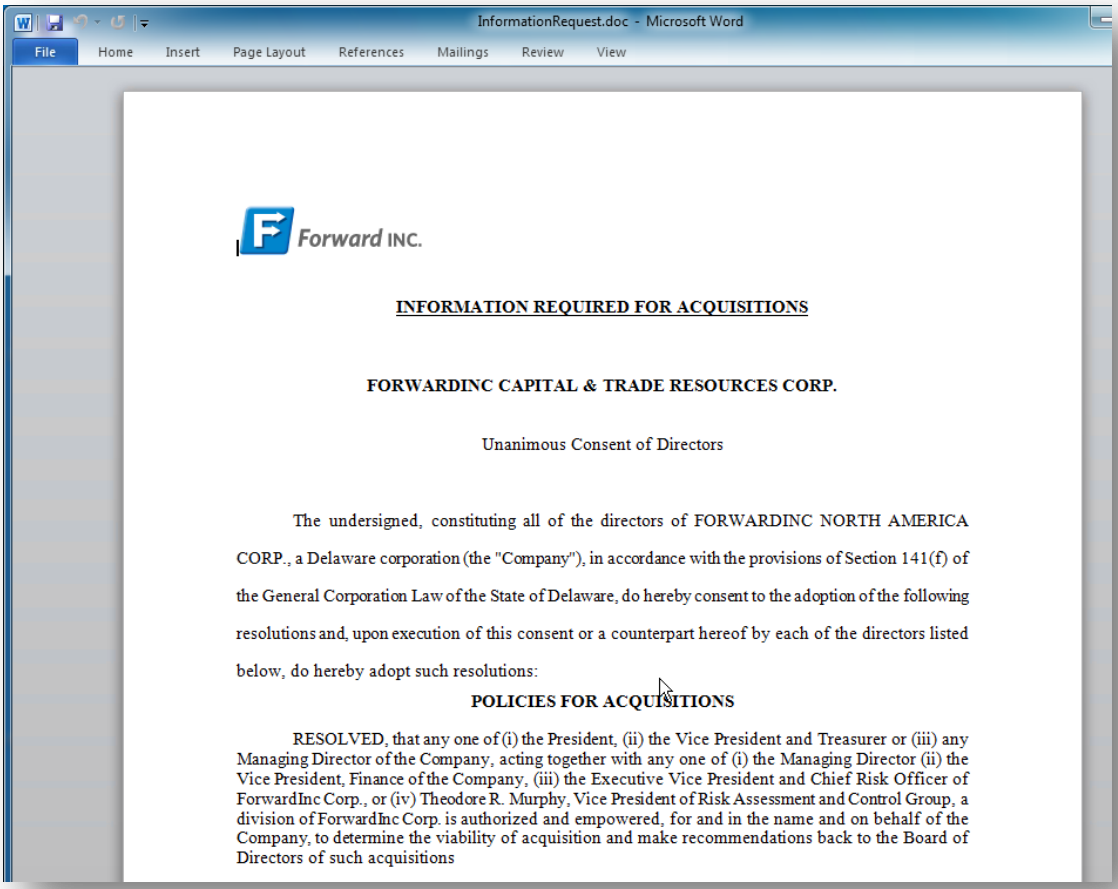
Σενάριο 1ο

Σε αυτό το σενάριο θα δούμε πώς το εργαλείο CA DataMinder προστατεύει αποθηκευμένα δεδομένα που βρίσκονται σε Διακομιστές του δικτύου και τα οποία διαμοιράζονται μέσω κοινόχρηστων φακέλων.



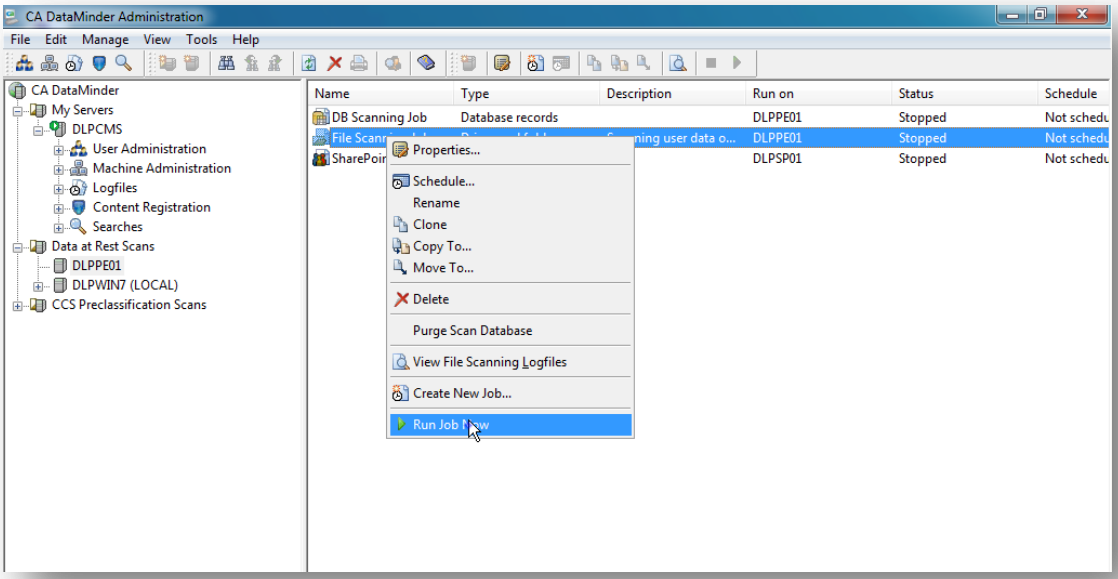
Εικόνα 4.57: Δεδομένα σε αδράνεια (Data at Rest). [012]

Μπορούμε να διακρίνουμε διάφορα αρχεία Word και Excel, όπως το ForwardForecast.xls το οποίο περιέχει οικονομικές προβλέψεις, το Insurance Claim Form.doc το οποίο περιέχει πληροφορίες σχετικά με την υγεία, και το Sales Pipeline Report.xls το οποίο περιέχει εμπιστευτικά δεδομένα σχετικά με τις πωλήσεις.



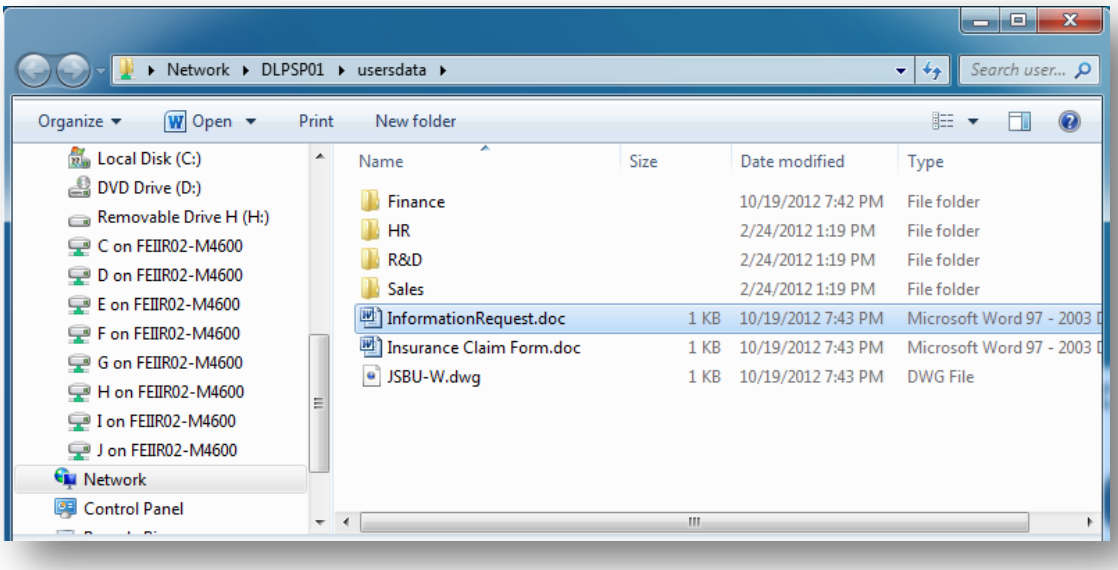
Εικόνα 4.58: Το αρχείο InformationRequest.doc. [012]

Το αρχείο InformationRequest.doc το οποίο περιέχει εμπιστευτικά δεδομένα είχε καταγραφεί στο εργαλείο CA DataMinder με την τεχνική αποτυπώματος αρχείων (Data Fingerprint), το περιεχόμενο του οποίου δεν μπορεί οποιοσδήποτε να έχει πρόσβαση.



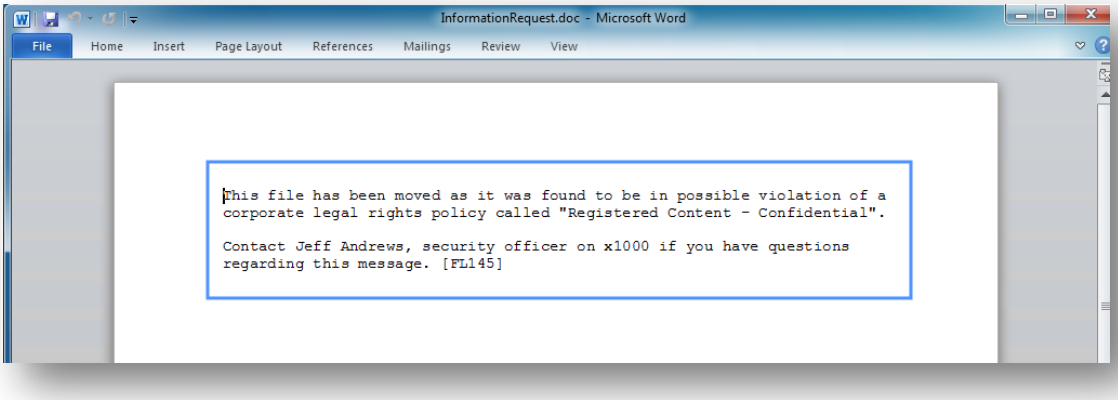
Εικόνα 4.59: CA DataMinder Administration.[012]

Ο Διαχειριστής του εργαλείου DLP μπορεί να δημιουργήσει προκαθορισμένες εβδομαδιαίες ή ημερήσιες σαρώσεις, έτσι ώστε να προστατεύονται τα πιο πάνω εμπιστευτικά δεδομένα.



Εικόνα 4.60: Δεδομένα σε αδράνεια (Data at Rest). [012]

Όπως διακρίνουμε, μετά από τη σάρωση το αρχείο με τις οικονομικές προβλέψεις έχει διαγραφεί και έχει αντικατασταθεί με το αρχείο informationRequest.doc το οποίο περιέχει το πιο κάτω μήνυμα. Το μήνυμα περιγράφει την παραβίαση της πολιτικής που έχει γίνει.



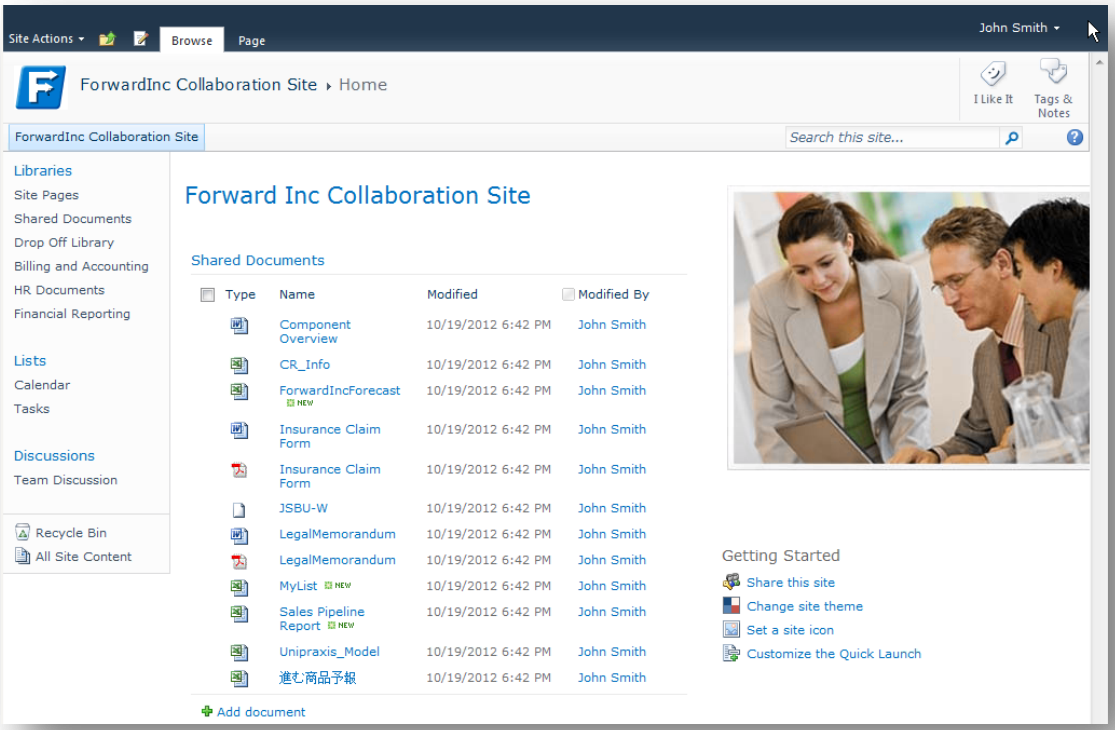
Εικόνα 4.61: Μήνυμα που περιγράφει την παραβίαση της πολιτικής. [012]

Η ασφαλής τοποθεσία δικτύου περιέχει όλα τα αυθεντικά αρχεία.

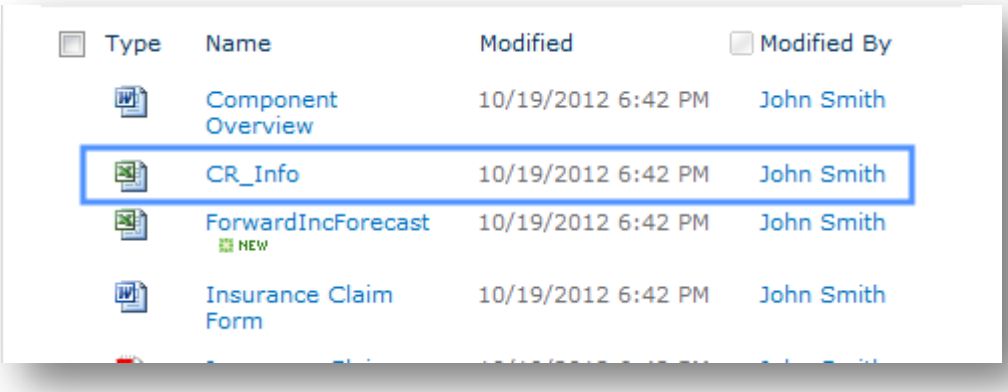
Σεναριο 2ο

Σε αυτό το σενάριο θα δούμε πως το εργαλείο CA DataMinder ανακαλύπτει και ελέγχει αποθηκευμένα δεδομένα στο SharePoint.

Στην πιο κάτω εικόνα διακρίνονται τα αρχεία που βρίσκονται στο SharePoint.

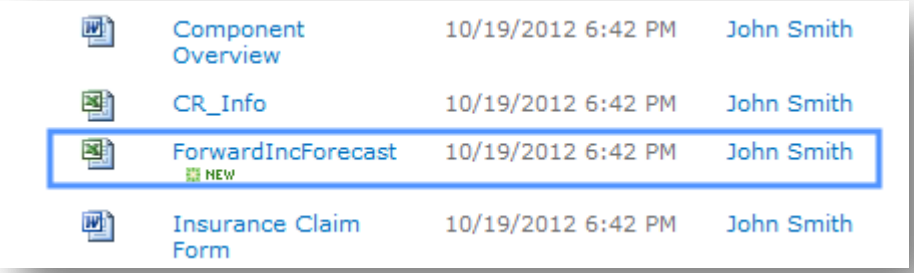


Εικόνα 4.62: Αρχεία που βρίσκονται στο SharePoint. [012]



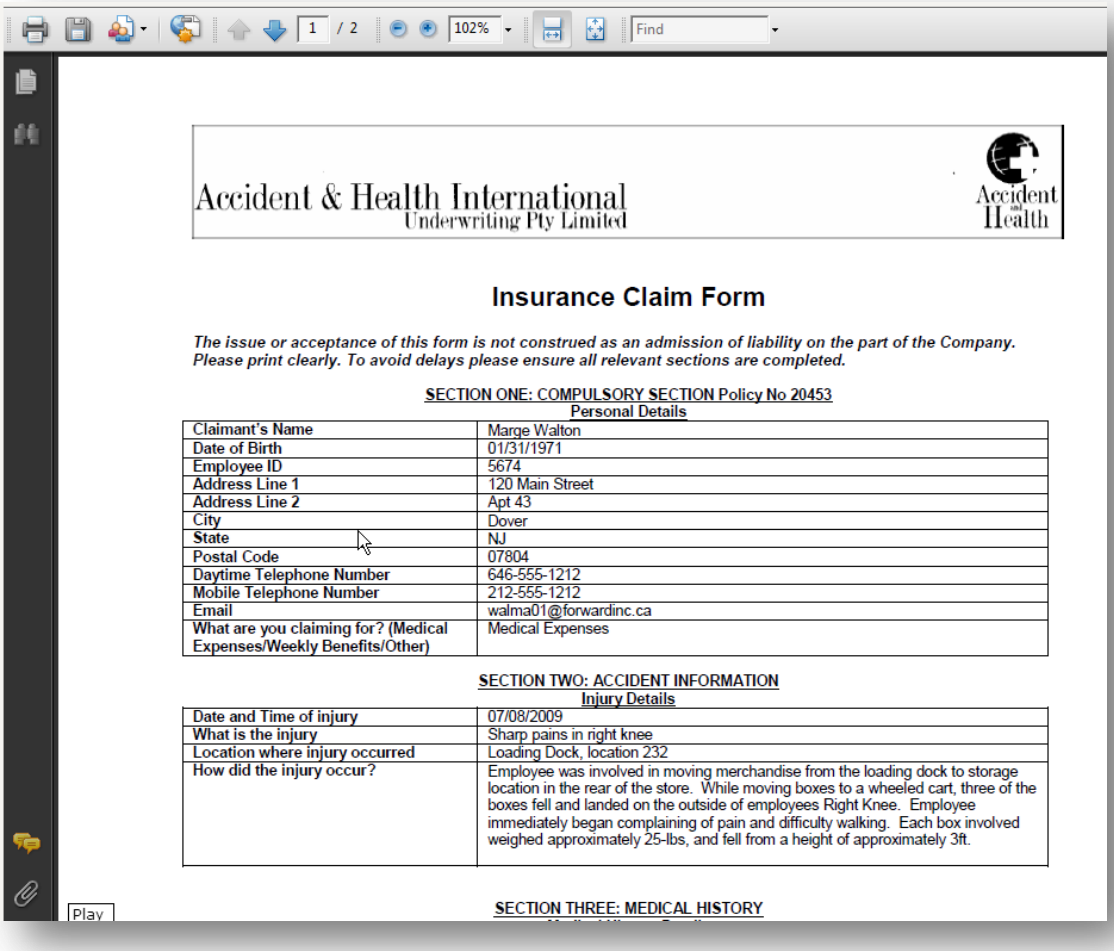
Εικόνα 4.63: Το αρχείο CR_Info.xlsx. [012]

Το αρχείο CR_info.xls περιέχει πληροφορίες από πιστωτικές κάρτες (credit card information).



Εικόνα 4.64: Το αρχείο ForwardIncForecast.xlsx. [012]

Το αρχείο ForwardIncForecast.xls περιέχει οικονομικές προβλέψεις.



Accident & Health International
Underwriting Pty Limited

Accident and Health

Insurance Claim Form

The issue or acceptance of this form is not construed as an admission of liability on the part of the Company. Please print clearly. To avoid delays please ensure all relevant sections are completed.

SECTION ONE: COMPULSORY SECTION Policy No 20453
Personal Details

Claimant's Name	Marge Walton
Date of Birth	01/31/1971
Employee ID	5674
Address Line 1	120 Main Street
Address Line 2	Apt 43
City	Dover
State	NJ
Postal Code	07804
Daytime Telephone Number	646-555-1212
Mobile Telephone Number	212-555-1212
Email	walma01@forwardinc.ca
What are you claiming for? (Medical Expenses/Weekly Benefits/Other)	Medical Expenses

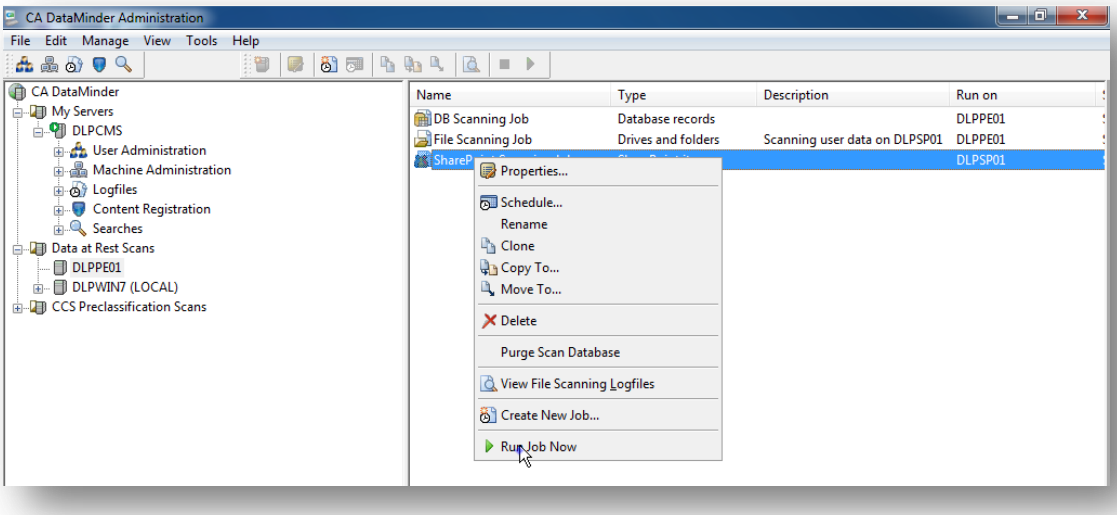
SECTION TWO: ACCIDENT INFORMATION
Injury Details

Date and Time of injury	07/08/2009
What is the injury	Sharp pains in right knee
Location where injury occurred	Loading Dock, location 232
How did the injury occur?	Employee was involved in moving merchandise from the loading dock to storage location in the rear of the store. While moving boxes to a wheeled cart, three of the boxes fell and landed on the outside of employees Right Knee. Employee immediately began complaining of pain and difficulty walking. Each box involved weighed approximately 25-lbs, and fell from a height of approximately 3ft.

SECTION THREE: MEDICAL HISTORY

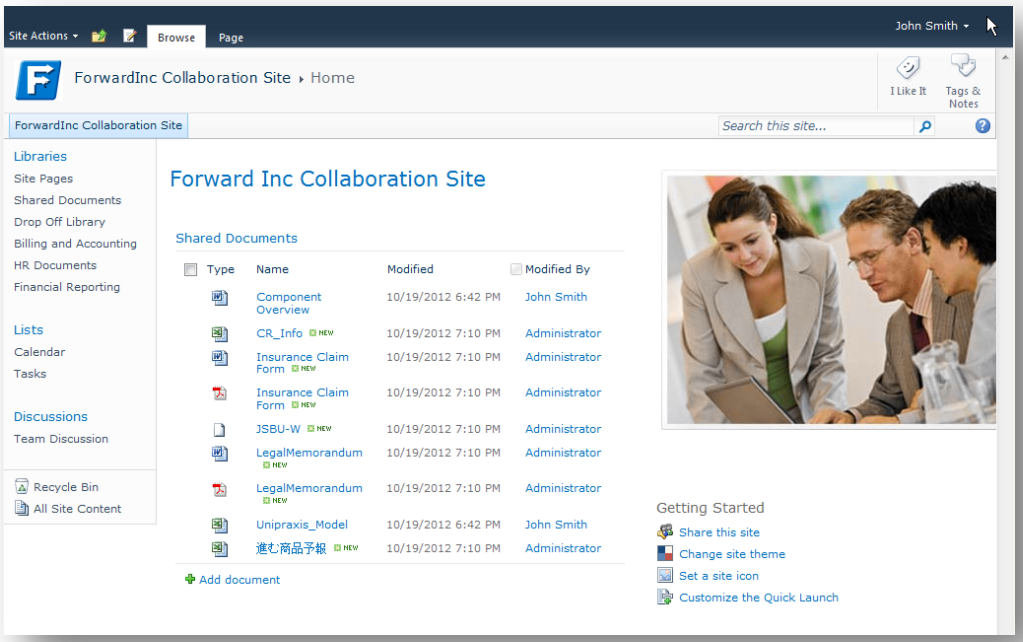
Εικόνα 4.65: Το αρχείο Insurance Claim Form.pdf[012]

Το αρχείο Insurance Claim Form.pdf περιέχει πληροφορίες σχετικά με την υγεία των πελατών. Αυτά τα αρχεία, καθώς και πολλά άλλα, δεν θα πρέπει να είναι αποθηκευμένα σε κοινόχρηστες περιοχές.



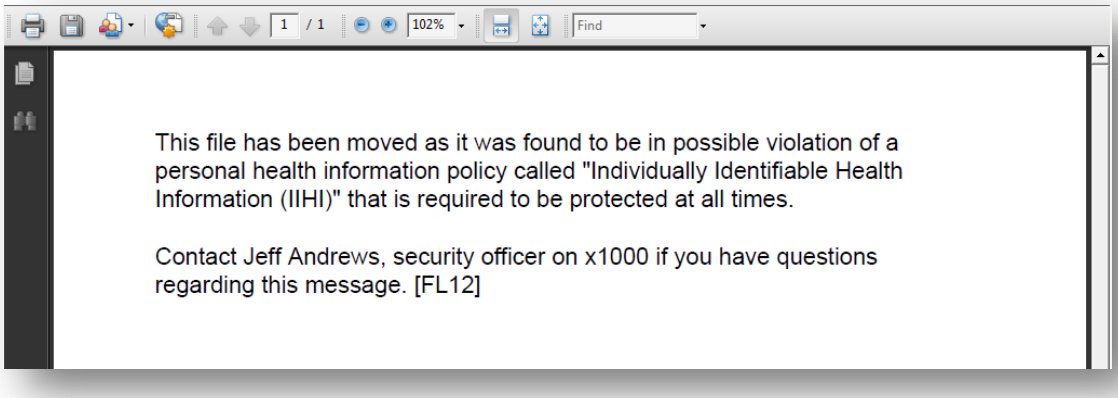
Εικόνα 4.66: CA DataMinder Administration. [012]

Ο Διαχειριστής του εργαλείου DLP μπορεί να δημιουργήσει προκαθορισμένες εβδομαδιαίες ή ημερήσιες σαρώσεις, έτσι ώστε να προστατεύονται τα πιο πάνω εμπιστευτικά δεδομένα.



Εικόνα 4.67: Αρχεία που βρίσκονται στο SharePoint. [012]

Όπως διακρίνουμε το αρχείο με τις πληροφορίες σχετικά με την υγεία των πελατών έχει διαγραφεί και έχει αντικατασταθεί με το αρχείο Insurance Claim Form το οποίο περιέχει το πιο κάτω μήνυμα. Το μήνυμα περιγράφει την παραβίαση της πολιτικής που έχει γίνει. [012]



Εικόνα 4.68: Μήνυμα που περιγράφει την παραβίαση της πολιτικής. [012]

Κεφάλαιο 5
Ζητήματα Ιδιωτικότητας

Στο παρόν κεφάλαιο θα μελετήσουμε τα εργαλεία Αποτροπής Απώλειας Δεδομένων ως προς την ιδιωτικότητα. Παρόλο που με την τεχνολογία Αποτροπής Απώλειας Δεδομένων σε ένα Οργανισμό θέλουμε να προστατεύουμε τον Οργανισμό από τυχόν διαρροή, εκούσια ή ακουσία, εμπιστευτικών δεδομένων, εν τούτοις ελλοχεύει ο κίνδυνος να παραβιαστεί η ιδιωτικότητα των υπάλληλων του οργανισμού. Ως εκ τούτου, μία βέλτιστη προσέγγιση είναι αυτή η οποία βρίσκει, κατά το δυνατόν, την ισορροπία μεταξύ συμφερόντων του οργανισμού και της ιδιωτικής ζωής των εργαζομένων.

5.1 Τι εννοούμε με το όρο ιδιωτικότητα

Η Ιδιωτικότητα (Privacy), στενά συνυφασμένη με την προστασία προσωπικών δεδομένων, αποτελεί ένα θεμελιώδες δικαίωμα του καθενός (σύμφωνα και με το Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης). Ουσιαστικά, με τον όρο ιδιωτικότητα αναφερόμαστε στην επιθυμία ενός ατόμου να ελέγχει την αποκάλυψη των προσωπικών του πληροφοριών.

Ειδικότερα, βάσει του ορισμού του Alan F.Westin, η ιδιωτικότητα ορίζεται ως εξής: "Η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν για τον εαυτό τους πότε, πώς και σε ποιο ακριβώς βαθμό οι πληροφορίες για τα άτομά τους γνωστοποιούνται στους υπόλοιπους με τους οποίους επικοινωνούν". Έχουν ωστόσο διατυπωθεί και άλλοι ορισμοί: για παράδειγμα, οι Αμερικανοί δικαστές Warren και Brandeis όρισαν την Ιδιωτικότητα ως «το δικαίωμα του ατόμου σε μια ανενόχλητη ιδιωτική ζωή (the right to be let alone)». [114]

Η Ιδιωτικότητα ως ορισμός στην σύγχρονη εποχή με τις τεχνολογικές προκλήσεις και εξελίξεις, έχει εμπλουτιστεί με επιμέρους δικαιώματα, όπως το δικαίωμα σε ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, αποκλειστικός έλεγχος της πρόσβασης στο ιδιωτικό χώρο (ή άσυλο κατοικίας), η ελαχιστοποίηση των παρεμβάσεων (intrusiveness), η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της ανωνυμίας και της απόσυρσης.

Ωστόσο, οι ραγδαίες εξελίξεις της τεχνολογίας της Πληροφορικής μέσω της μεγάλης κλίμακας Πληροφοριακών Συστημάτων και της δυνατότητας συγκέντρωσης αποθήκευσης και επεξεργασίας μεγάλου όγκου Δεδομένων μέσω Βάσεων Δεδομένων και Διαδικτύου γεννούν αρνητικές επιπτώσεις σε θέματα ιδιωτικότητας. Το πρόβλημα επιτείνεται από τη χρήση των μέσων κοινωνικής δικτύωσης (Social Media), της νεφοϋπολογιστικής (Cloud Computing), καθώς και των ασύρματων κινητών συσκευών.

Υπάρχει στέρεο νομικό υπόβαθρο σε όλα τα Κράτη Μέλη της Ευρωπαϊκής Ένωσης αναφορικά με την προστασία των προσωπικών δεδομένων. Ως εκ τούτου, έχουν πλήρως προσδιοριστεί βασικές αρχές για τη νομιμότητα της επεξεργασίας, ενώ σε κάθε Κράτος Μέλος υπάρχει Αρχή που είναι υπεύθυνη για τον έλεγχο της συμμόρφωσης με το νομικό αυτό πλαίσιο. Παρόλα αυτά, η εξέλιξη της τεχνολογίας δημιουργεί κινδύνους παραβίασης των προσωπικών δεδομένων, κάτι το οποίο πρέπει πάντοτε να λαμβάνεται υπόψη κατά την ανάπτυξη τεχνολογικών προϊόντων ή υπηρεσιών. Η λεγόμενη αρχή της ιδιωτικότητας κατά τη σχεδίαση (Privacy-by-Design) πρέπει να αποτελεί οδηγό κατά την ανάπτυξη οποιουδήποτε τεχνολογικού προϊόντος, έτσι ώστε από τα πρώτα στάδια υλοποίησής του να λαμβάνεται μέριμνα ώστε να μην καταστρατηγείται η νομοθεσία περί προστασίας προσωπικών δεδομένων.[113]

Τα ανωτέρω ισχύουν και για τις τεχνολογίες Αποτροπής Απώλειας Δεδομένων: με βάση την αρχή της ιδιωτικότητας κατά τη σχεδίαση, ο κατασκευαστής ενός εργαλείου Αποτροπής Απώλειας Δεδομένων πρέπει να έχει κατά νου τα θέματα ασφαλείας όπως η Ιδιωτικότητα και η

Προστασία των Δεδομένων σε ολόκληρο το κύκλο ζωής (Life Cycle) της κατασκευής της τεχνολογίας. Με άλλα λόγια, πρέπει από τα πρώτα στάδια του σχεδιασμού για την ανάπτυξη ενός Εργαλείου Αποτροπής Απώλειας Δεδομένων μέχρι την χρήση και την τελική διάθεση του προϊόντος του να έχει ενσωματωμένα στα πλάνα του τα θέματα ιδιωτικότητας. Στο παρόν κεφάλαιο εστιάζουμε σε αυτό ακριβώς το ζήτημα.[023, 039, 040, 052, 103, 108, 113, 114, 116, 126, 129]

5.2 Κατηγοριοποίηση των Δεδομένων

Τα δεδομένα αποτελούν ένα πολύ κρίσιμο αγαθό που χρήζουν ιδιαίτερης προστασίας. Αναλόγως της φύσης τους, αλλά και στο περιβάλλον στο οποίο εντάσσονται, διακρίνονται σε κατηγορίες:

α) **Εμπιστευτικά δεδομένα** (Confidential data) είναι οποιαδήποτε δεδομένα τα οποία ένας οργανισμός επιθυμεί να προστατεύει. [137]

β) **Προσωπικά δεδομένα** (Personal data) είναι κάθε πληροφορία (άμεση ή έμμεση) που αναφέρεται σε φυσικό πρόσωπο και χαρακτηρίζει το υποκείμενο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη . Με απλά λόγια, οποιαδήποτε πληροφορία αναφορικά με το άτομο θεωρείται εν γένει προσωπικό του δεδομένο.

Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία. [137]

γ) **Ευαίσθητα δεδομένα** (Sensitive data). είναι τα προσωπικά δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, υγεία, κοινωνική πρόνοια, ερωτική ζωή, ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα παραπάνω ενώσεις. Ουσιαστικά είναι προσωπικά δεδομένα τα οποία, λόγω της φύσης τους, εμπίπτουν στο σκληρό πυρήνα της ιδιωτικότητας και χρήζουν ακόμα μεγαλύτερης προστασίας (προβλέπεται στους σχετικούς νόμους).

Τα προσωπικά δεδομένα, τα οποία δεν είναι ευαίσθητα (π.χ. το ονοματεπώνυμο ή το τηλέφωνο κάποιου), είθισται να χαρακτηρίζονται ως απλά προσωπικά δεδομένα. [137]

5.3 Παρακολούθηση στο χώρο εργασίας και Νομικό Πλαίσιο

Η παρακολούθηση στο χώρο εργασίας στην Ευρωπαϊκή Ένωση διέπεται από διάφορους νόμους περί ιδιωτικότητας (Privacy Laws), Κανόνες (Rules) και Κανονισμούς (Regulations).

Η προστασία της ιδιωτικής ζωής θεμελιώνεται στο Ευρωπαϊκό Δίκαιο.: ήδη από το 1950 η αναγνωρίζεται ως δικαίωμα με το **άρθρο 8** της Ευρωπαϊκής Σύμβασης για την προστασία των ανθρωπίνων δικαιωμάτων, η όποια αναφέρει «Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του» [144]**.** Το 1981 το Συμβούλιο της Ευρώπης με τη **Σύμβαση 108** για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Προσωπικών Δεδομένων, αναφέρει ότι «Οι πληροφορίες προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή άλλες πεποιθήσεις, όπως και οι πληροφορίες προσωπικού χαρακτήρα που σχετίζονται με την υγεία ή την σεξουαλική ζωή, δεν δύνανται να αποτελέσουν αντικείμενο αυτοματοποιημένης επεξεργασίας, εάν το εσωτερικό δίκαιο δεν προβλέπει κατάλληλες εγγυήσεις. Το αυτό ισχύει για τις πληροφορίες προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες» [145]**.** Το 1992 η **Συνθήκη** για τη λειτουργία της ευρωπαϊκής Ένωσης απαιτεί από τα κράτη μέλη να σέβονται τα θεμελιώδη δικαιώματα που εγγυάται η Ευρωπαϊκή Σύμβαση.

Η Ευρωπαϊκή Νομοθεσία για την προστασία των ανθρωπίνων δικαιωμάτων ορίζεται από την **οδηγία 95/46/ΕΚ** του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. [141] Ειδικότερα θέματα ρυθμίζονται με την **Οδηγία 2002/58/ΕΚ** αναφορικά με την προστασία των φυσικών προσώπων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, η οποία με τη σειρά της τροποποιήθηκε πιο πρόσφατα από την Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009.[131, 134]

Όλα τα κράτη μέλη έχουν ενσωματώσει την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου στην δική τους έννομη τάξη. Συνεπώς, σε όλα τα κράτη μέλη υπάρχει σε γενικές γραμμές ένα κοινό νομικό πλαίσιο (με μικρές επιμέρους διαφορές).[141] Η Κύπρος έχει ενσωματώσει την οδηγία με τους Νόμους 138(Ι) του 2001, 37(Ι) του 2003 και 105(Ι)/2012 -

Ανεπίσημη Ενοποίηση Ανεπίσημη Ενοποίηση του Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001, αρ. 138(I)/2001, όπως έχει τροποποιηθεί.[138] Και με τον Κυρωτικός Νόμος αρ. 30(III) του 2003 Ε.Ε. Παρ I(III) Αρ. 3732, 4.7.2003 Ο Περί Πρόσθετου Πρωτόκολλου στη Σύμβαση για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα Κυρωτικός Νόμος του 2003, αρ. 30(III)/2003.[130]

Η αρμόδια υπηρεσία για προστασία των προσωπικών δεδομένων στην Κύπρο είναι το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Office of the Commissioner for Personal Data Protection).[130]

Η δε Ελλάδα (Greece) έχει ενσωματώσει την οδηγία με το ν. 2472/1997 για την προστασία του Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα.[139]. Η Οδηγία 2002/58/ΕΚ έχει ενσωματωθεί με το ν. 3471/2006[141]. Η αρμόδια αρχή για προστασία των προσωπικών δεδομένων στην Ελλάδα είναι το Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Hellenic Data Protection Authority) [124].

Στο άρθρο 29 της Οδηγίας 95/46/ΕΚ προβλέπεται η θέσπιση ειδικής συμβουλευτικής ομάδας ομάδας, απαρτιζόμενης από εκπροσώπους των αρχών προστασίας των δεδομένων των κρατών μελών, η οποία ενεργεί ανεξάρτητα και είναι επιφορτισμένη, μεταξύ άλλων, με την εξέταση κάθε ζητήματος το οποίο καλύπτει την εφαρμογή των εθνικών μέτρων που θεσπίστηκαν βάσει της οδηγίας 95/46/ΕΚ, προκειμένου να συμβάλει στην ομοιόμορφη εφαρμογή των εν λόγων μέτρων [141]. Η Ομάδα αυτή, γνωστή και ως Ομάδα Εργασίας **του άρθρου 29** (Article 29 Working Party) εκδίδει διάφορες γνώμες για κρίσιμα ζητήματα που προκύπτουν από διαφόρου τύπου επεξεργασίες προσωπικών δεδομένων. [007, 050, 123]

Πέραν των εθνικών αρχών και της Ομάδας Εργασίας του Άρθρου 29, υπάρχουν και άλλα ευρωπαϊκά όργανα επιφορτισμένα με αρμοδιότητες που άπτονται της προστασίας προσωπικών δεδομένων. Ο **Ευρωπαίος Επόπτης Προστασίας Δεδομένων** (European Data Protection Supervisor) είναι ανεξάρτητη εποπτική Αρχή η οποία είναι αρμόδια για την παρακολούθηση της εφαρμογής στα όργανα και τους οργανισμούς της Κοινότητας των κοινοτικών πράξεων που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (Κανονισμός 45/2001/ΕΚ).[132] Περαιτέρω, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Network and Information Security Agency - ENISA), δημιουργήθηκε για να ενδυναμώσει τη δυνατότητα της Ευρωπαϊκής

Ένωσης, των Κρατών μελών της Ε.Ε. και της επαγγελματικής κοινότητας να αποφεύγει, να διευθύνει και να ανταποκρίνεται σε προβλήματα που αφορούν την ασφάλεια των δικτύων και πληροφοριών. [031, 050]

5.4 Καλές πρακτικές για εφαρμογή DLP

Με τα Εργαλεία Αποτροπής Απώλειας Δεδομένων εκτελείται παρακολούθηση των δεδομένων ενός οργανισμού. Προφανώς, η σάρωση του περιεχομένου των αρχείων έχει εκ των πραγμάτων ως αποτέλεσμα την παραβίαση του θεμελιώδους δικαιώματος της ιδιωτικότητας. Ως εκ τούτου, οι Οργανισμοί θα πρέπει να βρουν κάποιες πρακτικές έτσι ώστε να περιορίσουν την παραβίαση της ιδιωτικότητας των υπαλλήλων χωρίς να πλήττουν και να θέτουν σε κίνδυνο τον οργανισμό.

Ιστορικά, οι εργοδότες έχουν ισχυριστεί πολλούς λόγους για τους οποίους επιθυμούν ηλεκτρονική παρακολούθηση. Μερικοί από τους λόγους είναι:

- Η παρακολούθηση της παραγωγικότητας των εργαζομένων στο χώρο εργασίας.

- Η προστασία από την μη εξουσιοδοτημένη χρήση, αποκάλυψη ή μεταφορά εμπιστευτικών δεδομένων, πληροφορίες που αφορούν τους εργαζομένους και πληροφορίες που αφορούν τους πελάτες.

- Η μεγιστοποίηση της παραγωγικής χρήσης των συστημάτων πληροφορικής του οργανισμού.

- Η παρακολούθηση της συμμόρφωσης των εργαζομένων με τις πολιτικές του οργανισμού που σχετίζονται με τη χρήση των συστημάτων πληροφορικής, σύστημα ηλεκτρονικού ταχυδρομείου και την πρόσβαση στο διαδίκτυο.

- Η αποφυγή της βιομηχανικής κατασκοπίας, όπως η κλοπή των εμπορικών μυστικών, παραβίαση πνευματικών δικαιωμάτων. [023]

Υπάρχουν κάποιες γενικές αρχές για την παρακολούθηση στο χώρο εργασίας όπως έχουν καθοριστεί από την προαναφερθείσα Ομάδα Εργασίας του άρθρου 29. Οι αρχές αυτές αποτελούν και τον οδηγό για τα διάφορα κράτη-μέλη και τις εθνικές αρχές προστασίας προσωπικών δεδομένων. Για παράδειγμα, η ελληνική Προστασίας Προσωπικών Δεδομένων έχει

εκδώσει μια απόφαση σχετικά με την παρακολούθηση στο χώρο εργασίας (αρ. 61/2004)., αναφορικά με χρήση προγράμματος απομακρυσμένης σύνδεσης σε υπολογιστές εργαζομένων. [007, 023, 050, 123]

Γενικότερα, η ομάδα εργασίας του άρθρου 29 έχει επισημάνει ότι ο εργαζόμενος δεν χάνει το δικαίωμα της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων κάθε πρωί στην είσοδο του τόπου εργασίας. Εξυπακούεται ότι οι νόμοι των χωρών περί ιδιωτικότητας και προστασίας προσωπικών δεδομένων εφαρμόζονται στην παρακολούθηση στο εργασιακό χώρο (Workplace monitoring).[007, 050, 123]

Εν τούτοις, κάθε περιορισμός του δικαιώματος του εργαζομένου στην ιδιωτική του ζωή πρέπει να είναι ανάλογη με την πιθανή ζημία ή βλάβη που μπορούν να προκαλέσουν οι ενέργειες των εργαζομένων, η αντίθετα η παρακολούθηση θα πρέπει να είναι ανάλογη προς τους κινδύνους που αντιμετωπίζει ο οργανισμός. Το σαφέστερο παράδειγμα γι αυτό είναι οι περιπτώσεις όπου ο εργοδότης είναι θύμα εγκληματικής πράξης ενός εργαζομένου.

Προσπαθώντας να αποτυπώσουμε, τις γενικές αρχές προστασίας προσωπικών δεδομένων, στην περίπτωση χρήσης συστημάτων DLP, θα αναφέρουμε τα κάτωθι βασικά χαρακτηριστικά:

1. Οι εργοδότες θα πρέπει να είναι ξεκάθαροι σχετικά με το σκοπό της παρακολούθησης, ο οποίος θα πρέπει να είναι νόμιμος και θεμιτός. **Ο προσδιορισμός του σκοπού για την παρακολούθηση** είναι απαραίτητος, προκειμένου να διαπραγματευτεί ο εργοδότης με τους εργαζομένους , τα εργατικά συμβούλια (Works Councils) και τις Αρχές Προστασίας Δεδομένων (Data Protection Authorities).

   Προκειμένου για ένα εργοδότη να κρίνει κατά πόσο η παρακολούθηση αποτελεί ανάλογη απάντηση στο πρόβλημα που επιδιώκει να αντιμετωπίσει, θα πρέπει να εξετάσει μια σειρά από ορισμένους παράγοντες όπως:

   - Πρέπει να γίνει προσδιορισμός με σαφήνεια των λόγων για τους οποίους γίνεται η παρακολούθηση και τα οφέλη που είναι πιθανό να έχουμε από την παρακολούθηση.

   - Πρέπει να γίνει εντοπισμός των πιθανών δυσμενών επιπτώσεων από την παρακολούθηση.

- Πρέπει να ληφθούν υπόψη εναλλακτικές λύσεις για παρακολούθηση ή διαφορετικοί τρόποι με τους οποίους θα μπορούσε αυτή να πραγματοποιηθεί.

- Πρέπει να ληφθούν υπόψη οι υποχρεώσεις που απορρέουν από το υπάρχον νομικό πλαίσιο.

- Πρέπει να κρίνει εάν η παρακολούθηση είναι δικαιολογημένη.

2. Οι εργαζόμενοι θα πρέπει να γνωρίζουν τη φύση, την έκταση και τους λόγους για τους οποίους γίνεται η παρακολούθηση (εκτός από εξαιρετικές περιπτώσεις περιστάσεις όπου η μυστική παρακολούθηση είναι δικαιολογημένη). Όλα τα μέτρα παρακολούθησης θα πρέπει να είναι απολύτως διάφανα για τους εργαζομένους.

3. Όλα τα προσωπικά στοιχεία που συλλέγονται κατά την διάρκεια της παρακολούθησης στο εργασιακό περιβάλλον πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με το σκοπό για τον οποίον δικαιολογείται η παρακολούθηση. Κάθε παρακολούθηση πρέπει να εκτελείται με το λιγότερο δυνατό παρεμβατικό τρόπο. Σε κάθε περίπτωση, πρέπει να εφαρμόζονται οι γενικές αρχές της οδηγίας 95/46/ΕΚ σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων, συμπεριλαμβανομένης της παρακολούθησης στο χώρο εργασίας.

   Κατά συνέπεια και το Εργαλείο Αποτροπής Απώλειας Δεδομένων θα πρέπει να επεξεργάζεται όσο γίνεται λιγότερα δεδομένα εν όψη του επιδιωκόμενου σκοπού του. Αυτό με τη σειρά του συνεπάγεται ότι θα πρέπει να παράγονται όσο γίνεται λιγότερες ψευδώς θετικές ειδοποιήσεις.

4. Είναι εξίσου σημαντικό για τον οργανισμό και τους εργοδότες να κατανοήσουν την τεχνολογία που έχουν επιλέξει για παρακολούθηση και να είναι σε θέση να την εξηγήσουν στους εργαζομένους ή ακόμα σε εκπροσώπους τους (πχ. συνδικαλιστικές οργανώσεις). Δεν πρέπει να αγνοηθεί το γεγονός ότι σε πολλές περιπτώσεις οι εργαζόμενοι έχουν δικαίωμα να συμμετέχουν σε αποφάσεις που επηρεάζουν τις συνθήκες εργασίας. Επιπλέον, μπορεί να είναι αναγκαίο να προβεί ο οργανισμός σε εξηγήσεις προς στις αρμόδιες αρχές προστασίας δεδομένων όπως είναι το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού χαρακτήρα που είναι υπεύθυνο για στην Κύπρο.

5. Ο οργανισμός πρέπει να διαβουλευτεί με τους εργαζομένους σχετικά με το σκοπό τον οποίο γίνεται η παρακολούθηση, το τρόπο παρακολούθησης, τι συμβαίνει κατά την παρακολούθηση και τι θα γίνει σχετικά με τις πληροφορίες που συλλέγονται κατά την παρακολούθηση. Επίσης, ο οργανισμός θα πρέπει να είναι προετοιμασμένος να εξηγήσει γιατί αυτό δεν μπορεί να επιτευχθεί με άλλα μέσα εκτός από ην αυτόματη παρακολούθηση.

6. Έχει ουσιαστική σημασία να πληροφορεί ο εργοδότης τον εργαζόμενο για την παρουσία, τη χρήση και το σκοπό οποιουδήποτε εξοπλισμού ανίχνευσης, ακόμα και κατά το στάδιο λειτουργίας ενός συστήματος DLP. Η άμεση πληροφόρηση μπορεί να επιτευχθεί εύκολα με λογισμικό όπως τα προειδοποιητικά παράθυρα που ανοίγουν και προειδοποιούν τον εργαζόμενο ότι το σύστημα ανιχνεύει μια μη επιτρεπόμενη χρήση του δικτύου η/και έλαβε μέτρα για την πρόληψη της. [007, 050, 123]

7. Επίσης, πρέπει να προσδιοριστεί το άτομο εντός του οργανισμού (System DLP Administrator) όπου μπορεί να παρακολουθεί τους εργαζόμενους και να διασφαλίζει ότι έχουν επίγνωση των ευθυνών τους. Η Ομάδα Εργασίας του Άρθρου 29 εφιστά την προσοχή στο ρόλο του διαχειριστή του συστήματος, που είναι ένας εργαζόμενος ο οποίος κατέχει σημαντικές ευθύνες από άποψη προστασίας των δεδομένων. Έχει μεγάλη σημασία να εξασφαλιστεί ότι ο διαχειριστής του συστήματος, καθώς και οποιοσδήποτε άλλος έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα σχετικά με εργαζομένους στο πλαίσιο της παρακολούθησης, θα υπόκεινται σε μια αυστηρή υποχρέωση επαγγελματικού απόρρητου όσον αφορά τις εμπιστευτικές πληροφορίες στις οποίες έχει πρόσβαση. Σε κάθε περίπτωση, πρέπει να προστατεύονται τα δεδομένα που τηρούνται στο πλαίσιο ενός συστήματος DLP από μη εξουσιοδοτημένες προσβάσεις. [007, 050, 123]

8. Οι εργοδότες επίσης, σύμφωνα με τα όσα έχει αναφέρει η ομάδα εργασίας του άρθρου 29, μπορούν να εξετάσουν τη δυνατότητα παροχής δυο λογαριασμών ηλεκτρονικών ταχυδρομείου στους εργαζόμενους: έναν μόνο για επαγγελματικούς σκοπούς στο οποίο θα είναι δυνατή η παρακολούθηση μέσα στα επιτρεπτά όρια (με υποχρέωση αποστολής επαγγελματικών ηλεκτρονικών μηνυμάτων μόνο μέσω αυτής της διεύθυνσης) και ένα δεύτερο λογαριασμό μόνο για καθαρά ιδιωτικούς σκοπούς που θα υπόκειται μόνο σε μέτρα ασφάλειας και θα ελέγχεται για καταχρήσεις σε εξαιρετικές περιπτώσεις. [007, 050, 123]

Σημειώνεται ότι για ένα οποιοδήποτε σύστημα παρακολούθησης, ο εργοδότης δεν μπορεί να επικαλεστεί ως επιχείρημα τη συναίνεση των υπαλλήλων του (ακόμα και αν προσκομίσει ενυπόγραφες συγκαταθέσεις αυτών). Η ομάδα εργασίας του άρθρου 29 έχει διατυπώσει την άποψη ότι «Εάν ο εργοδότης πρέπει να προβεί στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, ως αναγκαία και αναπόφευκτη συνέπεια της σχέσης απασχόλησης, η προσπάθειας νομιμοποίησης της επεξεργασίας αυτής μέσω της συγκατάθεσης οδηγεί σε παραπλάνηση. Η προσφυγή στη συγκατάθεση πρέπει να περιορίζεται σε περιπτώσεις όπου ο εργαζόμενος έχει πράγματι ελευθερία επιλογής και μπορεί να αποσύρει τη συγκατάθεση του μεταγενέστερα χωρίς να υφίσταται ζημιά». Και τούτο διότι η συγκατάθεση στο εργασιακό περιβάλλον δεν μπορεί ποτέ να θεωρηθεί ελεύθερη (η μη συγκατάθεση μπορεί να επιφέρει δυσμενείς συνέπειες στον εργαζόμενο, όπως π.χ. απόλυσή του).

Σε κάθε περίπτωση, θα πρέπει να υπάρχει πολιτική (Policy) στον οργανισμό η οποία θα καθορίζει ξεκάθαρους τους κανόνες (Rules) και τα πρότυπα (standards) για τον οργανισμό σχετικά με την φύση και την έκταση της παρακολούθησης (monitoring). Είναι απαραίτητο οι εργαζόμενοι να έχουν επίγνωση της πολιτικής. [007, 008, 017, 023, 029, 030, 031, 032, 033, 039, 040, 045, 050, 052, 081, 097, 103, 108, 116, 123, 124, 125, 130, 132, 136, 147]

Κεφάλαιο 6
Συγκριτική Αποτίμηση

Στο παρόν κεφάλαιο θα γίνει μια συγκριτική αποτίμηση των διαφόρων τεχνικών, μεθόδων ανίχνευσης δεδομένων των οποίων εφαρμόζονται στα εργαλεία Αποτροπής Απώλειας Δεδομένων. Οι διάφορες τεχνικές ανίχνευσης θα αξιολογηθούν ως προς την αποτελεσματικότητα ανίχνευσης διαρροής δεδομένων και ταυτόχρονα θα εξεταστούν κατά πόσο οι μέθοδοι αυτές είναι φιλικές ως προς την ιδιωτικότητα.

6.1 Αξιολόγηση Τεχνικών, Μεθόδων Ανίχνευσης Συμβάντων.

Στο κεφάλαιο 3 έχουν περιγραφτεί επτά από τις πιο σημαντικές τεχνικές, μεθόδους ανίχνευσης εμπιστευτικών δεδομένων.

6.1.1 Αντιστοίχηση Λέξεων-Κλειδιών

Η μέθοδος αντιστοίχηση Λέξεων-Κλειδιών (Keyword Matching) θεωρείτε γρήγορη και αποτελεσματική μέθοδος άλλα με περιορισμένες δυνατότητες. Εντοπίζει δεδομένα στα οποία το περιεχόμενο τους είναι μόνο στατικό κείμενο. Εάν αλλάξει το κείμενο των δεδομένων τότε υπάρχει πιθανότητα το εργαλείο μας να επιστρέφει υψηλό δίκτυ από Ψευδώς Θετικές ειδοποιήσεις (False Positives). Η μέθοδος αντιστοίχηση Λέξεων-Κλειδιών είναι δύσκολο να προσφέρει πολύ υψηλή ακρίβεια.

Επιπλέον, με την μέθοδο αντιστοίχηση Λέξεων-Κλειδιών διαβάζεται και συγκρίνεται το περιεχόμενο του αρχείου, γεγονός που εγείρει ζητήματα ως προς την ιδιωτικότητας και προστασία προσωπικών δεδομένων του εργαζομένου. [026, 042, 057, 061, 069, 075, 088]

6.1.2 Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων

Η μέθοδος αντιστοίχιση κανόνων και τυπικών εκφράσεων (Rule Based και Regular Expression Matching) είναι ιδανική για τον εντοπισμό περιγραφικών δεδομένων (Described data), και μπορεί οποιοσδήποτε να δημιουργήσει και να επεξεργαστεί εύκολα τους δικούς του κανόνες προσαρμοσμένους στις δίκες του ανάγκες. Η μέθοδος αντιστοίχισης κανόνων και τυπικών εκφράσεων προσφέρει μικρή προστασία σε αρχεία με μη δομημένο περιεχόμενο. Επιπλέον, παρουσιάζονται ψηλά ποσοστά από Ψευδώς Θετικές ειδοποιήσεις. Η μέθοδος αντιστοίχισης κανόνων και τυπικών εκφράσεων είναι δύσκολο να προσφέρει πολύ υψηλή ακρίβεια.

Η μέθοδος αντιστοίχισης κανόνων και τυπικών εκφράσεων αναλύει το περιεχόμενο των δεδομένων με βάση συγκεκριμένους κανόνες. Το γεγονός ότι αναλύει και συγκρίνει χωρίς να διαβάζεται το περιεχόμενο του αρχείου (αν δεν ικανοποιείται κάποιος κανόνας) έχει ως αποτέλεσμα η μέθοδος αυτή να είναι πιο φιλική ως προς την ιδιωτικότητα και προστασίας προσωπικών δεδομένων (εξακολουθεί πάντως, και αυτή, να ελέγχει περιεχόμενα αρχείων/μηνυμάτων). [026, 042, 058, 061, 069, 075, 080, 088]

6.1.3 Αποτύπωμα Δεδομένων

Η Μέθοδος Αποτύπωμα Δεδομένων (Data Fingerprinting) είναι ιδανική για το εντοπισμό δομημένων (structured) και μη δομημένων (unstructured) δεδομένων. Προσφέρει υψηλό δίκτυ ακρίβειας στο εντοπισμό εμπιστευτικών αρχείων. Επιπλέον έχει πολύ χαμηλό δίκτυ από Ψευδώς

Θετικές ειδοποιήσεις. Όμως είναι ακατόρθωτο να έχουμε πρόσβαση και σύγκριση σε όλα τα δεδομένα μας με αυτήν την μέθοδο.

Η μέθοδος Αποτύπωμα Δεδομένων δεν παραβιάζει τα θέματα ιδιωτικότητας καθώς η μέθοδος συγκρίνει την συνάρτηση κατακερματισμού των αρχείων και δεν προβαίνει σε οποιαδήποτε ανάγνωση του περιεχομένου του. Επίσης δεν αναμένεται να παραχθούν ψευδώς θετικές ειδοποιήσεις [026, 042, 058, 061, 069, 075,082, 088, 099, 109]

6.1.4 Χαρακτηριστικά των Αρχείων

Η μέθοδος Χαρακτηριστικά των αρχείων (File Attribute) παρουσιάζει ψήλο ποσοστό από Ψευδώς θετικές ειδοποιήσεις. Πολλές φορές τα χαρακτηριστικά των αρχείων δεν μπορούν να μη δώσουν την ακρίβεια την οποία ζητούμε.

Επιπλέον με την μέθοδο Χαρακτηριστικά των αρχείων δεν παραβιάζουμε ζητήματα ιδιωτικότητας για το λόγο ότι δεν προβαίνουμε στην ανάγνωση περιεχομένου του αρχείου.[026, 061, 069]

6.1.5 Ανάλυση Βάσει Εννοιών

Η μέθοδος Ανάλυση Βάσει Εννοιών (Conceptual Lexicon Analysis) παρουσιάζει ψηλά ποσοστά από Ψευδώς θετικά (False Positives). Επιπλέον, με αυτή την μέθοδο τίθενται ερωτηματικά ως προς την παραβίαση της ιδιωτικότητας εφόσον γίνεται ανάγνωση του περιεχομένου του αρχείου. [026, 042, 058, 069, 075, 088]

6.1.6 Κατηγορίες

Η μέθοδος Κατηγορίες (Categories) εξοικονομά πολύτιμο χρόνο για το λόγο ότι προσφέρουν προ εγκατεστημένες κατηγορίες σε ένα εργαλείο Αποτροπής Απώλειας Δεδομένων. Εξυπακούεται πως όλες οι κατηγορίες δεν μπορούν να εξυπηρετήσουν και να ταιριάσουν σε όλους τους τύπους και μεγέθη οργανισμών. Παρουσιάζουν υψηλή ακρίβεια για συνήθης δεδομένα. Αλλά δεν παύουν να παρουσιάζουν υψηλό δίκτυ Ψευδώς θετικά (False Positives).

Η μέθοδος κατηγορίες χρησιμοποιούν συνδυασμό τεχνικών οι οποίες αναφέρθηκαν πιο πάνω. Η μέθοδος αυτή χρήζει προσοχής ως προς την ιδιωτικότητα, εφόσον για τον εντοπισμό χρησιμοποιείται η ανάγνωση αρχείου. [042, 049, 069, 075, 088]

6.1.7 Αλγόριθμοι Μηχανικής Μάθησης

Η μέθοδος η οποία χρησιμοποιείται για την ελαχιστοποίηση των Ψευδών θετικών (False positives) είναι οι αλγόριθμοι Μηχανικής Μάθησης. Όσο περισσότερο είναι εκπαιδευμένος ο αλγόριθμος τόσο μεγαλύτερη ακρίβεια έχουμε αλλά όμως δυστυχώς μπορεί να υπάρξει και το αντίθετο. Αναπόφευκτα με τους αλγόριθμους μηχανικής μάθησης τίθεται θέμα ιδιωτικότητας, αφού για να συγκριθούν τα αρχεία κατά την φάση της εντόπισης πρέπει να διαβαστούν από το εργαλείο αποτροπής απώλειας δεδομένων. [026, 042, 058, 069, 075, 082, 088, 107]

Οι επτά πιο πάνω τεχνικές ανίχνευσης εμπιστευτικών πληροφοριών συμπεριλαμβάνονται στα περισσότερα εργαλεία αποτροπής απώλειας δεδομένων. Η χρησιμοποίηση ενός συνδυασμού των πιο πάνω τεχνικών στα εργαλεία μας θα επιφέρει ελαχιστοποίηση των Ψευδώς θετικών (False Positives) και μεγάλο βαθμό ακρίβειας.

Είναι αναπόφευκτο πως χρησιμοποιώντας κάποιες από τις επτά τεχνικές εγείρονται θέματα παραβίασης της ιδιωτικότητας, αφού διαβάζεται περιεχόμενο αρχείων. Η βέλτιστη λύση θα πρέπει να είναι εκείνη που να σέβεται και να ακολουθεί όλες τις αρχές που περιγράφονται στο Κεφάλαιο 5 (παρ. 5.3), με τις εξής πρόσθετες ιδιότητες:

1. Άπαξ και ελέγχεται οποιουδήποτε τύπου αρχείο και δεν θεωρείται ύποπτο, το σύστημα DLP δεν θα πρέπει να κάνει απολύτως καμία καταγραφή/καταχώρηση.

2. Επιλογή συστήματος DLP με τις λιγότερες δυνατές Ψευδώς θετικές Ειδοποιήσεις (False Positive Alarms), έτσι ώστε να ελαχιστοποιείται η πιθανότητα να ελεγχθούν αρχεία ως «ύποπτα» διαρροής, χωρίς να πρέπει.

3. Εφόσον υπάρξει Ψευδώς θετική ειδοποίηση (False Positive Alarm), να γίνεται άμεση διαγραφή της σχετικής καταχώρησης από το σύστημα DLP.

Κεφάλαιο 7
Επίλογος

Στην παρούσα εργασία μελετήθηκαν τα εργαλεία αποτροπής απώλειας δεδομένων, τα οποία γνωρίζουν μεγάλη άνθηση τα τελευταία χρόνια ως άμεση απόρροια του γεγονότος ότι πλέον οι επιχειρήσεις επεξεργάζονται, μέσω των πληροφοριακών τους συστημάτων, μεγάλο εύρος ιδιαίτερα εμπιστευτικών δεδομένων. Πράγματι, παρατηρώντας τις τεχνολογίες ασφαλείας, προκύπτει ότι ένα εργαλείο Αποτροπής Απώλειας Δεδομένων είναι η μόνη λύση (εν είδει αυτοματοποιημένου εργαλείου) που παρέχει προστασία των δεδομένων ενός οργανισμού από την διαρροή δεδομένων από το εσωτερικό του οργανισμού προς το εξωτερικό περιβάλλον.

Υπάρχουν διάφορες τεχνικές για την ανίχνευση διαρροής κρίσιμης πληροφορίας από έναν οργανισμό: καταλληλότερη επιλογή διαφαίνεται ότι είναι αυτή που πληροί τις απαιτήσεις σύμφωνα με το μέγεθος του οργανισμού και τον όγκο (αλλά και σπουδαιότητα) των δεδομένων. Ένας συνδυασμός από τις διάφορες τεχνικές ανίχνευσης φαίνεται ότι υπερτερεί, σε σχέση με το να χρησιμοποιηθεί αποκλειστικά κάποια εξ αυτών.

Ωστόσο, κάθε τέτοιο εργαλείο αυτομάτως επεξεργάζεται δεδομένα εργαζομένων, γεγονός που με τη σειρά του μπορεί να αποτελεί παραβίαση των νομικών επιταγών ως προς την

ιδιωτικότητα (ιδίως όταν το εργαλείο ανιχνεύει λανθασμένα μία δραστηριότητα υπαλλήλου ως αθέμιτη, οπότε μελετάται αναλυτικά η ενέργεια του συγκεκριμένου υπαλλήλου, που μπορεί να αποδειχτεί ότι είναι μία απλή αποστολή προσωπικού του ηλεκτρονικού μηνύματος, χωρίς να δημιουργεί κίνδυνο για την εταιρεία).

Κατά συνέπεια, η απόφαση για το αν ένα τέτοιο εργαλείο πρέπει να χρησιμοποιείται, καθώς και – εφόσον ληφθεί θετική απόφαση – ο τρόπος λειτουργίας αυτού, αποτελούν ζητήματα ιδιαίτερης δυσκολίας γιατί προκύπτει σύγκρουση αντίρροπων συμφερόντων: του εργοδότη από τη μία πλευρά για την προστασία των δεδομένων των πελατών του, καθώς και την εργαζομένων από την άλλη πλευρά για την προστασία της ιδιωτικότητάς τους. Ως εκ τούτου, απαιτείται πάντοτε μία στάθμιση των δύο αυτών συμφερόντων.

Ως γενική αρχή, που προκύπτει ως συμπέρασμα αυτής της εργασίας, είναι ότι πριν την τοποθέτηση ενός Εργαλείου Αποτροπής Απώλειας Δεδομένων θα πρέπει να προηγείται μία ανάλυση επιπτώσεων στην ιδιωτικότητα (Privacy Impact Assessment – PIA). Η Ανάλυση Επιπτώσεων στην Ιδιωτικότητα είναι ένα εργαλείο το οποίο χρησιμοποιείται για τον προσδιορισμό των κινδύνων ως προς την ιδιωτικότητα και τη λήψη μέτρων για τη μείωση/εξάλειψή τους. Ο οργανισμός, με τις πληροφορίες που θα αποκτήσει με την εκπόνηση μίας PIA, θα είναι σε θέση να διασφαλίσει ότι η προτεινόμενη λύση παρακολούθησης (DLP) του χώρου εργασίας είναι ανάλογη προς τους κινδύνους (Risk) που προσπαθεί να διαχειριστεί. Επιπλέον, με την ανάλυση επιπτώσεων στην ιδιωτικότητα θα είναι έτοιμος ο οργανισμός να διαβουλευτεί μαζί με τους εργαζόμενους του σχετικά με την τεχνολογία λαμβάνοντας υπόψη τους νόμους της εκάστοτε χώρας, το μέγεθος του οργανισμού και την ύπαρξη οποιωνδήποτε συλλογικών συμβάσεων εργασίας.[045]

Με την τοποθέτηση ενός Εργαλείου Αποτροπής Απώλειας Δεδομένων θα πρέπει να γίνεται πλήρης ενημέρωση των εργαζομένων σχετικά με την λειτουργία και το σκοπό του.

Από τα παραπάνω καθίσταται προφανές ότι είναι αναγκαίο να δημιουργούνται καινούργιες τεχνικές και αλγόριθμοι οι οποίοι θα επιστρέψουν τις λιγότερες Ψευδώς θετικές ειδοποιήσεις, και ταυτόχρονα να παρέχουν ευελιξία στο εκάστοτε οργανισμό να θέτει τα δικά του κριτήρια που να συγκεκριμενοποιούν το τι θεωρούν διαρροή και τι όχι, έτσι ώστε να ελαχιστοποιείται η πιθανότητα να πλήττεται η ιδιωτικότητα των εργαζομένων τους.

Βιβλιογραφία

[001] A DLP Experts «Data Loss Prevention Leading Vendors Review» A DLP Experts White Paper, January 2014.

[002] A DLP Experts, «Five Tips to Ensure Data Loss Prevention Success,» January 2013.

[003] A DLP Experts, «White Paper Five Tips To Ensure Data Loss Prevention Success,» A DLP Experts , January 2013.

[004] Absolute Software Corporation, «Absolute DLP Track and Prevent Data Breaches Datasheet,» 2013.

[005] Absolute Software Corporation, «Absolute Web Monitor Enforce Acceptable Use Datasheet,» 2013.

[006] Absolute Software, «Absolute Software Acquires Data Security and Data Loss Prevention Assets from Palisade Systems,» 25 June 2013. URL: http://www.absolute.com/en/about/pressroom/press-releases/2013/6/25/absolute-software-acquires-data-security-and-data-loss-prevention-assets-from-palisade-systems.

[007] Article 29 – Data Protection Working Party 5062/01/EN/Final WP 48 Opinion 8/2001 «on the processing of personal data in the employment context», Adopted on 13 September 2001, 2001.

[008] R. Bloor, "Dealing with the enterprise data threat How Zecurion Protects Corporate Data," Zecurion, New York, 2013.

[009] H. Bradley, «Data Loss Prevention-Best Practices,Managing Sensitive data in the enterprise,» 2007.

[010] B. Butler, «IT security vendor Verdasys brings DLP to the cloud; Data loss prevention technology flags suspicious activity from afar.(data loss prevention)(cloud computing,» Network World, January 2013.

[011] CA Technologies, «CA DataMinder Classification Data Sheet,» 2012.

[012] CA Technologies, «CA DataMinder DLP,»Video, URL: http://www.ca.com/us/securecenter/ca-dataminder.aspx.

[013] CA Technologies, «CA DataMinder Endpoint Data sheet,» 2012.

[014] CA Technologies, «CA DataMinder Platform Deployment Guide Release

14.1,» 2012.

[015] CA Technologies, «CA DataMinder™ Express,» 2012.

[016] CA Technologies, «CA DataMinder™ Stored Data,» 2012.

[017] C. Casper, «Gartner Hype Cycle for Privacy, 2013,» Gartner , july 2013 .

[018] Checkpoint, «Introduction to Data Loss Prevention,» 15 January 2014. URL: https://sc1.checkpoint.com/documents/R77/CP_R77_DataLossPrevention_AdminGuide/62453.htm.

[019] A. Chuvakin, «Content-Aware DLP Architecture and Operational Practices,» Gartner, 2013.

[020] A. Chuvakin, «Gartner Technical Professional Advice Enterprise Content-Aware DLP Architecture and Operational Practices,» Gartner , March 2013 .

[021] A. Chuvakin, «Security Incident Response in the Age of ART,» Gartner Technical Professional Advice , September 2013.

[022] A. Chuvakin, T. Henry, «Enterprise Content-Aware DLP Solution Comparison and Select Vendor Profiles,» Gartner Technical Professional Advice , April 2013.

[023] G. Clayton, «Data Loss Prevention and Monitoring in the Workplace: Best Practice Guide for Europe Whitepaper,» Symantec, Dallas, USA.

[024] Code Green Networks, «Complete Data Loss Prevention from Code Green Networks Technology Brief,» 2010.

[025] Code Green Networks, «TrueDLP Enterprise Data Loss Prevention without the complexity,» URL: http://www.codegreennetworks.com/.

[026] A. Cornelissen, «Covert Channel Data Leakage Protection A model for detecting and preventing data leakage through covert channels», Nijmegen/Amstelveen: University of Twente, 2012.

[027] M. Datardina, M. Li, «Information Leakage and Data Loss Prevention,» June 13, 2011.

[028] N. Deepa, S. Priyadarsini, R. Sathiyaseelan, M. Varun Kumar, «Image Based DLP Security for Risk Professionals -A High Impact Strategy,» International Review on Computers and Software (I.RE.CO.S.), τόμ. 7, November 2012.

[029] T. Elchayani, «A Delicate Balance: DLP and Privacy,» PineApp Blog Enterprise IT Security, 7 September 2010. URL: http://pineapp.wordpress.com/2010/08/31/a-delicate-balance-dlp-and-

privacy/.

[030] European Commission, «Collecting & processing personal data: what is legal?,» 16 July 2013. URL: http://ec.europa.eu/justice/data-protection/data-collection/legal/index_en.htm.

[031] European Network and Information Security Agency «European Network and Information Security Agency,» URL: http://www.enisa.europa.eu/.

[032] Field Fisher Waterhouse, «Data security law and breach action,» URL: http://www.ffw.com/practices/technology-and-outsourcing/data-security-breach-action.aspx.

[033] Field Fisher Waterhouse, «Privacy & information,» URL: http://www.ffw.com/practices/privacy-and-information.aspx.

[034] General Dynamics Fidelis Cybersecurity Solutions, «Fidelis XPS Face Advanced Threats with Confidence Technical Data Sheet».

[035] General Dynamics Fidelis Cybersecurity Solutions, «Fidelis XPS™ Power Tools Achieving Advanced Threat Management, Data Breach Prevention, Intelligent Network Forensics with Fidelis XPS,» June 2011.

[036] General Dynamics Fidelis Cybersecurity Solutions, «Fidelis XPS™ Power Tools: Malware Detection Stack,» June 2013.

[037] General Dynamics Fidelis Cybersecurity Solutions, «General Dynamics Fidelis Cybersecurity Solutions,» URL: http://www.fidelissecurity.com/.

[038] General Dynamics Fidelis Cybersecurity Solutions. Inc., «Fidelis XPS™Solution Overview,» January 2013.

[039] N. Gnanasambandam, J. Staddon, «Personalized Privacy Policies: Challenges for Data Loss Prevention».

[040] P. Gordon, «Workplace Privacy 2014: What's New and What Employers May Expect,» Littler, 7 January 2014. URL: http://www.littler.com/publication-press/publication/workplace-privacy-2014-what%E2%80%99s-new-and-what-employers-may-expect.

[041] GTB Technologies, «GTB Technologies Next Generation DLP,» URL: http://www.gtbtechnologies.com/.

[042] M. Hart, P. Manadhata, R. Johnson, «Text Classification for Data Loss Prevention,» Springer Berlin / Heidelberg, τόμ. 6794, pp. 18-37, 2011.

[043] J. Hawes , «2013 an epic year for data breaches with over 800 million

records lost,» February 2014.

[044] B. Hunter, «Data Loss Prevention Best Practices- Managing Sensitive Data in the Enterprise».

[045] Information Commisioner's Office, «Privacy impact assessment,» URL: http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

[046] Infowatch, «InfoWatch Traffic Monitor Enterprise Monitoring and Classification of information flows,» 2013.

[047] Infowatch, «Infowatch Traffic Monitor Enterprise,» URL: https://infowatch.com/products/traffic_monitor_enterprise.

[048] M. Jach, «Data loss prevention Refreshing data security to meet an evolving threat environment,» July 2012.

[049] Jscape, «Exploring Regular Expressions in DLP,» 12 April 2012. URL: http://www.jscape.com/blog/bid/79591/Exploring-Regular-Expressions-in-DLP.

[050] Justice - European Commission «Ομάδα Εργασίας του Άρθρου 29,» URL: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.ht.

[051] P. Kanagasingham, «Data Loss Prevention", SANS Institute InfoSec Reading Room,» August 2008.

[052] L. Kauffman, «What security risks are associated with DLP Systems?,» StackExchange, 5 September 2013. URL: http://security.stackexchange.com/questions/41814/what-security-risks-are-associated-with-dlp-systems.

[053] B. Lakshmi, K. Parish, V. Kumar, A. Banu, K. Reddy , «Data Confidentiality and Loss Prevention using Virtual Private Database,» March 2013.

[054] S. Lee, T. Kim, I. Choi, «Apparatus and security system for data loss prevention, and operating method of data loss prevention apparatus,» Somansa Co., Ltd, July 2013.

[055] R. Liles, J. Pearce, M. Saher , «Breach Detection System Product Analysis Fidelis XPS,» NSS labs , 2013.

[056] R. Liu, «Data Loss Prevention,» INSECURE IT, April 2010.

[057] R. Mackey, «LP: It's Not Just for Big Firms Anymore».

[058] Manasdeep, «Data Leakage Prevention – Implementation And Challenges,» Network Intelligence, August 2012.

[059] McAfee, «McAfee Data Loss Prevention,» URL: http://www.mcafee.com/us/products/data-protection/data-loss-prevention.aspx.

[060] K. McDonald, «Above the Clouds: Managing Risk in the World of Cloud Computing,» IT Governance Ltd, February 2010.

[061] T. Micro, «Trend Micro Data Loss Prevention Endpoint Administrator's Guide,» Trend Micro, November 2010.

[062] A. Miller, C. Tucker , «Encryption and the Loss of Patient Data,» 2011.

[063] M. Miller, «Is It Safe? Protecting Your Computer, Your Business, and Yourself Online,» Que, January 2008.

[064] Open Security Foundation, «Data Loss db Open Security Foundation,» URL: http://datalossdb.org/.

[065] P. Parker, «The 2009-2014 World Outlook for Information Data Loss Prevention (DLP),» Icon Group International, 2008.

[066] L. Peace, «Reading Room Document Metadata, the Silent Killer…,» Sans institute InfoSec , March 2008.

[067] J. Peersman, «Preventing Data Breaches by Proactive Data mining,» Utrecht University , p. 61, December 28, 2012.

[068] C. Porter, «Email Security with Cisco IronPort,» Cisco Press, April 2012.

[069] E. Quellet, «Gartner 2013 Buyer's Guide to Content-Aware DLP,» Gartner , August 2013 .

[070] E. Quellet, «Magic Quadrant for Content-Aware Data Loss Prevention,» Gartner , 12 December 2013 .

[071] RSA Conference Europe, «Privacy concerns with adopting DLP technology,» 2009.

[072] RSA, «RSA Data Loss Prevention Helping organizations address the challenges of securiting data at rest, in motion and in use».

[073] RSA, «RSA Data Loss Prevention,» URL: http://www.emc.com/security/rsa-data-loss-prevention.htm.

[074] RSA, «The Security Division of EMC RSA Data Loss Prevention Suite v9.0

Security Target».

[075] SANS Institute, «Understanding and Selecting a Data Loss Prevention Solution», URL: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[076] H. Sethuraman, M. Haseeb , «Master's Thesis Data Loss/Leakage Prevention», 2012.

[077] A. Shabtai, Y. Elovici, L. Rokach, «Chapter 3 A Taxonomy of Data Leakage Prevention Solutions,» A Survey of Data Leakage Detection and Prevention Solutions, Springer Briefs in Computer Science, 2012, pp. 13-15 .

[078] J. Sigholm, M. Raciti., «Best-Effort Data Leakage Prevention in Inter-Organizational Tactical MANETs».

[079] R. Smallwood, B. Blair, «Safeguarding Critical E-Documents: Implementing a Program for Securing Confidential Information Assets,» John Wiley & Sons, July 2012.

[080] Stackoverflow, «How do you detect Credit card type based on number?,» 16 Σεμπτεμβριο 2008. URL: http://stackoverflow.com/questions/72768/how-do-you-detect-credit-card-type-based-on-number.

[081] T. Stevens, «Identity, Privacy and Trust The Data Trust Blog,» ComputerWeekly.com, 20 October 2009. URL: http://www.computerweekly.com/blogs/the-data-trust-blog/2009/10/dlp-and-privacy.html.

[082] Symantec, «Machine Learning Sets New Standard for Data Loss Prevention: Describe, Fingerprint, Learn», URL: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-dlp_machine_learning.WP_en-us.pdf

[083] Symantec, «Symantec Data Loss Prevention,» URL: http://www.symantec.com/data-loss-prevention.

[084] Symantec, «Symantec Enterprise Vault Overview Store, manage, and discover critical business information Data sheet: Archiving and eDiscovery».

[085] Symantec, «What's New in Symantec Data Loss Prevention 12 Data Sheet: Data Loss Prevention».

[086] Symantec, «White Paper: Data Loss Prevention Machine Learning Sets New Standard for Data Loss Prevention: Describe, Fingerprint, Learn,» Symantec,

2010.

[087] T. Takebayashi, H. Tsuda, T. Hasebe, R Masuoka , «Data Loss Prevention Technologies,» Fujitsu Sci. Tech. j, τόμ. 46, αρ. 1, 2010.

[088] T. Torsteinbø, «Data Loss Prevention Systems and Their Weaknesses», 2012.

[089] Triton, «Triton Data security Products Data Loss Prevention,» URL: http://www.websense.com/content/websense-data-security-products.aspx.

[090] Trustwave, «2014 Trustwave Security Pressures Report».

[091] Trustwave, «Data Loss Prevention: Discover Discover, a component of TrustwaveData Loss Prevention (DLP) suite, offers a simpler and more scalable way to manage content risk and prevent data loss».

[092] Trustwave, «Discover, a component of Trustwave's Data Loss Prevention (DLP) suite, offers a simpler and more scalable way to manage content risk and prevent data loss.,» .

[093] Trustwave, «Trustwave Data Loss Prevention Trustwave's Data Loss Prevention (DLP) Solution is a content control solution designed to monitor and prevent data loss across your network».

[094] Trustwave, «Trustwave Managed Security Services An ideal, cost-effective solution to protect any organization's key information assets and allow internal IT staff to concentrate on their core competencies,».

[095] Trustwave, «Trustwave's Data Loss Prevention,» URL: https://www3.trustwave.com/data-loss-prevention/dlp-overview.php.

[096] Turle M., «Data security: Past, present and future,» p. 5 1 – 5 8, 2 0 0 9.

[097] C. Umhoefer, M. Hallé, «EUROPE: Focus on new Regulation No. 611/2013 detailing notification procedures for providers of publicly-available electronic communications services in the event of a personal data breach,» Privacy Matters, 2 December 2013. URL: EUROPE: Focus on new Regulation No. 611/2013 detailing notification procedures for providers of publicly-available electronic communications services in the event of a personal data breach.

[098] J. Vacca, «Data Loss Protection,» σε Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, November 5, 2012.

[099] Verdasys, «Data Classification A scalable Approach to managing sensitive

Data White Paper,» 2013.

[100] Verdasys, «DLP 3.0 Meeting Today's Data Protection Challenges: DLP 3.0 And Enterprise Information Protection White Paper,» 2013.

[101] Verdasys, «Protection unstructured data identification, classification, and management White Paper,» 2013.

[102] Verdasys, «Verdasys DLP3.0 – Data Loss Prevention,» URL: https://www.verdasys.com/solutions/dlp-3.0.html.

[103] J. Wagley, «EU Balks at Employee Monitoring,» Security Management Security's Web Connection, 3 March 2010. URL: http://www.securitymanagement.com/article/eu-balks-employee-monitoring-006229.

[104] Websense , «A Buyer's Guide to Data Loss Protection Solutions».

[105] Websense Data Security Suite, «Unified Data Loss Prevention For Gateways, Endpoints And Discovery,» 2013.

[106] Websense, «A Buyer's Guide to Data Loss Protection Solutions,» 2013.

[107] Websense, «Introduction to Machine Learning for Websense® Data Security,» Websense, 31 October 2012.

[108] Wikipedia, «Employee monitoring From Wikipedia, the free encyclopedia,» Wikipedia, 8 February 2014. URL: http://en.wikipedia.org/wiki/Employee_monitoring.

[109] Wikipedia, «Fingerprint (computing) From Wikipedia, the free encyclopedia,» 29 January 2014. URL: http://en.wikipedia.org/wiki/Fingerprint_(computing).

[110] Wikipedia, «List of Issuer Identification Numbers, From Wikipedia, the free encyclopedia,» 24 February 2014. URL: http://en.wikipedia.org/wiki/List_of_Issuer_Identification_Numbers.

[111] Wikipedia, «Machine learning From Wikipedia, the free encyclopedia,» Wikipedia, 20 February 2014. URL: http://en.wikipedia.org/wiki/Machine_learning.

[112] Wikipedia, «Personally identifiable information From Wikipedia, the free encyclopedia,» 9 February 2014. URL: http://en.wikipedia.org/wiki/Personally_identifiable_information.

[113] Wikipedia, «Privacy by Design From Wikipedia, the free encyclopedia,» 27

January 2014. URL: http://en.wikipedia.org/wiki/Privacy_by_Design.

[114] Wikipedia, «Privacy From Wikipedia, the free encyclopedia,» 26 February 2014. URL: http://en.wikipedia.org/wiki/Privacy.

[115] A. Woody, «Enterprise Security: A Data-Centric Approach to Securing the Enterprise,» Packt Publishing, February 2013.

[116] V. Zdor, «DLP vs. Privacy Laws Infowatch,» Infowatch, 14 September 2011. URL: http://infowatch.com/node/2328.

[117] Zecurion, «Keep your data secure in the cloud Using encryption to ensure your online data is protected from compromise,» New York, 2013.

[118] Zecurion, «Product overview Zdiscovery. Zecurion Zdiscovery scans all stored data across corporate networks, reveals inappropriately stored confidential information and determines violations of security policies.,» New York, 2013.

[119] Zecurion, «Product Overview Zgate. Zgate is the most comprehensive Data Loss Prevention (DLP) product available, enabling companies to monitor all forms of outbound network», New York, 2013.

[120] Zecurion, «Product Overview Zlock. Zecurion Zlock is designed to protect against leaks of con¬dential information at the end-points of the network. Zecurion Zlock allows you to control the use of devices connected to ports including USB, LPT, COM, IrDA, IEEE 13», New York, 2013.

[121] Zecurion, «Product Overview Zserver. Zecurion Zserver is designed to securely protect the data stored on servers and on backup media. The system encrypts the information contained on hard drives, disk arrays and SAN storage using an innovative, sophisticated en», New York, 2013.

[122] Zecurion, «Zecurion Protection From The Inside Out,» URL: http://www.zecurion.com/tag/zecurion-dlp/, New York, 2013.

[123] Άρθρο 29 – Ομάδα Εργασίας για την Προστασία των Δεδομένων 5401/01/EL/Τελικό WP 55 «Έγγραφο εργασίας για την επιτήρηση των ηλεκτρονικών επικοινωνιών στον τόπο εργασίας» εκδόθηκε στις 29 Μαΐου 2002.

[124] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Hellenic Data Protection Authority (HDPA), Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,» URL: http://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL.

[125] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «ΑΠΟΦΑΣΗ ΑΡ. 61 / 2004 Πρόσβαση εργοδότη στους προσωπικούς υπολογιστές των εργαζομένων,» 2004.

[126] Βικιπαίδεια, «Απειλές και μηχανισμοί προστασίας της ιδιωτικότητας στα ασύρματα και κινητά δίκτυα,» URL: http://el.wikipedia.org/wiki/Απειλές και μηχανισμοί προστασίας της ιδιωτικότητας στα ασύρματα και κινητά δίκτυα, 19 Φεβρουαρίου 2013.

[127] Βικιπαίδεια, «Μηχανική μάθηση Από τη Βικιπαίδεια, την ελεύθερη εγκυκλοπαίδεια,» URL: http://el.wikipedia.org/wiki/Μηχανική μάθηση, 25 Μαΐος 2013.

[128] Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, Σ. Κάτσικας, «Τεχνολογίες Αναχωμάτων Ασφαλείας,» σε Ασφάλεια Δικτύων Υπολογιστών, 2003.

[129] Σ. Γκρίτζαλης, Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Κάτσικας, Προστασία της ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Τεχνικά και Νομικά Θέματα, Αθήνα: Παπασωτηρίου, 2010.

[130] Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, «Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,» URL: http://www.dataprotection.gov.cy.

[131] Ευροπαικό Κοινοβούλιο, «Οδηγία 2009/136/ΕΚ του Ευρωπαικου Κοινοβουλίου και του Συμβουλιου της 25ης Νοεμβριου 2009,» 2009.

[132] Ευροπαίος Επόπτης Προστασίας Δεδομένων, «European Data Protection Supervisor,» URL: http://www.edps.europa.eu/EDPSWEB/.

[133] Ευρωπαϊκή Επιτροπή – Προστασία προσωπικών δεδομένων, «Ευρωπαϊκή Επιτροπή – Προστασία προσωπικών δεδομένων,» URL: http://ec.europa.eu/justice/data-protection/index_en.htm.

[134] Ευρωπαϊκό Κοινοβούλιο, «Οδηγία 2002/58/ΕΚ του Ευρωπαικού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικα με την επεξεργασια των δεδομένων προσωπικού χαρακτήρα την προστασία της ιδιωτικής ζωή; στον τομέα των ηλεκτρονικών επικοινωνιών,» Βρυξέλλες, 2002.

[135] Κυπριακή Δημοκρατία, «Νόμος αρ. 30(ΙΙΙ)/2003 Ε.Ε. Παρ. Ι(ΙΙΙ) Αρ. 3732, 4.7.2003,» 2003.

[136] Κυρωτικός Νόμος αρ. 30(ΙΙΙ) του 2003 Ε.Ε. Παρ Ι(ΙΙΙ) Αρ. 3732, 4.7.2003 Ο Περί Πρόσθετου Πρωτόκολλου στη Σύμβαση για την Προστασία του Ατόμου από την Αυτοματοποιημένη Επεξεργασία Δεδομένων Προσωπικού

Χαρακτήρα Κυρωτικός Νόμος του 2003, αρ. 30(III)/20, 2003.

[137] Κ. Λιμνιώτης, «Σημειώσεις μαθήματος κρυπτογραφίας κεφάλαιο Προστασία Προσωπικών δεδομένων – θεσμικό πλαίσιο».

[138] Νόμοι 138(I) του 2001, 37(I) του 2003 και 105(I)/2012 - Ανεπίσημη Ενοποίηση Ανεπίσημη Ενοποίηση του Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001, αρ. 138(I)/2001, όπως έχει τροποποιηθεί, 2001.

[139] Νόμος 2472/1997 «Προστασία Του Ατόμου Από Την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα ΜΕ ΕΝΣΜΑΤΜΕΝΕΣ ΤΙΣ ΤΡΟΠΟΠΟΙΗΣΕΙΣ», 1997.

[140] Νόμος 3471/2006 (ΦΕΚ 133/Α'/28.6.2006) «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997» 1997.

[141] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Επίσημη Εφημερίδα των, 1995.

[142] Οδηγία Αρ. 115 / 2001 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», 2001.

[143] Συμβούλιο της Ευρώπης, «Ενοποιημένη απόδοση της Συνθήκης για την Ευρωπαϊκή Ένωση και της Συνθήκης για τη λειτουργία της Ευρωπαικής Ένωσης 2012/ψ 326/01,» 2012.

[144] Συμβούλιο της Ευρώπης, «Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών όπως τροποποιήθηκε με τα Πρωτόκολλα No. 11 και No. 14,» Ρώμη, 1950.

[145] Συμβούλιο της Ευρώπης, «Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοποιημένη επεξεργασία προσωπικών δεδομένων,» Στρασβούργο, 1981.

[146] Το ελληνικό Σύνταγμα, «Το ελληνικό Σύνταγμα,» URL: http://www.hri.org/docs/syntagma/.

[147] Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. (2000/C 364/01) Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, 2000.

Παράρτημα Α
Αντιστοίχηση Ελληνικών – Αγγλικών Όρων

Άγκιστρα-Αγκύλες	Curly Brackets
Αισθητήρας	Sensors
Αισθητήρας Δικτύου	Network Sensor
Ακολουθίες Δυαδικών Ψηφίων	Bit Sequences
Αλγόριθμοι Με Επίβλεψη	Supervised Learning Algorithms
Αλγόριθμοι Μηχανικής Μάθησης	Machine Learning
Αλγόριθμοι Χωρίς Επίβλεψη	Unsupervised Learning Algorithms
Άμεσα Μηνύματα	Instant Messaging

Ανακαλύπτει	Discovers
Ανάλυση Βάσει Εννοιών	Conceptual lexicon Analysis
Ανάλυση Δεδομένων	Data Analysis
Ανάλυση επιπτώσεων στην ιδιωτικότητα	Privacy Impact Assessment – PIA
Ανατροφοδότηση	Feedback
Αναφορές	Reports
Αναχαιτιστής Δικτύου	Network Interceptor
Αναχαιτιστικό	Interceptors
Αναχώματα Ασφαλείας	Firewalls
Αντιγράψει	Copy
Αντιστοίχηση Λέξεων Κλειδιών	Keyword Matching
Αντιστοίχιση Κανόνων και Τυπικών Εκφράσεων	Ruled based και Regular Expression
Απειλές	Threats
Απλό Πρωτόκολλο Μεταφοράς Αλληλογραφίας	Simple Mail Transport Protocol
Αποθηκευμένα	Stored
Αποτροπή Απώλειας Δεδομένων	Data Loss Prevention
Αποτύπωμα Δεδομένων	Data Fingerprinting

Απώλεια Δεδομένων	Data Loss
Αριθμός Κοινωνικής Ασφάλισης	Social Security Number
Αρνητικά Παραδείγματα	Negative Examples
Αρχεία Καταγραφής Έλεγχου	Audit Logs
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	Data Protection Authority
Αρχή της ιδιωτικότητας κατά τη σχεδίαση	Privacy-by-Design
Ασπίδα	Shield
Ασφαλές Πρωτόκολλο Μεταφοράς Υπερκείμενου	Secure Hypertext Transport Protocol
Βαθμό	Rate
Βαθμός Ομοιότητας	Similarity Score
Βάσεις Δεδομένων	Database
Γεγονότα	Events
Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	Office of the Commissioner for Personal Data Protection
Γραφικό Περιβάλλον Χρήστη	Graphical User Interface
Δεδομένα Που Βρίσκονται Σε Αδράνεια	Data At Rest
Δεδομένα Σε Καταληκτικό Σημείο	Data At The Endpoint
Δεδομένα Σε Κίνηση	Data In Motion

Διακομιστές	Servers
Διακομιστές Αποθήκευσης Αρχείων	File Servers
Διακομιστές Αποτροπής Απώλειας Δεδομένων	Data Loss Prevention Server
Διακομιστή Ταχυδρομείου	Mail Server
Διακομιστής Ιστού	Web Servers
Διαρροή Δεδομένων	Data Leakage
Διαχειρίζεται	Manages
Διαχειριστές Συστήματος	System Administrators
Διεκδικητές	Challengers
Δίκτυο Ευρείας Περιοχής	Wide Area Network
Δομημένα Δεδομένα	Structured Data
Ειδικές Ενέργειες	Custom Actions
Ειδοποιητικό Μήνυμα	Incident
Εικονίδιο Συστήματος	System Tray Icon
Εκπαίδευση	Training
Ελεγκτής Δικτύου	Network Controller
Εμπιστευτικά δεδομένα	Confidential data
Εμπιστευτικότητα	Confidentiality

Ενέργεια	Action
Εντοπισμός / Ανίχνευση	Detection
Εξειδικευμένοι παίκτες	Niche Players
Εξωτερική Επίθεση	Outside Attack
Επιθέσεις	Attacks
Επιρράματα	Patches
Επιχειρησιακό Πλαίσιο	Business Context
Εργαλεία Διαμόρφωσης	Configuration Tools
Εργαλεία Διαχείρισης Ευπαθειών	Vulnerability Management Tools
Εργατικά συμβούλια	Works Councils
Εσωτερικές Επιθέσεις	Inside Attacks
Ευαίσθητα δεδομένα	Sensitive Data
Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών	European Network and Information Security Agency - ENISA
Ευρωπαίος Επόπτης Προστασίας Δεδομένων	European Data Protection Supervisor
Εφαρμογές	Applications
Εφαρμογής Ιστού	Web Application
Ηγέτης	Leader

Ηλεκτρονικό Ταχυδρομείο	Email
Ημερομηνία Δημιουργίας	Date Of Creation
Ημερομηνία Τελευταίας Πρόσβασης Στο Αρχείο	Data At Last Access
Θετικά Παραδείγματα	Positive Examples
Ιδιόκτητα Αρχεία	Proprietary Files
Ιδιοκτήτη Του Αρχείου	File Owner
Ιδιωτικότητα	Privacy
Ιός	Virus
Κακόβουλο Λογισμικό	Malicious Software Malware
Κανόνες	Rules
Κανονισμούς	Regulations
Καταχωρημένα Δεδομένα	Registered Data
Κατεβάζουν	Download
Κατηγορίες	Categories
Κατηγορίες	Categories
Κατηγοριοποιητή	Classifier
Κεντρικά Γραφεία	Headquarters Office
Κοινά κανάλια επικοινωνίας δικτύου	Common Network Communications Channels

Κοινόχρηστα αρχεία	Share Files
Κρυπτογραφικές Συναρτήσεις Κατακερματισμού	Cryptographic Hash Functions
Κύκλο ζωής	Life Cycle
Λειτουργικού Συστήματος	Operating System
Λογισμικό	Software
Μέγεθος	Size
Μέγιστο	Maximum
Μέσων κοινωνικής δικτύωσης	Social Media
Μετά Δεδομένα	Meta-Data
Μη Δομημένο Περιεχόμενο	Unstructured Content
Μη Εξουσιοδοτημένη Μετάδοση	Unauthorized Transmission
Μηχανή εντοπισμού και κατηγοριοποίησης δεδομένων	Data Identification and Classification engine
Μηχανική Μάθηση	Machine Learning
Μοναδική	Unique
Νεφοϋπολογιστική	Cloud Computing
Παρεμβάσεις	Intrusiveness
Περιγραφικά Δεδομένα	Described Data

Περιεχόμενο	Content
Πιστωτικές Κάρτες	Visa Card
Πολιτική	Policy
Προέκταση Του Αρχείου	File Extension
Προκαθορισμένες Πολιτικές Και Ρυθμίσεις	Configuration Settings Και Policy Files
Προσωπικά δεδομένα	Personal Data
Πρότυπα	Standards
Προφίλ	Profile
Πρωτόκολλο Μεταφοράς Αρχείων	File Transfer Protocol
Πρωτόκολλο Μεταφοράς Υπερκείμενου	Hypertext Transport Protocol
Πρωτόκολλο Προσπέλασης Μηνυμάτων Διαδικτύου	Internet Message Access Protocol
Πρωτόκολλο Ταχυδρομείου	Post Office Protocol
Πρωτόκολλο Του Επιπέδου Εφαρμογής	Application Layer Protocol
Πύλες δικτύου	Gateways
Πυρήνα	Kernel
Σαρωτές Ευπαθειών	Vulnerability Scanners
Σκουλήκια	Worms
Σουίτες Εργαλείων Αποτροπής Απώλειας	Data Loss Prevention Suites

Δεδομένων	
Στοχοθετημένη Μηχανή	Targeted Machine
Συμβάν	Event
Συναρτήσεις Μιας Κατεύθυνσης	One Way Functions
Συνάρτηση Κατακερματισμού	Hash Function
Σύνδεση Στο Διαδίκτυο	Internet Connection
Συστήματα Ανίχνευσης Εισβολών	Intrusion Detection Systems-IDS
Συστήματα Πρόληψης Εισβολών	Intrusion Prevention Systems-IPS
Σφάλματα Λογισμικού	Software Bugs
Τελικος Χρήστης	End-User
Τερματικό	Endpoint
Τεχνητής Νοημοσύνης	Artificial Intelligence
Τομείς	Domains
Τοπικό Δίκτυο	Local Network
Τρέχουσα Διαδικασία	Running Process
Τρωτά Σημεία	Vulnerabilities
Τύπος Αρχείου	File Type
Υλικό	Hardware

Υπηρεσία	Service
Υποκαταστήματα	Branch Offices
Υπολογιστές Γραφείου	Desktop Pcs
Φορητοί Υπολογιστές	Laptops
Χαρακτηριστικά Γνωρίσματα	Feature Extraction
Χαρακτηριστικά Των Αρχείων	File Attribute
Ψευδώς Αρνητικά	False Negatives
Ψευδώς Θετικά	False Positives