ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΕΠΙΣΤΗΜΟΝΙΚΟ – ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Διακυβέρνηση Δεδομένων και Κυβερνοασφάλεια

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος, Κ. Τζοβανάκης

Επιβλέπων: Κωνσταντίνος Δεμέστιχας
Επίκ. Καθηγητής Γεωπονικού Πανεπιστημίου Αθηνών

Αθήνα, Ιούνιος 2024

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ Μ/Υ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ
ΤΜΗΜΑΤΟΣ ΒΙΟΜΗΧΑΝΙΚΗΣ ΔΙΟΙΚΗΣΗΣ & ΤΕΧΝΟΛΟΓΙΑΣ
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

ΔΙΕΠΙΣΤΗΜΟΝΙΚΟ – ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΤΕΧΝΟ-ΟΙΚΟΝΟΜΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Διακυβέρνηση Δεδομένων και Κυβερνοασφάλεια

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Γεώργιος, Κ. Τζοβανάκης

Επιβλέπων: Κωνσταντίνος Δεμέστιχας
Επίκ. Καθηγητής Γεωπονικού Πανεπιστημίου Αθηνών

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13η Ιουνίου 2024.

.....	.....	.....
Κωνσταντίνος Δεμέστιχας	Ευγενία Αδαμοπούλου	Ευστάθιος Συκάς
Επίκ. Καθηγητής Γεωπονικού Πανεπιστημίου Αθηνών	Ε.ΔΙ.Π. ΕΜΠ	Ομότιμος Καθηγητής ΕΜΠ

Αθήνα, Ιούνιος 2024

.....

Γεώργιος, Κ. Τζοβανάκης

Διπλωματούχος μεταπτυχιακού προγράμματος: «Τεχνοοικονομικά Συστήματα» της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Ε.Μ.Π.

Περίληψη

Η παρούσα εργασία εξετάζει δύο θεμελιώδεις τομείς της σύγχρονης ψηφιακής εποχής: τη διακυβέρνηση των δεδομένων και την κυβερνοασφάλεια. Η έρευνα αναδεικνύει την ανάγκη για ορθή διαχείριση και προστασία των δεδομένων ως ένα στρατηγικό πλεονέκτημα για τους οργανισμούς, το οποίο μπορεί να προωθήσει την καινοτομία και την ανάπτυξη. Η κυβερνοασφάλεια, αντιθέτως, επικεντρώνεται στην ανάλυση των αυξανόμενων απειλών που αντιμετωπίζουν οι ψηφιακές υποδομές και προτείνει τεχνολογικές λύσεις και διαδικασίες για την αποτελεσματική προστασία των δεδομένων.

Επιπλέον, η εργασία υπογραμμίζει τη σημασία της ανάπτυξης μιας ολοκληρωμένης στρατηγικής που συνδυάζει τις αρχές της διακυβέρνησης δεδομένων με τις πρακτικές της κυβερνοασφάλειας, με σκοπό την αντιμετώπιση των σύγχρονων ψηφιακών απειλών. Αυτή η προσέγγιση περιλαμβάνει την αξιοποίηση νέων τεχνολογιών, όπως το blockchain και η τεχνητή νοημοσύνη, οι οποίες δύνανται να αυτοματοποιήσουν τις διαδικασίες και να ενισχύσουν την ασφάλεια και τη διαφάνεια των δεδομένων.

Τέλος, τονίζεται η επιτακτική ανάγκη για συνεχή εκπαίδευση και ενημέρωση του ανθρώπινου δυναμικού, προκειμένου να αναγνωρίζονται και να αντιμετωπίζονται αποτελεσματικά οι εξελισσόμενες απειλές στον κυβερνοχώρο. Η ενσωμάτωση της κυβερνοασφάλειας στη συνολική επιχειρησιακή στρατηγική και η συμμόρφωση με τις σχετικές νομοθετικές ρυθμίσεις αποτελούν κρίσιμες παραμέτρους για την επίτευξη ανθεκτικότητας και ασφάλειας σε ένα δυναμικά μεταβαλλόμενο τεχνολογικό περιβάλλον.

- <u>Λέξεις Κλειδιά:</u> Διακυβέρνηση δεδομένων, Κυβερνοασφάλεια, Ψηφιακές απειλές, Διαχείριση Δεδομένων, Ασφάλεια Δεδομένων

Abstract

This thesis examines two fundamental areas of the contemporary digital era: data governance and cybersecurity. Highlights the need for proper management and protection of data as a strategic advantage for organizations, which can foster innovation and development. In contrast, cybersecurity focuses on analyzing the increasing threats faced by digital infrastructures and proposes technological solutions and processes for effective data protection.

Furthermore, the thesis emphasizes the importance of developing an integrated strategy that combines the principles of data governance with cybersecurity practices to address modern digital threats. This approach includes leveraging new technologies such as blockchain and artificial intelligence, which can automate processes and enhance the security and transparency of data.

Finally, underscores the urgent need for continuous education and training of human resources to effectively recognize and combat evolving cyber threats. Integrating cybersecurity into the overall business strategy and ensuring compliance with relevant legislative regulations are critical parameters for achieving resilience and security in a dynamically changing technological environment.

- Key words: Data Governance, Cybersecurity, Digital Threats, Data Management, Data Security

Πίνακας Περιεχομένων

Εικόνες

Εισαγωγή

Στη σύγχρονη ψηφιακή εποχή, η διακυβέρνηση δεδομένων και η κυβερνοασφάλεια αναδεικνύονται ως δύο ουσιαστικές διαστάσεις που διαμορφώνουν τον τρόπο λειτουργίας των επιχειρήσεων και των οργανισμών στον ψηφιακό κόσμο. Η πανταχού παρουσία της τεχνολογίας σε κάθε πτυχή της ζωής μας έχει επιφέρει μια αναπόφευκτη αύξηση στην πολυπλοκότητα και στις απειλές που αντιμετωπίζουν τα δεδομένα και οι ψηφιακοί πόροι.

Η Διακυβέρνηση Δεδομένων δεν αντιμετωπίζεται πλέον απλώς ως ένα σύνολο κανόνων και διαδικασιών για τη διαχείριση και την προστασία των δεδομένων, αλλά έχει εξελιχθεί σε έναν πυλώνα για την καινοτομία και την ανάπτυξη. Οι οργανισμοί αναγνωρίζουν την αξία των δεδομένων ως πόρο που μπορεί να τους προσφέρει ανταγωνιστικό πλεονέκτημα και να τους καθοδηγήσει προς στρατηγικές αποφάσεις. Μέσω μιας ολοκληρωμένης διακυβέρνησης δεδομένων, οι οργανισμοί μπορούν να εξασφαλίσουν την ορθή χρήση, ανάλυση και επεξεργασία των δεδομένων τους, προωθώντας την καινοτομία και την ανάπτυξη νέων προϊόντων και υπηρεσιών.

Από την άλλη πλευρά, η κυβερνοασφάλεια αποτελεί την απάντηση στις αυξημένες απειλές και επιθέσεις που αντιμετωπίζουν τα δεδομένα και οι ψηφιακοί πόροι. Η ασφάλεια των δεδομένων και η προστασία από κυβερνοεπιθέσεις απαιτούν μια ολοκληρωμένη προσέγγιση, που συμπεριλαμβάνει τεχνολογικά μέσα, διαδικασίες και εκπαίδευση του προσωπικού.

Η συνέργεια μεταξύ αυτών των δύο τομέων είναι κρίσιμη για την επίτευξη υψηλού επιπέδου ασφάλειας και προστασίας των δεδομένων. Μια ολοκληρωμένη προσέγγιση που συνδυάζει την ορθή διακυβέρνηση δεδομένων με αποτελεσματικά μέτρα κυβερνοασφάλειας ενισχύει την αντίληψη και την αντίδραση σε πιθανές απειλές, ενώ ταυτόχρονα διασφαλίζει τη συμμόρφωση με τους κανονισμούς και τις προδιαγραφές περί προστασίας δεδομένων. Μόνο μέσω μιας συνεκτικής και συνεχούς προσπάθειας μπορούν οι οργανισμοί να διασφαλίσουν την ασφάλεια, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων τους σε έναν πολύπλοκο και επικίνδυνο ψηφιακό κόσμο.

Συνεπώς, η ενσωμάτωση και η διασύνδεση της διακυβέρνησης δεδομένων και της κυβερνοασφάλειας αποτελούν κρίσιμα στοιχεία για την επίτευξη ανθεκτικότητας σε έναν διαρκώς μεταβαλλόμενο τεχνολογικό περιβάλλον. Οι προκλήσεις που ανακύπτουν είναι πολλαπλές και απαιτούν μια στρατηγική που ξεπερνά τα συμβατικά όρια της τεχνολογίας, εμπλέκοντας την εταιρική διακυβέρνηση, την εσωτερική πολιτική και την εξωτερική ρυθμιστική συμμόρφωση.

Η ανάγκη για διαρκή εκπαίδευση και ενημέρωση του ανθρώπινου δυναμικού γίνεται επιτακτική, καθώς οι απειλές εξελίσσονται και γίνονται πιο εξειδικευμένες. Οι οργανισμοί πρέπει να επενδύσουν σε προγράμματα συνεχούς κατάρτισης και ανάπτυξης δεξιοτήτων, ενισχύοντας την ικανότητα του προσωπικού να αναγνωρίζει και να αντιμετωπίζει τις κυβερνοαπειλές. Επιπλέον, οι οργανισμοί πρέπει να εξασφαλίζουν ότι οι πολιτικές και οι διαδικασίες τους είναι ευέλικτες και μπορούν να προσαρμόζονται γρήγορα σε νέα δεδομένα και καταστάσεις.

Η αξιοποίηση των νέων τεχνολογιών όπως το blockchain, τα μηχανικά μαθήματα και η τεχνητή νοημοσύνη μπορεί να προσφέρει σημαντικές λύσεις στην ενίσχυση της διακυβέρνησης δεδομένων και της κυβερνοασφάλειας. Αυτές οι τεχνολογίες διευκολύνουν την αυτοματοποίηση των διαδικασιών και την αποτελεσματική διαχείριση των ροών δεδομένων, ενώ παράλληλα προσφέρουν προηγμένες δυνατότητες παρακολούθησης και ανάλυσης, ενισχύοντας την ασφάλεια και τη διαφάνεια.

Τέλος, η ολοκληρωμένη στρατηγική διακυβέρνησης δεδομένων και κυβερνοασφάλειας απαιτεί μια πολυεπίπεδη προσέγγιση που συνδυάζει τεχνολογικές καινοτομίες, οργανωτικές πολιτικές, και νομική ρύθμιση. Η συνεχής προσαρμογή και εξέλιξη αυτών των στοιχείων συμβάλλει στην ενίσχυση της ασφάλειας και της ανθεκτικότητας των οργανισμών σε έναν αβέβαιο και δυναμικό ψηφιακό κόσμο.

1 Κυβερνοασφάλεια – Ορισμοί και Θεμελιώδη Θέματα

Η Κυβερνοασφάλεια αποτελεί ένα από τα πιο κρίσιμα και επίκαιρα θέματα στη σύγχρονη ψηφιακή εποχή. Καθώς οι τεχνολογικές εξελίξεις αυξάνουν την εξάρτησή μας από το διαδίκτυο και τις ψηφιακές υποδομές, η ασφάλεια των πληροφοριών και η προστασία των συστημάτων γίνονται ολοένα και πιο ζωτικής σημασίας.

Στο πλαίσιο αυτό, η Κυβερνοασφάλεια αποσκοπεί στην προστασία των δεδομένων, των δικτύων και των συστημάτων από απειλές όπως οι κυβερνοεπιθέσεις, οι χρήστες κακόβουλου λογισμικού και οι διαρροές πληροφοριών. Στόχος της είναι η διασφάλιση της εμπιστοσύνης και της ακεραιότητας των ψηφιακών συναλλαγών και επικοινωνιών, καθώς και η προαγωγή της ομαλής λειτουργίας των οργανισμών και των κοινωνιών.

Κατά τη διάρκεια της παρούσας εργασίας, θα εξερευνήσουμε τις βασικές έννοιες, τις τρέχουσες τάσεις και τις προκλήσεις που συναντά η Κυβερνοασφάλεια στον ψηφιακό κόσμο, καθώς και τις στρατηγικές και τις πρακτικές που χρησιμοποιούνται για την αντιμετώπισή τους.

1.1 Ορισμός και Σημασία της Κυβερνοασφάλειας

1.1.1 Ορισμός Κυβερνοασφάλειας

Η Κυβερνοασφάλεια αναφέρεται στο σύνολο των μέτρων και των πρακτικών που έχουν σχεδιαστεί για την προστασία των ψηφιακών συστημάτων, των δικτύων, των δεδομένων και των ψηφιακών υποδομών από κινδύνους, επιθέσεις και απειλές. Η Κυβερνοασφάλεια επιδιώκει την εξασφάλιση της ακεραιότητας, της εμπιστοσύνης και της διαθεσιμότητας των ψηφιακών πόρων και υπηρεσιών.

Πιο συγκεκριμένα, η πρακτική της προστασίας συστημάτων υπολογιστών, δικτύων και δεδομένων από μη εξουσιοδοτημένη πρόσβαση και κακόβουλες επιθέσεις. Σε μια εποχή όπου η πληροφορία αποτελεί τον πολυτιμότερο πόρο και οι ψηφιακές τεχνολογίες υποστηρίζουν και διαμορφώνουν την καθημερινότητά μας, η κυβερνοασφάλεια αποτελεί κρίσιμο κομμάτι για τη διασφάλιση της εμπιστοσύνης, της ακεραιότητας και της διαθεσιμότητας των ψηφιακών πόρων και υπηρεσιών. Εφαρμόζεται τόσο από ιδιώτες όσο και από επιχειρήσεις, μέσω της συλλογής λογισμικού, των διαδικασιών και των συστημάτων που σχεδιάζονται για το σκοπό αυτό. Καθώς η πολυπλοκότητα και η ποικιλομορφία των δεδομένων συνεχώς αυξάνεται και οι επιχειρήσεις επεκτείνονται στον διαδικτυακό χώρο, η κυβερνοασφάλεια αποτελεί επίκαιρο και κρίσιμο ζήτημα για την προστασία από τις κυβερνοεπιθέσεις και τις απειλές του ψηφιακού κόσμου. [11]

Η σημασία της Κυβερνοασφάλειας είναι ουσιώδης στην εποχή μας, καθώς ολοένα και περισσότερες δραστηριότητες μεταφέρονται στον ψηφιακό χώρο. Οι επιθέσεις και οι απειλές στον κυβερνοχώρο έχουν αυξηθεί σε αριθμό, πολυπλοκότητα και καταστροφικές συνέπειες, επηρεάζοντας οργανισμούς, κυβερνήσεις και ιδιώτες παγκοσμίως. Από την κλοπή εμπιστευτικών δεδομένων μέχρι την απειλή της εθνικής ασφάλειας, η Κυβερνοασφάλεια αποτελεί προτεραιότητα για κάθε οργανισμό που λειτουργεί στον ψηφιακό χώρο.

Στο πλαίσιο αυτό, η κατανόηση των βασικών αρχών και των συναφών εννοιολογικών πλαισίων της Κυβερνοασφάλειας αποτελεί αναγκαία προϋπόθεση για την αντιμετώπιση των προκλήσεων και την επίτευξη των στόχων της ασφάλειας στον ψηφιακό κόσμο.

1.1.2 Ορισμός Κυβερνοχώρου

Ο κυβερνοχώρος είναι ένας ψηφιακός χώρος που περιλαμβάνει όλα τα δίκτυα, υποδομές και τεχνολογίες που επιτρέπουν την επικοινωνία και ανταλλαγή δεδομένων μέσω της χρήσης ηλεκτρονικών συσκευών. Είναι ένας χώρος χωρίς φυσικά όρια, καθώς εκτείνεται παντού όπου υπάρχει πρόσβαση σε δίκτυο και ψηφιακή τεχνολογία. Η εξέλιξη του ίντερνετ και η αύξηση των συνδεδεμένων συσκευών έχουν κάνει τον κυβερνοχώρο μια ολοένα και πιο σημαντική έννοια στον σύγχρονο κόσμο. [11]

1.1.3 Συνέπειες της Κυβερνοασφάλειας

Η αποτυχία στην εφαρμογή και τη διατήρηση επαρκούς κυβερνοασφάλειας μπορεί να οδηγήσει σε σοβαρές συνέπειες για άτομα, επιχειρήσεις και κράτη. Από την απώλεια εμπιστευτικών πληροφοριών και την παραβίαση δεδομένων, μέχρι την οικονομική ζημία και τη ζημία στη φήμη, οι επιπτώσεις μπορεί να είναι καταστροφικές. Επίσης, οι κυβερνοεπιθέσεις μπορούν να επηρεάσουν κρίσιμες υποδομές όπως ενεργειακά δίκτυα, νοσοκομεία και μεταφορικά συστήματα, καθιστώντας τις απειλές αυτές ζήτημα εθνικής ασφάλειας.

Η ασφάλεια, σαν έννοια αλλά και ως πραγματικότητα σχετίζεται με πολλές υποπεριοχές από τις οποίες ξεχωρίζουν:

Εικόνα 1: Υποπεριοχές της Ασφάλειας

- ✓ **Φυσική Ασφάλεια (Physical security):** Αφορά την προστασία των φυσικών πόρων ή των πληροφοριών που είναι αποθηκευμένες σε ένα φυσικό μέσο.
- ✓ **Ασφάλεια Πληροφοριών (Information Security):** Είναι οι μηχανισμοί για τη θωράκιση της πληροφορίας, δηλαδή του αποτελέσματος της επεξεργασίας των δεδομένων.
- ✓ **Οικονομική Ασφάλεια (Financial Security):** Αυτή η κατηγορία αναφέρεται σε οικονομικές συναλλαγές, πωλήσεις και γενικότερα σε εκείνο το είδος πληροφορίας που σχετίζεται με την οικονομία. Είναι τα συστήματα που προστατεύουν τις ατομικές οικονομικές ελευθερίες.
- ✓ **Ασφάλεια Υπολογιστών (Computer Security):** Αναφέρεται στην προστασία των υπολογιστικών μονάδων από μη εξουσιοδοτημένη πρόσβαση μέσω κατάλληλων συστημάτων ελέγχου πρόσβασης και ισχυρής πολιτικής φυσικής ασφάλειας.
- ✓ **Ασφάλεια Δικτύων (Network Security):** Ορίζεται ως η διαδικασία λήψης προληπτικών μέτρων ως προς το φυσικό επίπεδο και το λογισμικό με στόχο την προστασία της δικτυακής υποδομής από μη εξουσιοδοτημένη πρόσβαση, κακή χρήση, δυσλειτουργία, τροποποίηση, καταστροφή ή ακατάλληλη αποκάλυψη.
- ✓ **Πρότυπα Ασφάλειας (Security standards):** Τα πρότυπα ασφαλείας είναι ένα οργανωμένο σύνολο από συγκεκριμένες κατευθυντήριες γραμμές που ένας

οργανισμός ή μια οργάνωση υποχρεούται να ακολουθεί για την ενίσχυση της ασφάλειάς του/της. Τα πρότυπα περιγράφουν λεπτομερώς τους τύπους υλικού και λογισμικού που πρέπει να χρησιμοποιούνται, το που, το πότε και το ποια είναι τα άτομα που μπορούν να χρησιμοποιούν το καθετί. Εκδίδονται από εθνικούς ή διεθνείς, δημόσιους και ιδιωτικούς, οργανισμούς προτύπων ασφαλείας. [12]

Η ασφάλεια δικτύων εμπεριέχει τέσσερις πολύ βασικές έννοιες, κάθε μία από τις οποίες σχετίζεται με διαφορετικού είδους προβλήματα:

- ✓ **Μυστικότητα (secrecy):** Διασφαλίζει ότι μη εξουσιοδοτημένοι χρήστες δε θα έχουν πρόσβαση σε απόρρητες πληροφορίες.
- ✓ **Πιστοποίηση αυθεντικότητας (authentication):** Η διαβεβαίωση ότι η οντότητα με την οποία γίνεται η επικοινωνία είναι πράγματι αυτή που ισχυρίζεται ότι είναι.
- ✓ **Μη απόρριψη υποχρέωσης ή οφειλής (non-repudiation):** Παρέχει προστασία απέναντι στην άρνηση μιας οντότητας που συμμετέχει στην επικοινωνία ότι δεν το έχει πράξει. Αποδεικνύει ότι μία οντότητα πράγματι έστειλε ή έλαβε ένα μήνυμα.
- ✓ **Έλεγχος ακεραιότητας (integrity control):** Η εξακρίβωση ότι τα δεδομένα που ελήφθησαν είναι ακριβώς αυτά που εστάλησαν από μία εξουσιοδοτημένη οντότητα, δεν έχει παρεισφρήσει δηλαδή κάποια τροποποίηση από έναν τρίτο.

1.1.4 Προκλήσεις στην Κυβερνοασφάλεια

Με την αυξανόμενη εξάρτηση από τις ψηφιακές τεχνολογίες, οι προκλήσεις στον τομέα της κυβερνοασφάλειας γίνονται περισσότερο περίπλοκες και πολυδιάστατες. Η κλίμακα και η ευρυτέρητα των ψηφιακών δικτύων σημαίνει ότι οι απειλές μπορεί να προέλθουν από πολλαπλές πηγές, συμπεριλαμβανομένων κρατικών φορέων, οργανωμένων εγκληματικών ομάδων, και απλών ατόμων που επιδιώκουν να εκμεταλλευτούν τεχνολογικά κενά. Η πολυπλοκότητα των πληροφοριακών συστημάτων και η διαρκής εξέλιξη των τεχνολογιών δημιουργούν σημαντικές προκλήσεις στην ανίχνευση, πρόληψη και αντιμετώπιση κυβερνοαπειλών. [11], [12]

Κρίσιμοι τομείς, όπως οι μεταφορές, η ενέργεια, η υγεία και ο χρηματοοικονομικός κλάδος, εξαρτώνται όλο και περισσότερο από τις ψηφιακές τεχνολογίες για την άσκηση των βασικών δραστηριοτήτων τους. Παρότι η ψηφιοποίηση προσφέρει τεράστιες ευκαιρίες και δίνει λύσεις σε πολλές από τις προκλήσεις που αντιμετωπίζει η Ευρώπη, μεταξύ άλλων και κατά τη διάρκεια της κρίσης της COVID-19, εκθέτει επίσης την οικονομία και την κοινωνία σε κυβερνοαπειλές.

1.1.5 Κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση

Η Κυβερνοασφάλεια αποτελεί προτεραιότητα για την Ευρωπαϊκή Ένωση (ΕΕ) καθώς αντιμετωπίζει τις συνεχώς εξελισσόμενες απειλές στον ψηφιακό τομέα. Με την αύξηση των κυβερνοεπιθέσεων και των προκλήσεων στον ψηφιακό χώρο, η ΕΕ έχει αναγνωρίσει την ανάγκη για ενιαίες προσεγγίσεις και συνεργασία μεταξύ των κρατών μελών για την προστασία των ψηφιακών υποδομών και των πολιτών της. [13]

1.1.6 Πολιτικές και Πρωτοβουλίες της ΕΕ για την Κυβερνοασφάλεια

Η ΕΕ έχει υιοθετήσει πολλές πολιτικές και πρωτοβουλίες για την ενίσχυση της κυβερνοασφάλειας εντός του κοινού χώρου της. Η Διαδικτυακή Ασφάλεια και Προστασία (Cybersecurity Strategy) της ΕΕ, για παράδειγμα, προβλέπει τη δημιουργία ενός ενιαίου πλαισίου για την αντιμετώπιση των κυβερνοεπιθέσεων και την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών.

Η ΕΕ έχει επίσης εγκρίνει νομοθεσία που αφορά την κυβερνοασφάλεια, περιλαμβανομένου του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) που θεσπίζει αυστηρές απαιτήσεις για την προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ.

Με την ανάπτυξη κοινών στόχων και προσεγγίσεων, η ΕΕ και τα κράτη μέλη συνεργάζονται ενεργά στον τομέα της κυβερνοασφάλειας. Αυτή η συνεργασία περιλαμβάνει την ανταλλαγή πληροφοριών, την ανάπτυξη κοινών πρακτικών και την ενίσχυση των ψηφιακών ικανοτήτων σε επίπεδο ΕΕ.

Μέσω αυτών των πρωτοβουλιών και της ενιαίας δράσης, η ΕΕ επιδιώκει να ενισχύσει την αντίληψη και την προστασία των πολιτών και των οργανισμών της από τις απειλές στον ψηφιακό χώρο και να προωθήσει ένα ασφαλές και αξιόπιστο ψηφιακό περιβάλλον. [13]

1.1.7 Τεχνολογίες Κυβερνοασφάλειας

Για την αντιμετώπιση κυβερνοαπειλών, χρησιμοποιούνται διάφορες τεχνολογίες. Ανάμεσα σε αυτές, τα αντιιικά προγράμματα, τα συστήματα ανίχνευσης και πρόληψης εισβολών, η κρυπτογράφηση δεδομένων και οι προηγμένες τεχνολογίες τεχνητής νοημοσύνης και μηχανικής μάθησης χρησιμοποιούνται για την ανάλυση του κυβερνοχώρου και την πρόβλεψη

κυβερνοεπιθέσεων. Οι τεχνολογίες αυτές επιτρέπουν την ταχύτερη αντίδραση σε απειλές και την αυτοματοποίηση πολλών διαδικασιών ασφαλείας.

1.2 Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

Η διαδικασία της ψηφιακής εξέλιξης αντιπροσωπεύει μια αναπόφευκτη πραγματικότητα, η οποία δεν μόνο ότι πρέπει, αλλά θα πρέπει να αντιμετωπιστεί με στρατηγικότητα και σύνεση. Κατά την επόμενη περίοδο, οι τεχνολογικές καινοτομίες αναμένεται να αποτελέσουν τους θεμέλιους λίθους της ανάπτυξης, παρέχοντας στις επιχειρήσεις και τους οργανισμούς μοναδικές ευκαιρίες, τις οποίες δεν έχουν προηγουμένως γνωρίσει, καθώς δημιουργούν αξία και ανταγωνιστικό πλεονέκτημα. Ωστόσο, για να αποσπάσουν τα μέγιστα οφέλη από την ψηφιακή μετάβαση, οι οργανισμοί αντιμετωπίζουν την ανάγκη για μια εκσυγχρονισμένη και αποτελεσματική στρατηγική Κυβερνοασφάλειας. Αυτή η στρατηγική πρέπει να κατευθύνει τον οργανισμό προς την επίτευξη μέγιστου επιπέδου ασφάλειας, προετοιμάζοντάς τον για την αντιμετώπιση πιθανών κυβερνοεπιθέσεων. Καθώς οι νέες τεχνολογίες παράγουν τη φαινομενική αναταραχή που είναι γνωστή ως "ψηφιακή διατάραξη", εισάγοντας νέες μορφές απειλών στον κυβερνοχώρο και ενισχύοντας τις υπάρχουσες, είναι αναγκαία η ανάπτυξη προηγμένων δεξιοτήτων επόμενης γενιάς. Οι οργανισμοί πρέπει να είναι σε θέση να αναγνωρίζουν συνεχώς τις ευκαιρίες και τους κινδύνους που σχετίζονται με την ψηφιακή καινοτομία, να εξισορροπούν την ανάγκη για προστασία από τις υφιστάμενες απειλές με την ανάγκη υιοθέτησης νέων στρατηγικών, οι οποίες εκμεταλλεύονται την ψηφιακή τεχνολογία και διαμορφώνουν τις βάσεις για την αειφόρο ανάπτυξη. Σε αυτό το πλαίσιο, οι οργανισμοί πρέπει να αναπτύξουν βαθιά κατανόηση του προφίλ κινδύνου τους, να αξιολογήσουν το υφιστάμενο επίπεδο των μηχανισμών ασφάλειας και να καταρτίσουν ολοκληρωμένο πρόγραμμα Κυβερνοασφάλειας για την προστασία τους από τους κινδύνους του κυβερνοχώρου. [13]

1.2.1 Τάσεις που διαμορφώνουν την Κυβερνοασφάλεια στην εποχή μας

Απουσία οριοθέτησης:

Οι νέες τεχνολογίες, όπως το υπολογιστικό νέφος, επιβραδύνουν τη διάκριση μεταξύ των τεχνολογικών ορίων και της περιφέρειας που πρέπει να προστατευθεί από έναν οργανισμό.

Νέες τεχνολογίες:

Η αυξημένη εφαρμογή νέων τεχνολογιών, όπως η ρομποτική, η αυτοματοποίηση, η τεχνητή νοημοσύνη και η ευέλικτη ανάπτυξη (agile), διαμορφώνουν την ταχύτητα της επιχειρηματικής και τεχνολογικής καινοτομίας, αυξάνοντας ταυτόχρονα τους κινδύνους στον Κυβερνοχώρο και πολλαπλασιάζοντας την πολυπλοκότητα των προγραμμάτων προστασίας των οργανισμών, τα οποία συχνά βασίζονται σε παραδοσιακές προσεγγίσεις και μεθόδους.

Διαδίκτυο των Πραγμάτων (IoT):

Είτε πρόκειται για έξυπνους αισθητήρες σε ένα έξυπνο εργοστάσιο είτε για απομακρυσμένη σύνδεση με μια αντλία ινσουλίνης, το IoT αναμένεται να επιφέρει θετικές επιπτώσεις στη ζωή μας. Ωστόσο, οι αυξημένοι κίνδυνοι στον Κυβερνοχώρο και οι σημαντικές επιπτώσεις παραβίασης ενδέχεται να αποτρέψουν την ανάπτυξη ή την αποδοχή αυτών των τεχνολογιών. [9]

Δίκτυα φορητών συσκευών:

Οι φορητές συσκευές δεν αποτελούν μόνο εργαλείο, αλλά αποτελούν επίσης έναν τρόπο ζωής. Δημιουργούνται νέες συμπεριφορές που σημαντικά επεκτείνουν το πεδίο και το εύρος των Κυβερνοεπιθέσεων, καθώς τα δίκτυα φορητών συσκευών είναι φυσικά γεωγραφικά διασκορπισμένα και ανομοιογενή. [9]

Αναίρεση των ορίων μεταξύ επαγγελματικής και προσωπικής ζωής:

Η ευρεία χρήση των προσωπικών μας συσκευών για επαγγελματικούς σκοπούς, αλλά και για την πρόσβαση σε κοινωνικά δίκτυα, έχει ως αποτέλεσμα την ανάμιξη προσωπικών και επιχειρηματικών δεδομένων, δυσχεραίνοντας την ασφάλειά τους.

Τεχνητή νοημοσύνη:

Η εισαγωγή της τεχνητής νοημοσύνης ως συμπληρωματικού ή αντικαταστατικού παράγοντα για τους εξειδικευμένους επαγγελματίες οδηγεί σε βελτιωμένες δυνατότητες και μειωμένο κόστος.

Ωστόσο, δημιουργεί νέους κινδύνους, όπως οι chatbots, οι οποίοι με κακόβουλη παρέμβαση μπορούν να λειτουργήσουν ως εργαλεία του επιτιθέμενου. [9]

Εξέλιξη και καινοτομία:

Οι καινοτόμοι οργανισμοί δημιουργούν νέα ψηφιακά μοντέλα παροχής υπηρεσιών, τα οποία προκαλούν προκλήσεις Κυβερνοασφάλειας σε όλα τα επίπεδα του οργανισμού.

Συνεργατικές πλατφόρμες:

Τα λογισμικά που ενσωματώνουν τα κοινωνικά δίκτυα σε επιχειρηματικές διαδικασίες μπορούν να επιταχύνουν την προώθηση της καινοτομίας, αλλά ταυτόχρονα αυξάνουν την εκθέσεων σε εξωτερικούς κινδύνους.

1.3 Η Σύγχρονη Εποχή ορίζει «Ασφάλεια Παντού»

Η διαχείριση κινδύνων στον Κυβερνοχώρο είναι μια δυναμικά μεταβαλλόμενη διαδικασία, βρίσκεται σε συνεχή εξέλιξη και μεταβάλλεται σύμφωνα με το εκάστοτε περιβάλλον απειλών. Η απεικόνιση της εξέλιξης του περιβάλλοντος Κυβερνοασφάλειας τα τελευταία δώδεκα χρόνια εμφανίζει ξεκάθαρα την ανάγκη για ολιστική προσέγγιση, εστιάζοντας στηνπρόληψη ώστε να βρει σε θέση ισχύος τους οργανισμούς.

1.3.1 Περίοδος 2008-2012: Εποχή Συμμόρφωσης

Κατά τη διάρκεια αυτής της περιόδου, η Κυβερνοασφάλεια καθιερώνεται ως κρίσιμος παράγοντας για τη λειτουργία των οργανισμών. Η έννοια της συμμόρφωσης αναδεικνύεται ως βασική αρχή, με την θέσπιση των πρώτων σημαντικών κανονιστικών προτύπων που θέτουν τις ελάχιστες απαιτήσεις για την προστασία των πληροφοριών και την ασφάλεια των συστημάτων. Οι οργανισμοί βρίσκονται υπό την πίεση να προσαρμοστούν σε αυτά τα νέα πρότυπα και να εφαρμόσουν αποτελεσματικά πολιτικές και διαδικασίες για τη διαχείριση των κυβερνοασφαλειακών κινδύνων.

1.3.2 Περίοδος 2012-2018: Εποχή Κινδύνου

Κατά τη διάρκεια αυτής της περιόδου, η Κυβερνοασφάλεια εξελίσσεται από τεχνικό θέμα σε επιχειρησιακό πρόβλημα, καθώς παρατηρούνται σημαντικά διεθνή περιστατικά παραβίασης. Αυτά τα γεγονότα αναδεικνύουν την ανάγκη για δημιουργία πλαισίων διαχείρισης κινδύνων και ενίσχυσης της ανθεκτικότητας των οργανισμών. Επιπλέον, οι οργανισμοί συνειδητοποιούν τη σημασία της πρόληψης και της έγκαιρης αντίδρασης σε επιθέσεις και παραβιάσεις. [13]

1.3.3 Περίοδος 2018-2024: Νέα εποχή με γνώμονα την Ασφάλεια Παντού

Η εμφάνιση νέων τεχνολογιών όπως η ψηφιοποίηση, το υπολογιστικό νέφος, το Internet of Things και η τεχνητή νοημοσύνη απαιτεί μια νέα προσέγγιση στην Κυβερνοασφάλεια. Ενώ οι αυξημένοι κίνδυνοι είναι προφανείς, η έμφαση δίνεται στη διαχείριση κινδύνων εκτός της περιοχής ελέγχου των οργανισμών, καθώς και στη συνεργασία μεταξύ των ενδιαφερόμενων φορέων για την αντιμετώπιση των κοινών απειλών. Αυτή η νέα εποχή επιβάλλει την ανάγκη για συνεχή εκπαίδευση, καινοτομία και προοπτική ευαισθητοποίησης στον τομέα της Κυβερνοασφάλειας. [13]

1.4 Η απειλή είναι μεγαλύτερη από ποτέ

Η απειλή στον κυβερνοχώρο είναι πιο εκτεταμένη και πιο σύνθετη από ποτέ. Αν αναλογιστούμε το ευρύτερο τεχνολογικό περιβάλλον ως ένα «πεδίο μάχης», θα διαπιστώσουμε ότι βρισκόμαστε αντιμέτωποι με μια συνεχή αντιπαράθεση όπου οι επιθέσεις προέρχονται από διάφορους εχθρούς και γίνονται με ποικίλα μέσα και μεθόδους. Οι κακόβουλοι στον κυβερνοχώρο, εξελισσόμενοι συνεχώς, δεν περιορίζονται μόνο στους οικονομικούς στόχους, αλλά επιδιώκουν επίσης πολιτικούς, κοινωνικούς ή ακόμα και ιδεολογικούς σκοπούς. [13]

1.4.1 Επιτιθέμενοι:

- ✓ Ανταγωνιστές και ανταγωνιστικές επιχειρήσεις που επιδιώκουν να κλονίσουν την ανταγωνιστική τους θέση.

- ✓ Τρίτα μέρη που μπορεί να είναι οργανωμένες εγκληματικές ομάδες, κρατικές υπηρεσίες ή ακόμα και χώρες που επιδιώκουν να αποκτήσουν πλεονέκτημα σε γεωπολιτικό επίπεδο.
- ✓ Εσωτερικοί χρήστες με κακόβουλες προθέσεις ή ακόμα και με αμέλεια στην ασφάλεια.

1.4.2 Πολύτιμα αγαθά:

- ✓ Οικονομικά δεδομένα που μπορούν να οδηγήσουν σε οικονομικές απώλειες ή επιπλέον πλεονεξία.
- ✓ Προσωπικά δεδομένα των πελατών που μπορούν να χρησιμοποιηθούν για απάτες ή κλοπή ταυτότητας.
- ✓ Στρατηγικά σχέδια και εμπιστευτικές πληροφορίες που μπορούν να επηρεάσουν την ανταγωνιστική θέση ή την πολιτική στρατηγική ενός οργανισμού.
- ✓ Πνευματική ιδιοκτησία που αποτελεί τον πυρήνα της καινοτομίας και του ανταγωνιστικού πλεονεκτήματος.
- ✓ Εγκαταστάσεις και υποδομές που αποτελούν το ζωτικό αναπαραγωγικό σύστημα ενός οργανισμού.

1.4.3 Μέθοδοι απειλής:

- ✓ Επιθέσεις ransomware που κρυπτογραφούν δεδομένα και απαιτούν λύτρα για την αποκρυπτογράφησή τους.
- ✓ Κοινωνική μηχανική και phishing που εκμεταλλεύονται την ανθρώπινη αφέλεια για την πρόσβαση σε ευαίσθητες πληροφορίες.
- ✓ Εκμετάλλευση ευπαθειών στο λογισμικό ή το υλικό ενός συστήματος για την αποκτήση πρόσβασης ή την παράκτιση βλαβών.
- ✓ Χρήση τεχνητής νοημοσύνης για την εντοπισμό ευπαθειών και την αυτοματοποιημένη επίθεση.
- ✓ Επιθέσεις στην εφοδιαστική αλυσίδα για να διακινδυνευθεί η ακεραιότητα των προϊόντων ή να προκαλείται ανεπανόρθωτη ζημιά. [12]

1.4.4 Επιπτώσεις:

- ✓ Κλοπή δεδομένων που μπορεί να οδηγήσει σε χρηματοοικονομικές απώλειες ή καταστροφική επίθεση στην επιχείρηση.
- ✓ Καταστροφική βλάβη στο ηλεκτρονικό ή φυσικό περιβάλλον του οργανισμού.
- ✓ Διακοπή της διαθεσιμότητας των υπηρεσιών μέσω επιθέσεων όπως οι DDoS.
- ✓ Αλλοίωση ή καταστροφή δεδομένων που μπορεί να έχει μακροπρόθεσμες συνέπειες στη λειτουργία του οργανισμού.
- ✓ Αρνητική δημοσιότητα που θα ζημιώσει τη φήμη και την εμπιστοσύνη των πελατών και του κοινού.
- ✓ Κίνδυνος για την ανθρώπινη ασφάλεια και το περιβάλλον, ειδικά σε βιομηχανικά περιβάλλοντα όπου η απότομη διακοπή των υπηρεσιών μπορεί να έχει σοβαρές συνέπειες.

1.5 Ομάδες Απειλών

Καθώς εξετάζουμε τους πιθανούς κινδύνους στον κυβερνοχώρο, πρέπει να δώσουμε ιδιαίτερη προσοχή στην απειλή που προέρχεται από τους εσωτερικούς χρήστες. Οι εργαζόμενοι και άλλα εξουσιοδοτημένα άτομα εντός του οργανισμού μπορούν να αποτελέσουν μια σημαντική πηγή κινδύνου, είτε προκαλώντας εσκεμμένα προβλήματα είτε λόγω αμέλειας ή έλλειψης επίγνωσης των κινδύνων. Από τη μια πλευρά, μπορεί να υπάρχουν εργαζόμενοι που προσπαθούν να εκμεταλλευτούν την πρόσβασή τους σε ευαίσθητες πληροφορίες για προσωπικό ή οικονομικό όφελος, ενώ από την άλλη πλευρά, μπορεί να υπάρχουν περιστατικά κακής χρήσης που οφείλονται σε αμέλεια ή έλλειψη κατάλληλης εκπαίδευσης.

Αναφορικά με το οργανωμένο έγκλημα, πρέπει να γνωρίζουμε ότι αυτές οι ομάδες είναι επαγγελματίες στην εκμετάλλευση ευπαθειών συστημάτων και δικτύων για να επιτύχουν τους στόχους τους. Η εμφάνιση τέτοιων επιθέσεων μπορεί να είναι παγκόσμια και δύσκολα ανιχνεύσιμη, καθώς αυτοί οι επιτιθέμενοι συχνά δρουν με διακριτικότητα και χρησιμοποιούν πολυεπίπεδες τεχνικές για να κρύψουν τα ίχνη τους. Οι αντικειμενικοί τους είναι συνήθως οικονομικά κίνητρα, αλλά ενίοτε μπορεί να πρόκειται και για προσωπικές αντιξοότητες ή πολιτικά κίνητρα.

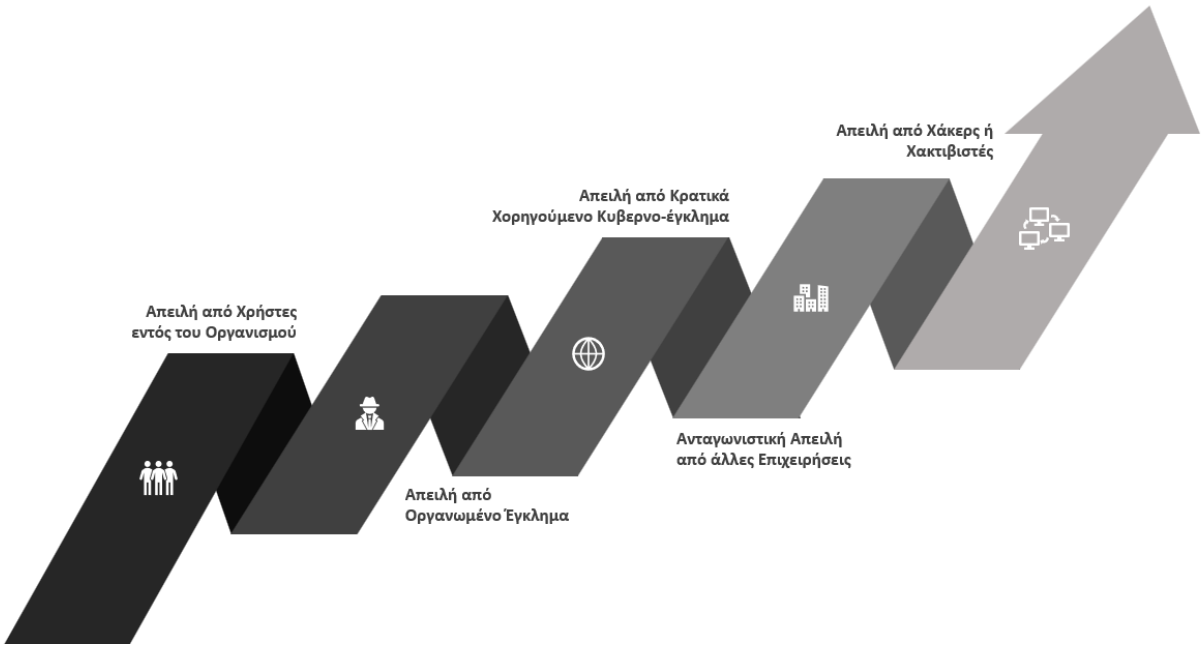
Επιπλέον, η απειλή από κρατικά χορηγούμενο κυβερνο-έγκλημα αποτελεί σημαντικό κίνδυνο για πολλούς οργανισμούς. Σε αυτήν την περίπτωση, κρατικοί φορείς μπορεί να επιδιώκουν τη διείσδυση ή την επιθετική ενέργεια ενάντια σε εταιρείες ή κυβερνητικά συστήματα για πολιτικά, οικονομικά ή κατασκοπευτικά κίνητρα. Οι επιπτώσεις μπορεί να είναι σοβαρές, καθώς η κλοπή

πληροφοριών ή η διακοπή της λειτουργίας μπορεί να προκαλέσει σημαντική οικονομική απώλεια ή ακόμα και να θέσει σε κίνδυνο την εθνική ασφάλεια. [13]

Επιπλέον, η ανταγωνιστική απειλή από άλλες επιχειρήσεις μπορεί να είναι σημαντική, καθώς οι ανταγωνιστές επιδιώκουν συχνά το ανταγωνιστικό πλεονέκτημα μέσω της πρόσβασης σε εμπιστευτικές πληροφορίες ή τη διατάραξη των δραστηριοτήτων του οργανισμού. Αυτό μπορεί να οδηγήσει σε σοβαρές επιπτώσεις για τη φήμη, την οικονομική απόδοση και την κατάσταση της αγοράς.

Τέλος, οι χάκερς ή οι χακτιβιστές αποτελούν μια σημαντική απειλή, καθώς μπορεί να επιδιώκουν την προσοχή ή την αύξηση της δημοτικότητάς τους μέσω διαφόρων ενεργειών. Αυτοί οι επιτιθέμενοι είναι πολύ ποικίλοι στα κίνητρά τους και μπορεί να προκαλέσουν πλήγμα στη φήμη του οργανισμού, διακόπτοντας τις λειτουργίες του ή κλέβοντας πληροφορίες. Επομένως, η απειλή από αυτούς τους παράγοντες πρέπει να ληφθεί σοβαρά υπόψη και να αντιμετωπιστεί με κατάλληλα μέτρα ασφαλείας και προληπτικές δράσεις.

Συνοπτικά, οι ομάδες απειλών της κυβερνοασφάλειας αποτυπώνονται στο παρακάτω σχήμα:



Εικόνα 2: Ομάδες Απειλών Κυβερνοασφάλειας

Σε ένα ευρύ πλαίσιο, τα κίνητρα που οδηγούν τους επιτιθέμενους στον κυβερνοχώρο είναι πολλαπλά και οι επιπτώσεις που προκύπτουν από τις κυβερνοεπιθέσεις μπορούν να είναι σημαντικές και δυσμενείς για τους στόχους τους. Οι επενδυτές, οι κυβερνήσεις και οι ρυθμιστικές αρχές απαιτούν όλο και περισσότερο από τις Διοικήσεις να επιδείξουν ενεργά την επιμέλεια στην πρόληψη, την αντιμετώπιση και τη μείωση των πιθανών επιπτώσεων σε περίπτωση περιστατικών κυβερνοασφάλειας, είτε αυτά προκαλούνται ακούσια είτε από σκόπιμες κυβερνοεπιθέσεις.

Τα συνήθη κίνητρα των κυβερνοεγκληματιών είναι ποικίλα και συχνά προσδιορίζονται από τις ανάγκες και τους στόχους τους. Σε πολλές περιπτώσεις, επιδιώκουν να ενισχύσουν τη φήμη τους μέσω των επιθέσεων, ενώ σε άλλες προσπαθούν να εξασφαλίσουν οικονομικό όφελος μέσω της κλοπής στοιχείων, όπως τραπεζικών ή πιστωτικών καρτών, ή ακόμα και πνευματικής ιδιοκτησίας για ανταγωνιστικό πλεονέκτημα. Τα ransomware επίσης αποτελούν δημοφιλή μέσο εκβιασμού για την κλείδωση δεδομένων με σκοπό την απόκτηση χρηματικής ανταμοιβής. Επιπλέον, κάποιες φορές οι κυβερνοεγκληματίες μπορεί να επιδιώκουν πολιτικά ή εθνικά κίνητρα, επιθυμώντας να προκαλέσουν πλήγμα στη φήμη ενός οργανισμού ή ακόμα και μιας ολόκληρης χώρας.

Οι επιπτώσεις των κυβερνοεπιθέσεων μπορούν να είναι σοβαρές και ποικίλες. Μπορεί να υπάρξουν οικονομικές κυρώσεις σε μορφή προστίμων από κρατικούς ή ρυθμιστικούς φορείς, ενώ η αρνητική δημοσιότητα που προκαλείται μπορεί να οδηγήσει σε μείωση της αξίας του οργανισμού και στη μείωση της εμπιστοσύνης από πελάτες και προμηθευτές. Επιπλέον, η κλοπή πνευματικής ιδιοκτησίας μπορεί να προκαλέσει μακροχρόνιες ζημιές στον οργανισμό, ενώ η απώλεια ή η αδυναμία πρόσβασης σε περιουσιακά στοιχεία ή πληροφορίες μπορεί να οδηγήσει σε καθυστερήσεις ή ακόμα και αποτυχία παράδοσης προϊόντων ή υπηρεσιών. Τέλος, οι διοικητικοί πόροι που αφιερώνονται στην αντιμετώπιση των κυβερνοεπιθέσεων μπορούν να επηρεάσουν τη λειτουργικότητα του οργανισμού και να οδηγήσουν σε οικονομικές απώλειες. Έτσι, η αντιμετώπιση των κυβερνοεπιθέσεων απαιτεί στρατηγική προσέγγιση και ανάληψη δράσης με βάση τις συνέπειες που μπορούν να προκύψουν.

Τονίζοντας τη σημασία της κυβερνοασφάλειας, η αύξηση των ψηφιοποιημένων επιχειρησιακών λειτουργιών συνοδεύεται από αυξημένο κίνδυνο ψηφιακής εκθεσιμότητας στον κυβερνοχώρο. Αυτός ο κίνδυνος δεν περιορίζεται μόνο στα συστήματα πληροφορικής (IT), αλλά επεκτείνεται και στην ανθρώπινη ζωή, τις βιομηχανικές υποδομές και το περιβάλλον. Η προσέγγιση της κυβερνοασφάλειας πρέπει να λαμβάνει υπόψη τη συνδυαστική φύση των απειλών, οι οποίες προέρχονται από διάφορες πτυχές της ψηφιακής παρουσίας των οργανισμών.

Καθώς οι επιπτώσεις των ασφαλειακών περιστατικών μπορούν να επηρεάσουν τη λειτουργία ολόκληρων κοινοτήτων και την οικονομία, η αντιμετώπιση της κυβερνοασφάλειας αποτελεί

κρίσιμη προτεραιότητα για τους οργανισμούς και τις κυβερνήσεις. Μέσω ολοκληρωμένων προσεγγίσεων, που περιλαμβάνουν τη συνεργασία μεταξύ των διαφόρων ενδιαφερόμενων φορέων και την εφαρμογή προληπτικών μέτρων, είναι δυνατόν να ενισχυθεί η ανθεκτικότητα των συστημάτων και να μειωθεί η επιρροή των επιθέσεων. Μέσω συνεχούς παρακολούθησης, ανάλυσης και ενημέρωσης για τις αλλαγές στον κυβερνοχώρο, οι οργανισμοί μπορούν να αναπτύξουν ευέλικτες και αποτελεσματικές στρατηγικές για την αντιμετώπιση των σύγχρονων απειλών στην κυβερνοασφάλεια.

1.6 Βέλτιστες πρακτικές Κυβερνοασφάλειας

Οι βέλτιστες πρακτικές κυβερνοασφάλειας συνιστούν μια συνολική προσέγγιση για την προστασία των ψηφιακών περιουσιών και την εξασφάλιση της ακεραιότητας και της ανθεκτικότητας των οργανισμών έναντι κυβερνοεπιθέσεων. Αυτή η προσέγγιση απαιτεί τη συνεργασία διαφόρων τομέων εντός ενός οργανισμού και την υιοθέτηση ενός συνολικού πλαισίου πολιτικών, τεχνολογικών μέτρων και διαδικασιών για την αντιμετώπιση των κινδύνων και την προστασία των ευαίσθητων πληροφοριών.

Μια συνολική προσέγγιση περιλαμβάνει πρώτα την ανάλυση και την κατανόηση των κινδύνων που αντιμετωπίζει ένας οργανισμός, συμπεριλαμβανομένων των εσωτερικών και εξωτερικών απειλών και των ευπαθειών του συστήματός του. Με βάση αυτήν την ανάλυση, αναπτύσσονται και υλοποιούνται πολιτικές ασφαλείας που ορίζουν τις αρχές και τις πρακτικές για την προστασία των πληροφοριών και των ψηφιακών περιουσιών.

Επιπλέον, η εφαρμογή τεχνολογικών μέτρων ασφαλείας είναι κρίσιμη για την προστασία των συστημάτων και των δεδομένων. Αυτά τα μέτρα μπορεί να περιλαμβάνουν την κρυπτογράφηση των δεδομένων, την εφαρμογή μηχανισμών ελέγχου πρόσβασης, τη χρήση λογισμικού ανίχνευσης και αντίδρασης σε επιθέσεις, καθώς και την ανάπτυξη πυραμίδων προστασίας για την αποτροπή εισβολών.

Επιπλέον, η εκπαίδευση και η ευαισθητοποίηση του προσωπικού είναι ουσιώδης για την αναγνώριση και την αντιμετώπιση των κινδύνων κυβερνοασφάλειας. Οι εργαζόμενοι πρέπει να εκπαιδευθούν για τις απειλές που αντιμετωπίζονται και τα βήματα που πρέπει να ακολουθήσουν σε περίπτωση παραβίασης της ασφάλειας.

Επιπλέον, η προσέγγιση των βέλτιστων πρακτικών κυβερνοασφάλειας πρέπει να είναι ευέλικτη και προσαρμοσμένη στις εξελίξεις του κυβερνοχώρου και τις νέες τεχνικές επιθέσεις. Αυτό σημαίνει ότι οι πολιτικές και οι τεχνολογικές πρακτικές πρέπει να αναθεωρούνται και να

ενημερώνονται τακτικά για να αντιμετωπίζουν τις αναδυόμενες απειλές και να προστατεύουν την ψηφιακή υποδομή του οργανισμού. [12]

1.7 Πως ψηφιακές τεχνολογίες βοηθούν στη διαχείριση κινδύνων

Η διαχείριση κινδύνων είναι ένας κρίσιμος παράγοντας για την επιτυχή λειτουργία και τη διατήρηση της ανταγωνιστικότητας ενός οργανισμού. Οι ψηφιακές τεχνολογίες προσφέρουν ένα ευρύ φάσμα εργαλείων και δυνατοτήτων που μπορούν να αναβαθμίσουν τη διαδικασία αυτή, ενώ ταυτόχρονα εισάγουν νέους κινδύνους που πρέπει να αντιμετωπιστούν. Ας αναλύσουμε τους τρεις βασικούς τρόπους με τους οποίους οι ψηφιακές τεχνολογίες επηρεάζουν τη διαχείριση κινδύνων:

1.7.1 Αποτελεσματικότητα:

Η χρήση ψηφιακών τεχνολογιών οδηγεί σε μείωση κόστους και επιτάχυνση των διαδικασιών διαχείρισης κινδύνων. Η εφαρμογή εργαλείων όπως η ρομποτική διαδικασία αυτοματοποίησης (RPA) επιτρέπει την αυτοματοποίηση επαναλαμβανόμενων και χρονοβόρων διαδικασιών, ενώ η αυτοματοποίηση της δημιουργίας αναφορών ύποπτης δραστηριότητας με χρήση αναγνώρισης γλώσσας βελτιώνει τη διαχείριση ενδεχόμενων απειλών. Επιπλέον, η τεχνολογία chatbot μπορεί να επιταχύνει την εύρεση κανονιστικών απαιτήσεων.

1.7.2 Ευφυΐα:

Οι ψηφιακές τεχνολογίες επιτρέπουν την ανάλυση μεγάλου όγκου δεδομένων και την αυτόματη εξαγωγή πληροφοριών. Η χρήση εφαρμογών παρακολούθησης και προσομοιώσεων διαχείρισης περιστατικών κρίσεων ενισχύει την ικανότητα αντίδρασης σε απρόβλεπτες καταστάσεις. Η χρήση της τεχνητής νοημοσύνης και της μηχανικής εκμάθησης επιτρέπει την ανίχνευση ύποπτων συμπεριφορών που μπορεί να οδηγήσουν σε κινδύνους.

1.7.3 Μετασχηματισμός:

Οι ψηφιακές τεχνολογίες επιτρέπουν την υιοθέτηση νέων προσεγγίσεων στη διαχείριση κινδύνων. Η χρήση τεχνολογιών blockchain στην εφοδιαστική αλυσίδα, για παράδειγμα,

ενισχύει τη διαφάνεια και την ασφάλεια. Οι προγνωστικές αναλύσεις συμπεριφορών στο διαδίκτυο βοηθούν στην προληπτική διαχείριση κινδύνων φήμης και ασφάλειας προϊόντων.

Η χρήση αυτών των τεχνολογιών απαιτεί προσεκτική αξιολόγηση και προετοιμασία, καθώς και διαρκή ενημέρωση και εκπαίδευση του προσωπικού. Παράλληλα, πρέπει να ληφθούν υπόψη η ηθική και οι νομικές πτυχές που σχετίζονται με τη χρήση των ψηφιακών τεχνολογιών στη διαχείριση κινδύνων.

1.8 Βέλτιστες Πρακτικές εφαρμογής Κυβερνοασφάλειας

Οι οργανισμοί στην εποχή της ψηφιακής μετάβασης αντιμετωπίζουν αυξανόμενες απειλές στον κυβερνοχώρο. Η ανάγκη για αποτελεσματική διαχείριση των κυβερνοκινδύνων και η επένδυση σε προηγμένες τεχνικές προστασίας είναι επιτακτικότερη από ποτέ. Οι πρακτικές που προτείνονται χωρίζονται σε τέσσερις βασικούς πυλώνες: Διακυβέρνηση, Προστασία, Επίγνωση και Ανθεκτικότητα.

1.8.1 1. Διακυβέρνηση

Ο πυλώνας της Διακυβέρνησης καλύπτει το διαχειριστικό και στρατηγικό μέρος της κυβερνοασφάλειας. Περιλαμβάνει την ανάπτυξη και την εφαρμογή πολιτικών που υποστηρίζουν τη στρατηγική του οργανισμού σε θέματα κυβερνοασφάλειας. Κεντρικό σημείο είναι η διαχείριση κινδύνων, όπου οι οργανισμοί πρέπει να αξιολογούν και να αναγνωρίζουν συστηματικά τις πιθανές απειλές και να αναπτύσσουν μηχανισμούς για την μείωση των επιπτώσεων τους. Επιπλέον, η διακυβέρνηση αφορά την υπεύθυνη ανατροφοδότηση και την ενσωμάτωση της κυβερνοασφάλειας στην κορυφαία διοίκηση των οργανισμών, καθιστώντας την έναν αναπόσπαστο τμήμα του οργανισμού.

Αυτό επιτυγχάνεται μέσω της ενσωμάτωσης μιας σειράς στρατηγικών και επιχειρηματικών πρακτικών που αναλύονται παρακάτω:

- Κατανόηση και Αντιμετώπιση Αναπτυσσόμενων Απειλών

Η ολιστική διαχείριση της κυβερνοασφάλειας αρχίζει με την ενσωμάτωση της κυβερνοασφάλειας στα αρχικά στάδια της επιχειρησιακής στρατηγικής του οργανισμού. Οι απειλές πρέπει να αναγνωρίζονται και να αξιολογούνται συστηματικά, με στόχο τη λήψη τεκμηριωμένων αποφάσεων. Αυτό επιτρέπει στους οργανισμούς να αναπτύξουν τις

απαραίτητες δυνατότητες για την ενίσχυση της επαγρύπνησης και της επίγνωσης σχετικά με τους κυβερνοκινδύνους.

- Σύνταξη Πλαισίου Διαχείρισης Κινδύνων

Η διαμόρφωση ενός σταθερού πλαισίου για την αναγνώριση, αξιολόγηση και παρακολούθηση των κινδύνων κυβερνοασφάλειας είναι κρίσιμη. Αυτό περιλαμβάνει την κατάρτιση σχεδίων αντιμετώπισης και την παρακολούθηση των κινδύνων, έχοντας υπόψη το προφίλ κινδύνου και το αποδεκτό επίπεδο αποδοχής κινδύνων. Η διαχείριση κινδύνων πρέπει να είναι εναρμονισμένη με την επιχειρηματική στρατηγική και να παρέχει τακτική πληροφόρηση στη διοίκηση για την υλοποίηση των απαραίτητων μέτρων ασφαλείας.

- Υλοποίηση Μοντέλου Λειτουργίας

Η σύνταξη ενός επιχειρησιακού μοντέλου για τη λειτουργία του προγράμματος κυβερνοασφάλειας είναι ζωτικής σημασίας. Περιλαμβάνει τη διαμόρφωση των οργανωτικών δομών, των ρόλων και των αρμοδιοτήτων, τόσο για τα εσωτερικά στελέχη όσο και για τους εξωτερικούς συνεργάτες. Η ευθυγράμμιση της στρατηγικής κυβερνοασφάλειας με την επιχειρησιακή στρατηγική εξασφαλίζει ότι οι απαιτούμενοι πόροι, διαδικασίες και τεχνολογίες είναι στη διάθεση του οργανισμού για την αντιμετώπιση των κυβερνοαπειλών.

- Σύνταξη του Πλαισίου και Υιοθέτηση Κουλτούρας Ασφάλειας

Το πλαίσιο κυβερνοασφάλειας πρέπει να περιλαμβάνει ολοκληρωμένες πολιτικές, διαδικασίες και πρότυπα, καθώς και να ενσωματώνεται στις καθημερινές λειτουργίες του οργανισμού. Η υιοθέτηση μιας κουλτούρας ασφάλειας και η εφαρμογή προγραμμάτων ευαισθητοποίησης είναι κρίσιμες για την ανάπτυξη του επιπέδου επαγρύπνησης και την κατανόηση της σημασίας της κυβερνοασφάλειας.

Μέσα από αυτές τις δράσεις, η διακυβέρνηση της κυβερνοασφάλειας γίνεται ένα ζωντανό μέρος της καθημερινής λειτουργίας του οργανισμού, διασφαλίζοντας ότι οι κυβερνοκίνδυνοι είναι επαρκώς αντιμετωπισμένοι και ότι η επιχείρηση είναι προετοιμασμένη για τις μελλοντικές απειλές.

1.8.2 2. Προστασία

Ο πυλώνας της Προστασίας επικεντρώνεται στην υλοποίηση φυσικών και ψηφιακών δικλείδων ασφαλείας για την προστασία του οργανισμού από κυβερνοεπιθέσεις. Αυτό περιλαμβάνει τεχνολογικά μέτρα όπως τείχη προστασίας, αντιιικό λογισμικό, κρυπτογράφηση δεδομένων και πιστοποίηση πολλαπλών παραγόντων (MFA). Παράλληλα, η σωστή συντήρηση και ενημέρωση των συστημάτων είναι ουσιώδης για την εξάλειψη των ευπαθειών και την ενίσχυση της συνολικής κυβερνοασφάλειας.

Τα κυριότερα στοιχεία που συνθέτουν αυτήν την προστασία είναι:

1.8.2.1 Υλοποίηση Ισχυρού Πλαισίου Κυβερνοασφάλειας

- Η δημιουργία ενός ολιστικού πλαισίου κυβερνοασφάλειας που ενσωματώνεται με την επιχειρησιακή στρατηγική είναι βασικός πυλώνας για τη θωράκιση των οργανισμών. Το πλαίσιο πρέπει να περιλαμβάνει:
- Στρατηγική και Επιχειρησιακό Μοντέλο: Ανάπτυξη και ενσωμάτωση των αρχών κυβερνοασφάλειας σε όλες τις λειτουργίες.
- Πολιτικές, Πρότυπα και Αρχιτεκτονική: Καθορισμός σαφών κανόνων και προτύπων που ορίζουν τις απαιτήσεις ασφάλειας.
- Κουλτούρα Κυβερνοασφάλειας: Προώθηση μιας κουλτούρας ευαισθητοποίησης και κατανόησης των κυβερνοκινδύνων.
- Διαχείριση Κινδύνων: Ενσωμάτωση διαδικασιών για την αναγνώριση, αξιολόγηση, και μετρίαση των κινδύνων. [12]

1.8.2.2 Προσδιορισμός και Διασφάλιση των Αγαθών Στρατηγικής Σημασίας

- Κρίσιμο βήμα για την προστασία είναι η ακριβής ταυτοποίηση των αγαθών που απαιτούν προστασία. Αυτά περιλαμβάνουν:
- Ανθρώπινο Δυναμικό: Ασφάλεια των πληροφοριών που διαχειρίζονται κρίσιμα στελέχη.
- Συστήματα και Διαδικασίες: Προστασία κρίσιμων συστημάτων και διασφάλιση της συνέχειας των λειτουργιών.
- Πληροφορίες: Εφαρμογή αυστηρών μέτρων ασφάλειας για τη διασφάλιση της εμπιστευτικότητας και ακεραιότητας των πληροφοριών.

1.8.2.3 Διαχείριση Δεδομένων και Αρχιτεκτονική Ασφάλειας

- Αρχιτεκτονική Ασφάλειας: Υιοθέτηση μοντέλων όπως η ασφάλεια εις βάθος και ζώνες ασφαλείας για την προστασία σε πολλαπλά επίπεδα.
- Κεντρικοποιημένη Διαχείριση Δεδομένων: Εφαρμογή συστημάτων διακυβέρνησης και e-Discovery για τη διαχείριση των πληροφοριών σε όλα τα στάδια του κύκλου ζωής τους.

1.8.2.4 Υλοποίηση Τεχνολογικών Μέτρων Ασφάλειας

- Η προστασία των υποδομών και των δεδομένων εξαρτάται από την εφαρμογή σύγχρονων τεχνολογικών μέτρων που ανταποκρίνονται στο προφίλ κινδύνου του οργανισμού. Τα μέτρα αυτά περιλαμβάνουν κρυπτογράφηση, πολιτικές πρόσβασης, ασφαλή δικτύωση και συστήματα ανίχνευσης εισβολών.

Η ενσωμάτωση αυτών των πολιτικών και μέτρων είναι κρίσιμη για τη διασφάλιση μιας στερεής υπεράσπισης ενάντια στις κυβερνοαπειλές, καθώς επίσης και για την προστασία της επιχειρηματικής λειτουργίας και της διαχείρισης τεχνολογίας σε όλα τα επίπεδα του οργανισμού.[12]

1.8.3 3. Επίγνωση

Ο τρίτος πυλώνας, η Επίγνωση, αναδεικνύει τη σημασία της γνώσης των απειλών και της κατάλληλης προετοιμασίας του προσωπικού. Οι οργανισμοί θα πρέπει να εφαρμόζουν συνεχείς εκπαιδευτικές προγράμματα για τους εργαζόμενους, ώστε να είναι ενημερωμένοι για τις νέες κυβερνοαπειλές και τις καλές πρακτικές. Επίσης, οι δράσεις ενημέρωσης πρέπει να καλύπτουν τον τρόπο αντιμετώπισης ύποπτων δραστηριοτήτων ή επιθέσεων, αυξάνοντας την γενική επιφυλακή και την ασφάλεια του οργανισμού. Η επίγνωση λοιπόν περιλαμβάνει την κατανόηση και αξιοποίηση πληροφοριών για την ορθή διαχείριση κυβερνοκινδύνων.

1.8.3.1 Προσδιορισμός Προφίλ Κινδύνου

- Η διαδικασία προσδιορισμού του προφίλ κινδύνου περιλαμβάνει την αναγνώριση και κατανόηση των κυβερνοαπειλών, καθώς και των μεθόδων και τεχνικών που χρησιμοποιούν οι επιτιθέμενοι. Αυτό επιτυγχάνεται μέσω:

- Συνεχούς Παρακολούθησης: Ενημερώσεις από CERTs, CSIRTs και ειδικευμένες πηγές κυβερνοευφυΐας.
- Αξιολόγηση Αλλαγών: Ανάλυση των επιπτώσεων από συγχωνεύσεις, εξαγορές και αλλαγές στα επιχειρησιακά μοντέλα που ενδέχεται να επηρεάσουν την ασφάλεια.

1.8.3.2 Έγκαιρη Διαχείριση Τεχνολογικών Ευπαθειών

- Κρίσιμος συντελεστής για την επίγνωση είναι η έγκαιρη εντόπιση και διαχείριση τεχνολογικών ευπαθειών:
- Χρήση CMDB: Αποτελεσματική καταγραφή και διαχείριση τεχνολογικών πόρων.
- Περιοδική Εκτίμηση Ευπαθειών: Συστηματικός έλεγχος και ενημέρωση για zero-day ευπαθειές.
- Αντισταθμιστικά Μέτρα: Εφαρμογή λύσεων για τη μείωση του κινδύνου εκμετάλλευσης ευπαθειών.

1.8.3.3 Διαμοίραση Πληροφοριών Κυβερνοευφυΐας

- Η κοινοποίηση πληροφοριών με αξιόπιστα κέντρα και άλλους οργανισμούς ενισχύει την ικανότητα του οργανισμού να αναγνωρίζει και να αντιδρά στις απειλές:
- Πλατφόρμες Κυβερνοευφυΐας: Χρήση εργαλείων όπως MISSP για την ανταλλαγή και την ανάλυση πληροφοριών σχετικά με κυβερνοαπειλές.
- Συνεργασία με CERTs/CSIRTs: Ενεργή συμμετοχή σε δίκτυα ανταπόκρισης για την ανταλλαγή πληροφοριών.

1.8.3.4 Προληπτικός Εντοπισμός Απειλών

- Η χρήση προηγμένων τεχνολογιών και τεχνικών για την πρόληψη και τον εντοπισμό απειλών πριν αυτές επηρεάσουν τον οργανισμό:
- Αναλυτικά Εργαλεία Δεδομένων: Χρήση AI, machine learning και data analytics για την ανάλυση και τη συσχέτιση δεδομένων που μπορεί να υποδεικνύουν επικείμενες επιθέσεις.
- Προσομοιώσεις Παραβίασης: Διεξαγωγή τακτικών penetration tests για την αξιολόγηση της ασφάλειας και την τεκμηρίωση των κινδύνων. [12]

Η συνεχής εκπαίδευση και ενημέρωση των εργαζομένων σχετικά με τις πρακτικές κυβερνοασφάλειας και τις τελευταίες τάσεις στον κυβερνοχώρο αποτελούν βασικό στοιχείο της ασφαλούς λειτουργίας. Με τη συνδυασμένη εφαρμογή όλων αυτών των στρατηγικών και τη διαρκή παρακολούθηση και προσαρμογή τους, ο οργανισμός αποκτά μια ολοκληρωμένη και αντιμετωπίσιμη προσέγγιση στην αντιμετώπιση κυβερνοαπειλών.

Επιπλέον, είναι σημαντικό να υπογραμμιστεί η ανάγκη συνεργασίας μεταξύ διαφορετικών τμημάτων του οργανισμού και άλλων εξωτερικών φορέων, όπως κρατικά ή διεθνής αρχές κυβερνοασφάλειας, για την ανταλλαγή πληροφοριών και τη συντονισμένη αντίδραση σε ενδεχόμενες απειλές. Μόνο μέσω της συνεργασίας και της συντονισμένης δράσης μπορεί να επιτευχθεί μια αποτελεσματική προστασία ενάντια στις διαρκώς εξελισσόμενες κυβερνοαπειλές.

1.8.4 4. Ανθεκτικότητα

Η ανθεκτικότητα ενός οργανισμού αποτελεί κρίσιμο παράγοντα για τη διατήρηση της λειτουργικότητάς του ακόμα και σε περιπτώσεις που η ασφάλειά του παραβιάζεται. Οι οργανισμοί θα πρέπει να υιοθετήσουν την αντίληψη ότι η ασφάλειά τους ενδέχεται να παραβιαστεί σε μεσοπρόθεσμο χρονικό ορίζοντα και να εφαρμόσουν σχέδια ανθεκτικότητας που θα τους επιτρέπουν να αντιμετωπίσουν αποτελεσματικά τις επιπτώσεις των περιστατικών ασφάλειας και να επαναφέρουν τις επιχειρησιακές τους λειτουργίες το συντομότερο δυνατόν.

Ένα αποτελεσματικό σχέδιο ανθεκτικότητας πρέπει να είναι σαφές, συνοπτικό και να περιλαμβάνει διάφορα στοιχεία. Συγκεκριμένα:

- Η διακυβέρνηση πρέπει να καθιερώσει διαλειτουργικό συντονισμό και διαχείριση τεκμηρίωσης και επικοινωνίας με τα εμπλεκόμενα μέρη.
- Η στρατηγική πρέπει να δημιουργήσει μια ισχυρή και ευθυγραμμισμένη στρατηγική για την αντιμετώπιση περιστατικών κυβερνοασφάλειας.
- Η τεχνολογία πρέπει να κατανοήσει τις τεχνικές παραμέτρους της διαχείρισης περιστατικών και της τεκμηρίωσης παραβιάσεων.
- Οι επιχειρησιακές λειτουργίες πρέπει να υλοποιηθούν με διασυνδεδεμένες διαδικασίες επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, με έμφαση στην αποτελεσματική επικοινωνία.
- Η διαχείριση κινδύνου και συμμόρφωση πρέπει να διαμορφώσει ένα σχέδιο ανθεκτικότητας που ενσωματώνει τις λειτουργίες της διαχείρισης κινδύνου και κανονιστικής συμμόρφωσης.

Μετά την εφαρμογή των σχεδίων, είναι σημαντικό να διεξάγονται συστηματικές δοκιμές σε ελεγχόμενο περιβάλλον ώστε να αξιολογείται συνεχώς η λειτουργικότητά τους. Οι δοκιμές μπορούν να περιλαμβάνουν την προσομοίωση περιστατικών ασφάλειας με εκτεταμένη διάρκεια και τη συμμετοχή όλων των εμπλεκόμενων μελών των ομάδων διαχείρισης κρίσεων. Επίσης, η εκτέλεση επίμονων δοκιμών παρείσδυσης μέσω της προσομοίωσης ρεαλιστικών κυβερνοεπιθέσεων από ανεξάρτητη εταιρία μπορεί να αξιολογήσει την απόκριση του οργανισμού σε αυτές τις απειλές.

Συνολικά, ο σχεδιασμός και η εφαρμογή μιας ενιαίας προσέγγισης για την αντιμετώπιση περιστατικών ασφάλειας βοηθούν στην ενίσχυση της ανθεκτικότητας και τη συμμόρφωση του οργανισμού με τις κανονιστικές απαιτήσεις, ενώ η προληπτική ανάλυση ενδείξεων παραβίασης συμβάλλει στην ανίχνευση και αντιμετώπιση πιθανών απειλών εγκαίρως.Συνολικά, οι τέσσερις πυλώνες αυτοί αποτελούν το θεμέλιο για μια ολιστική προσέγγιση στην κυβερνοασφάλεια, επιτρέποντας στους οργανισμούς να είναι προετοιμασμένοι για τις σημερινές αλλά και τις επερχόμενες απειλές στον κυβερνοχώρο. [12]

1.8.5 Σύνοψη

Η Κυβερνοασφάλεια αναδεικνύεται ως ο ακρογωνιαίος λίθος για τη διασφάλιση της ακεραιότητας και της ασφάλειας της κοινωνίας στην εποχή της ψηφιακής μετάβασης. Οι διαδικτυακές υποδομές και οι τεχνολογικές πλατφόρμες αποτελούν πλέον το θεμέλιο της λειτουργίας μας, και η απειλή από κυβερνοεγκληματίες είναι συνεχώς παρούσα.

Σε πρακτικό επίπεδο, η Κυβερνοασφάλεια επικεντρώνεται στην αποτελεσματική προστασία των ψηφιακών υποδομών και των δεδομένων από εισβολές, καθώς και στην άμυνα από κυβερνοεπιθέσεις και την αποκατάσταση μετά από ενδεχόμενες παραβιάσεις. Επιπλέον, εστιάζεται στη διασφάλιση της ιδιωτικότητας των πολιτών και στη δημιουργία εμπιστοσύνης προς τα ψηφιακά συστήματα και τις υπηρεσίες.

Σε ευρύτερο επίπεδο, η Κυβερνοασφάλεια παίζει ζωτικό ρόλο στην επιδίωξη της εθνικής και διεθνούς ασφάλειας, καθώς και στη διασφάλιση της δημόσιας υγείας και της οικονομικής σταθερότητας. Πέραν αυτού, η ενίσχυση των κυβερνοασφαλών συστημάτων συμβάλλει στην προώθηση της καινοτομίας και της ανταγωνιστικότητας τόσο σε εθνικό όσο και σε διεθνές επίπεδο.

Συνολικά, η Κυβερνοασφάλεια αποτελεί έναν κρίσιμο παράγοντα που απαιτεί στρατηγική προσέγγιση και συνεχή ενημέρωση, προκειμένου να αντιμετωπιστούν οι διαρκώς εξελισσόμενες

κυβερνοαπειλές. Μόνον με αυτόν τον τρόπο μπορούμε να διασφαλίσουμε μια ασφαλή, αξιόπιστη και ανθεκτική ψηφιακή κοινότητα και οικονομία.

2 Διακυβέρνηση Δεδομένων – Ορισμοί και Θεμελιώδη Θέματα

2.1 Ορισμός Διακυβέρνησης Δεδομένων -Data Governance

Η διακυβέρνηση δεδομένων αποτελεί, καταρχήν, μια λειτουργία διαχείρισης δεδομένων που διασφαλίζει την ποιότητα, την ακεραιότητα, την ασφάλεια και την επιθυμητή χρησιμότητα των δεδομένων που συλλέγονται από μια οργάνωση. Η διακυβέρνηση αυτών των δεδομένων πρέπει να εφαρμόζεται από τη στιγμή που συλλέγεται μια πληροφορία μέχρι και τη στιγμή που τα δεδομένα αυτά αφαιρούνται. Καθ' όλη τη διάρκεια αυτού του κύκλου ζωής, η διακυβέρνηση επικεντρώνεται στην επίτευξη της προσβασιμότητας και της χρησιμοποιησιμότητας των δεδομένων από όλα τα ενδιαφερόμενα μέρη, σύμφωνα πάντα με τα κανονιστικά πρότυπα. Αυτά τα πρότυπα είναι συχνά μια σύγκλιση των απαιτήσεων της βιομηχανίας, της κυβέρνησης και της εταιρικής ηθικής. Επιπλέον, η διακυβέρνηση δεδομένων πρέπει να διασφαλίζει την παροχή ενός ενοποιημένου και υψηλής ποιότητας ενός ολοκληρωμένου εικόνας όλων των δεδομένων εντός της επιχείρησης. Αυτό περιλαμβάνει την ακρίβεια, την ενημέρωση και τη συνέπεια των δεδομένων. Τέλος, η διακυβέρνηση δεδομένων πρέπει να εξασφαλίζει την ασφάλεια των δεδομένων, ώστε να διασφαλίζεται ότι προσπελάζονται μόνο από εξουσιοδοτημένους χρήστες, ότι είναι ελεγξιμα και ότι συμμορφώνονται με τους κανονισμούς. Η κύρια στόχος της διακυβέρνησης δεδομένων είναι να δημιουργήσει εμπιστοσύνη στην ποιότητα και την αξιοπιστία των δεδομένων. Τα αξιόπιστα δεδομένα είναι απαραίτητα για την υποστήριξη της διαδικασίας λήψης αποφάσεων, της ανάλυσης κινδύνων και της διαχείρισης χρησιμοποιώντας βασικούς δείκτες απόδοσης. Οι αρχές της διακυβέρνησης δεδομένων παραμένουν οι ίδιες, ανεξάρτητα από το μέγεθος της επιχείρησης ή την ποσότητα των δεδομένων, ενώ οι ειδικοί πρέπει να λαμβάνουν αποφάσεις σχετικά με τα εργαλεία και την υλοποίηση με βάση τις πρακτικές ανάγκες του περιβάλλοντος στο οποίο δραστηριοποιούνται. [2], [7]

2.2 Τι περιλαμβάνει η Διακυβέρνηση Δεδομένων

Η εμφάνιση της ανάλυσης μεγάλων δεδομένων, υποστηριζόμενη από την ευκολία μετάβασης στον νέφος και την συνεχή αύξηση της ικανότητας και της χωρητικότητας της υπολογιστικής ισχύος, έχει ενθαρρύνει και ενεργοποιήσει μία γρήγορα αναπτυσσόμενη κοινότητα καταναλωτών δεδομένων να συλλέγει, να αποθηκεύει και να αναλύει δεδομένα για προοπτικές και λήψη αποφάσεων. Σχεδόν κάθε εφαρμογή υπολογιστή σήμερα ενημερώνεται από επιχειρηματικά δεδομένα. Δεν είναι έκπληξη, συνεπώς, ότι νέες ιδέες αναπόφευκτα περιλαμβάνουν την ανάλυση υπαρχουσών δεδομένων με νέους τρόπους καθώς και τη συλλογή νέων συνόλων δεδομένων. Έχει οργάνωσή σας ένα μηχανισμό για τον έλεγχο νέων τεχνικών

ανάλυσης δεδομένων και για τη διασφάλιση ότι τα συλλεγόμενα δεδομένα αποθηκεύονται με ασφάλεια, ότι τα συλλεγόμενα δεδομένα είναι υψηλής ποιότητας και ότι οι προκύπτουσες δυνατότητες συμβάλλουν στην αξία του εμπορικού σας σήματος; Ενώ είναι πειραστικό να κοιτάξετε μόνο προς τη δύναμη και τις δυνατότητες της συλλογής δεδομένων και της ανάλυσης μεγάλων δεδομένων, η Διακυβέρνηση Δεδομένων είναι μία πολύ πραγματική, πολύ σημαντική σκέψη που δεν μπορεί να αγνοηθεί. Σε ένα πρόσφατο άρθρο του HBR, αναφέρθηκε ότι περισσότερο από το 70% των εργαζομένων έχουν πρόσβαση σε δεδομένα στα οποία δεν θα έπρεπε. Αυτό δεν σημαίνει ότι οι εταιρείες πρέπει να φοβούνται, μόνο να επισημαίνει τη σημασία της διακυβέρνησης και πώς μπορεί να οδηγήσει σε μετρήσιμα οφέλη για μία οργάνωση. [10]

Εικόνα 3: Data Governance

2.3 Ποιος είναι ο Σκοπός της Διακυβέρνησης Δεδομένων

Ο σκοπός της διακυβέρνησης δεδομένων είναι να παρέχει εμπιστοσύνη στα δεδομένα. Η διακυβέρνηση δεδομένων είναι πολύτιμη στο βαθμό που η παρουσία αυτής της διακυβέρνησης προσθέτει στην εμπιστοσύνη των ενδιαφερομένων στα δεδομένα που συλλέγονται, αναλύονται και δημοσιεύονται ή χρησιμοποιούνται για τη λήψη αποφάσεων. Η εξασφάλιση εμπιστοσύνης στα δεδομένα απαιτεί από τη στρατηγική διακυβέρνησης δεδομένων να αντιμετωπίσει τρεις βασικές πτυχές: την ανακαλύψιμοτητα, την ασφάλεια και την ευθύνη. Η ανακαλύψιμοτητα απαιτεί από τη διακυβέρνηση δεδομένων να καθιστά τεχνικά μεταδεδομένα, πληροφορίες καταγωγής και ένα επαγγελματικό γλωσσάρι εύκολα προσβάσιμα. Επιπλέον, τα επιχειρηματικά κρίσιμα δεδομένα πρέπει να είναι σωστά και πλήρη. Τέλος, η διαχείριση των κυρίων δεδομένων είναι απαραίτητη για να διασφαλιστεί ότι τα δεδομένα ταξινομούνται με ακρίβεια για να εξασφαλιστεί η κατάλληλη προστασία ενάντια σε αθέμιτες ή κακόβουλες αλλαγές ή διαρροές. Όσον αφορά την ασφάλεια, η νομική συμμόρφωση, η διαχείριση ευαίσθητων δεδομένων (προσωποποιημένες πληροφορίες, για παράδειγμα) και η πρόληψη της ασφάλειας και της διαρροής δεδομένων μπορεί να είναι όλα σημαντικά, ανάλογα με τον τομέα της επιχείρησης και το σύνολο δεδομένων που εξετάζεται. Αν η ανακαλύψιμοτητα και η ασφάλεια είναι σε εφαρμογή, τότε μπορείτε να αρχίσετε να αντιμετωπίζετε τα ίδια τα δεδομένα ως ένα προϊόν. Σε αυτό το σημείο, η ευθύνη γίνεται σημαντική και είναι απαραίτητο να παρέχετε ένα μοντέλο λειτουργίας για την ιδιοκτησία και την ευθύνη γύρω από τα όρια των τομέων δεδομένων. [8]

2.4 Βασικές Διαφορές Διακυβέρνησης Δεδομένων με την Ασφάλεια Δεδομένων

Η Διακυβέρνηση Δεδομένων συχνά συγχέεται με την Ασφάλεια Δεδομένων. Αυτά τα δύο θέματα διασταυρώνονται, αλλά έχουν διαφορετική έμφαση: Η διακυβέρνηση δεδομένων επικεντρώνεται κυρίως στο να καταστήσει τα δεδομένα προσβάσιμα, εύρισκα, και ευρετηριασμένα για αναζήτηση ανάμεσα στα σχετικά στοιχεία, συνήθως στο σύνολο του πληθυσμού γνώσης της οργάνωσης. Αυτός είναι ένας κρίσιμος τομέας της Διακυβέρνησης Δεδομένων, ο οποίος απαιτεί εργαλεία όπως ένα ευρετήριο μεταδεδομένων, ένα κατάλογο δεδομένων για την "αναζήτηση" δεδομένων. Η Διακυβέρνηση Δεδομένων επεκτείνει τη διευκόλυνση δεδομένων συμπεριλαμβάνοντας ένα ρεύμα εργασίας όπου μπορεί να λάβει χώρα η απόκτηση δεδομένων. Οι χρήστες μπορούν να αναζητήσουν δεδομένα, ανάλογα με το πλαίσιο και την περιγραφή, να βρουν τα σχετικά αποθετήρια δεδομένων και να ζητήσουν πρόσβαση, περιλαμβάνοντας την επιθυμητή χρήση ως δικαιολογία. Ένας εγκρίνων (διαχειριστής δεδομένων) θα πρέπει να εξετάσει το αίτημα, να καθορίσει εάν είναι δικαιολογημένο και εάν τα

δεδομένα που ζητούνται μπορούν πράγματι να εξυπηρετήσουν την επιχειρηματική περίπτωση, και να εκκινήσει ένα διαδικασία όπου τα δεδομένα μπορούν να γίνουν προσβάσιμα.

Η διευκόλυνση δεδομένων προχωρά πέρα από το να καθιστά τα δεδομένα προσβάσιμα και ανακαλύψιμα και μπαίνει στην εργαλειοθήκη που επιτρέπει τη γρήγορη ανάλυση και επεξεργασία των δεδομένων για να προκύψουν συμπεράσματα που σχετίζονται με την επιχείρηση: "πόσο ξοδεύει η επιχείρηση σε αυτό το θέμα", ή "μπορούμε να βελτιστοποιήσουμε αυτήν την αλυσίδα εφοδιασμού", και ούτω καθεξής. Το θέμα είναι κρίσιμο και απαιτεί γνώση για το πώς να εργαστεί κανείς με δεδομένα, καθώς και τι σημαίνουν πραγματικά τα δεδομένα - καλύτερα αντιμετωπιζόμενο με τη συμπερίληψη, από την αρχή, μεταδεδομένων που περιγράφουν τα δεδομένα και περιλαμβάνουν πρόταση αξίας, καταγωγή, καταγωγή, και ένα άτομο επικοινωνίας που επιμελείται και ανήκει στα δεδομένα που εξετάζονται, για να επιτρέψει περαιτέρω ερευνητική έρευνα. [1], [5]

Η Ασφάλεια Δεδομένων, η οποία και πάλι σχετίζεται σε μεγάλο βαθμό και διασταυρώνεται τόσο με τη διευκόλυνση όσο και με τη διακυβέρνηση των δεδομένων, σκεφτείτε κανονικά ως ένα σύνολο μηχανισμών που τίθενται σε εφαρμογή για να αποτρέψουν και να μπλοκάρουν την μη εξουσιοδοτημένη πρόσβαση. Η Διακυβέρνηση Δεδομένων βασίζεται σε μηχανισμούς ασφάλειας δεδομένων που τίθενται σε εφαρμογή, αλλά υπερβαίνει την απλή πρόληψη της μη εξουσιοδοτημένης πρόσβασης και προχωρά σε πολιτικές σχετικά με τα ίδια τα δεδομένα, τη μετασχηματιστική τους διαδικασία σύμφωνα με την κλάση των δεδομένων και τη δυνατότητα απόδειξης ότι οι πολιτικές που έχουν οριστεί για την πρόσβαση και τη μετασχηματιστική τους διαδικασία με τον χρόνο συμμορφώνονται. Η σωστή εφαρμογή των μηχανισμών ασφαλείας προάγει την εμπιστοσύνη που απαιτείται για να μοιραστούν δεδομένα ευρέως ή να "δημοκρατούνται η πρόσβαση" στα δεδομένα. [2]

Συνοπτικά, οι παραπάνω διαφορές παρουσιάζεται στον πίνακα στη συνέχεια:

Χαρακτηριστικά	**Διακυβέρνηση Δεδομένων**	**Ασφάλεια Δεδομένων**
Έμφαση	Στη διαχείριση και προσβασιμότητα των δεδομένων	Στην πρόληψη μη εξουσιοδοτημένης πρόσβασης και στην αποτροπή παραβιάσεων
Εργαλεία	Ευρετήριο μεταδεδομένων, κατάλογος δεδομένων	Μηχανισμοί πρόληψης και αποκλεισμού παραβιάσεων.

Επεξεργασία Δεδομένων	Προωθεί την ανάλυση και επεξεργασία για εύρεση συμπερασμάτων	Καθιστά την πρόσβαση σε δεδομένα ελεγχόμενη και ασφαλή.
Πολιτικές	Σχετικά με τη διαχείριση και τη μετασχηματιστική διαδικασία των δεδομένων	Σχετικά με την πρόσβαση και χρήση των δεδομένων
Εμπιστοσύνη	Μέσω σωστής διαχείρισης και προσβασιμότητας δεδομένων.	Μέσω αποτροπής παραβιάσεων και προστασίας των δεδομένων.

2.5 Διαδικασία εφαρμογής πλάνου Διακυβέρνησης Δεδομένων

2.5.1 Καθορισμός Στόχων

Ο καθορισμός στόχων ενός προγράμματος στο πλαίσιο του Data Governance αποτελεί βασικό παράγοντα, καθώς καθορίζει την κατεύθυνση και την επιτυχία του. Τα οφέλη της σαφούς καθορισμένων στόχων απεικονίζονται σε διάφορα επίπεδα του προγράμματος και αποτελούν κρίσιμο στοιχείο για την επιτυχή υλοποίησή του. [3]

Οι στόχοι ενός προγράμματος αποτελούν το κεντρικό μέσο επικοινωνίας με την ανώτερη ηγεσία και εξασφαλίζουν την υποστήριξή της. Επίσης, καθορίζουν τις δραστηριότητες και τις αποφάσεις των συμμετεχόντων, καθορίζοντας τους ρόλους και τις ευθύνες τους. Τέλος, καθορίζουν τις μετρικές που χρησιμοποιούνται για την αξιολόγηση της επίτευξης των αποτελεσμάτων του προγράμματος.

Η αποτυχία πολλών προγραμμάτων Διακυβέρνησης Δεδομένων οφείλεται συχνά στην έλλειψη σαφώς καθορισμένων στόχων. Σε τέτοιες περιπτώσεις, είναι σημαντικό να επανεξετάσουμε και να καθορίσουμε με σαφήνεια τους στόχους του προγράμματος. Επίσης, είναι σημαντικό να μετατρέψουμε τις φιλοδοξίες σε συγκεκριμένους στόχους προγράμματος, με αναφορά στην εμπειρία που αποκτήθηκε από παρόμοιες περιπτώσεις στο παρελθόν.

Συμπερασματικά, ο καθορισμός σαφών στόχων αποτελεί βασικό στοιχείο για την επιτυχή υλοποίηση ενός προγράμματος. Μέσω της σαφούς καθορισμένων στόχων, οργανώσεις μπορούν να δημιουργήσουν μια κουλτούρα που στηρίζεται στα δεδομένα και στην ευθύνη,

επιτυγχάνοντας την αποτελεσματική διαχείριση των προκλήσεων στον τομέα της διακυβέρνησης των δεδομένων. [2]

2.5.2 Ορισμός Κατευθυντήριων Αρχών

Οι κατευθυντήριες αρχές αντιπροσωπεύουν δηλώσεις που καθοδηγούν τη συμπεριφορά και τις αποφάσεις ενός οργανισμού στο πλαίσιο του προγράμματος Data Governance. Αποτελούν το σύνολο κοινών φιλοσοφιών και αξιών που διέπουν τη λειτουργία τους, ανεξάρτητα από τις καθημερινές αλλαγές και προκλήσεις. Στόχος τους είναι να λειτουργήσουν ως κύριος οδηγός κατά τη διάρκεια της εφαρμογής της Διακυβέρνησης Δεδομένων, αποτελώντας ένα είδος φιλοσοφικού αναφορικού σημείου για ενδεχόμενες ερωτήσεις ή διλήμματα που προκύπτουν.

Αντίθετα με τους προγραμματικούς στόχους, οι κατευθυντήριες αρχές δεν μπορούν να μετρηθούν, αλλά θεσμοθετούν κυριολεκτικά τα όρια για ένα πρόγραμμα. Αποτελούν δηλώσεις σχετικά με το "πώς" μπορεί να εκτελεστεί το πρόγραμμα, παρέχοντας καθοδήγηση και πλαίσιο δράσης.

Για να είναι αποτελεσματικές, οι κατευθυντήριες αρχές πρέπει να αντικατοπτρίζουν τον πολιτισμό, τα ιδανικά και τις αξίες του οργανισμού. Πρέπει να είναι συμβατές με το όραμα, την αποστολή και τις βασικές αρχές του οργανισμού. Έτσι, η διαδικασία καθορισμού των κατευθυντήριων αρχών απαιτεί μια διαφορετική προσέγγιση από τον καθορισμό των προγραμματικών στόχων.

Μια καλή συλλογή κατευθυντήριων αρχών μπορεί επίσης να ανακουφίσει την ανησυχία των ενδιαφερομένων φορέων του προγράμματος, ακόμα και αν δεν εμπλέκονται άμεσα στις καθημερινές λειτουργίες του προγράμματος. [2]

Εικόνα 4: Σύνοψη Κατευθυντήριων Αρχών

2.6 Κύκλος Ωρίμανσης Διακυβέρνησης Δεδομένων

Τα βιώσιμα προγράμματα διακυβέρνησης δεδομένων θεωρούνται ως συνεχιζόμενες προσπάθειες και όχι ως περιορισμένα έργα. Για την επίτευξη των βέλτιστων αποτελεσμάτων, τα αποτελεσματικά προγράμματα αξιολογούν ενδελεχώς τις οργανωτικές διαδικασίες που υποστηρίζουν τη διαχείριση δεδομένων και εντοπίζουν τα επιθυμητά αποτελέσματα. Τα προγράμματα αυτά ενσωματώνονται άνετα στις καθημερινές λειτουργίες και γίνονται αναπόσπαστο μέρος του οργανωτικού πολιτισμού.

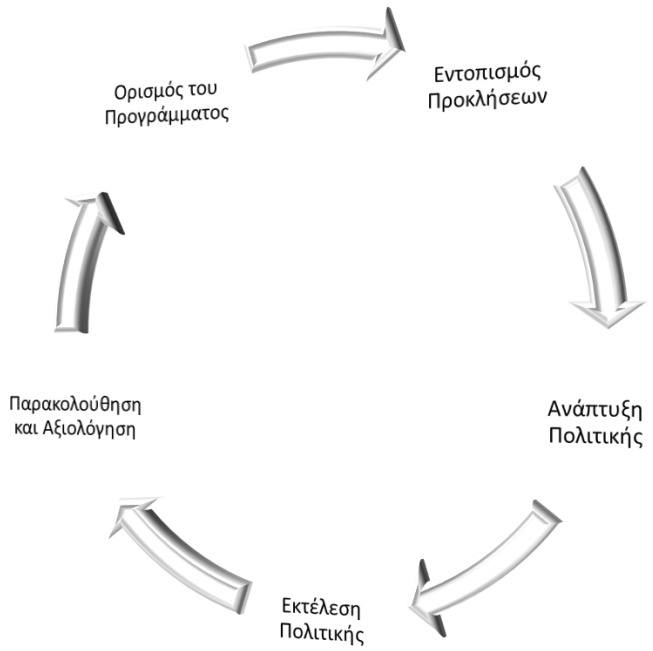
Οι οργανισμοί διανύουν μια σειρά από διακριτές φάσεις καθώς ξεκινούν και προχωρούν στις προσπάθειες Διακυβέρνησης Δεδομένων τους. Αυτό το ταξίδι είναι αέναο, αντανακλώντας έναν επαναλαμβανόμενο κύκλο που προσαρμόζεται στις εξελισσόμενες επιχειρηματικές ανάγκες. Παρόλο που η αρχική αφορμή για την υιοθέτηση της Διακυβέρνησης Δεδομένων μπορεί να διαφέρει μεταξύ των οργανισμών, οι θεμελιώδεις αρχές επιτυχίας παραμένουν συνεπείς. [3], [4]

Ο Κύκλος Ωριμότητας Διακυβέρνησης Δεδομένων περιλαμβάνει πέντε ουσιαστικά στάδια, κρίσιμα τόσο για την εγκατάσταση όσο και, κυρίως, για τη διατήρηση μιας πρωτοβουλίας Διακυβέρνησης Δεδομένων. Η πρόοδος μέσω αυτών των σταδίων ξεκινά γραμμικά αλλά σύντομα υιοθετεί ένα κυκλικό μοτίβο για να αντιμετωπίσει συνεχώς τις μεταβαλλόμενες οργανωτικές ανάγκες και λύσεις. Αυτός ο κύκλος διευκολύνει όχι μόνο την συνεχή προσαρμογή αλλά και τη φυσική εξέλιξη και ανάπτυξη. Τα πέντε κλειδιά στάδια του Κύκλου Ωριμότητας Διακυβέρνησης Δεδομένων περιγράφονται ως εξής:

1. Ορισμός του Προγράμματος
2. Εντοπισμός Προκλήσεων
3. Ανάπτυξη Πολιτικής
4. Εκτέλεση Πολιτικής
5. Παρακολούθηση και Αξιολόγηση

Κάθε στάδιο αποτελεί ουσιαστικό συστατικό του κύκλου, τονίζοντας τη σημασία μιας διατηρητικής και προσαρμοστικής προσέγγισης στη Διακυβέρνηση Δεδομένων μέσα σε έναν οργανισμό. [2]

Στην παρακάτω εικόνα αποτυπώνονται συνοπτικά τα παραπάνω στάδια:



Εικόνα 5: Κύκλος ωριμότητας διακυβέρνησης δεδομένων

2.6.1 Στάδιο 1 – Ορισμός του Προγράμματος

Τα επιτυχημένα προγράμματα Διακυβέρνησης Δεδομένων έχουν ένα κοινό στοιχείο — οι υπεύθυνοι του προγράμματος έχουν αφιερώσει χρόνο για να ορίσουν τα εξής:

Αρχική Εστίαση

Όπως σε κάθε πρόβλημα, το πρώτο βήμα για την επίλυσή του είναι ο ορισμός του τι ακριβώς είναι αυτό το "κάτι" και η σχεδίαση μιας προσέγγισης για την επίλυσή του. Αφιερώστε χρόνο για να σκεφτείτε τι χρειάζεστε για να αρχίσετε να λύνετε βραχυπρόθεσμα. Η εστίαση μπορεί πάντα να αλλάξει· στην πραγματικότητα, αυτό είναι ένδειξη ωριμότητας.

Στόχοι του Προγράμματος και Καθοδηγητικές Αρχές

Μέχρι τώρα, έχετε αποκτήσει μια αρκετά καλή κατανόηση ότι ο ορισμός στόχων αποτελεί ένα σημαντικό θεμέλιο για κάθε πρόγραμμα Διακυβέρνησης Δεδομένων. Εάν έχετε εκπληρώσει όλες τις άλλες συστάσεις και ακόμη δεν έχετε ορίσει στόχους για το πρόγραμμα, κάντε ένα βήμα πίσω και καταγράψτε τους. Χρειάζεστε αυτούς τους στόχους για να αντιμετωπίσετε τις προκλήσεις σας με μια πειθαρχημένη και μεθοδική προσέγγιση. Θα σας βοηθήσουν επίσης όταν χρειαστεί να επικοινωνήσετε δραστηριότητες και μετρήσεις του προγράμματος. [6]

Λήψη Αποφάσεων

Για την εξασφάλιση ότι οι συμμετέχοντες στο πρόγραμμα βρίσκονται στο κατάλληλο ιεραρχικό επίπεδο εντός της οργάνωσης για τη λήψη αποφάσεων, απαιτείται λεπτομερής κατανόηση των αιτημάτων κάθε ομάδας. Είναι σημαντικό να ξεκινά κανείς από τους στόχους του προγράμματος, ορίζοντας στη συνέχεια τις δραστηριότητες και/ή τις αποφάσεις που απαιτούνται. Ακολούθως, προβαίνει σε ανάθεση των ρόλων "υπεύθυνος," "υπόλογος," "συμβουλευόμενος," ή "ενημερωμένος" (πίνακας RACI). Οι αναθέσεις του ρόλου του "υπόλογου" απαιτούν ρόλους με το κατάλληλο επίπεδο εξουσίας. Απαραίτητο είναι η επανεξέταση των Ρόλων και των Ευθυνών για την κατασκευή του πίνακα RACI και τελικά την ονοματοδοσία των συμμετεχόντων. [6]

Χάρτη Πορείας

Αφού έχουν καθοριστεί το πεδίο εφαρμογής, οι στόχοι, οι καθοδηγητικές αρχές, το οργανωτικό πλαίσιο και οι ρόλοι και οι ευθύνες, το επόμενο βήμα είναι ο καθορισμός του σχεδίου λειτουργίας του προγράμματος. Αυτό περιλαμβάνει τη δημιουργία ενός χάρτη πορείας, ο οποίος δεν θα βοηθήσει μόνο στην εκτέλεση του προγράμματος, αλλά θα λειτουργήσει και ως εργαλείο επικοινωνίας και μέτρησης.

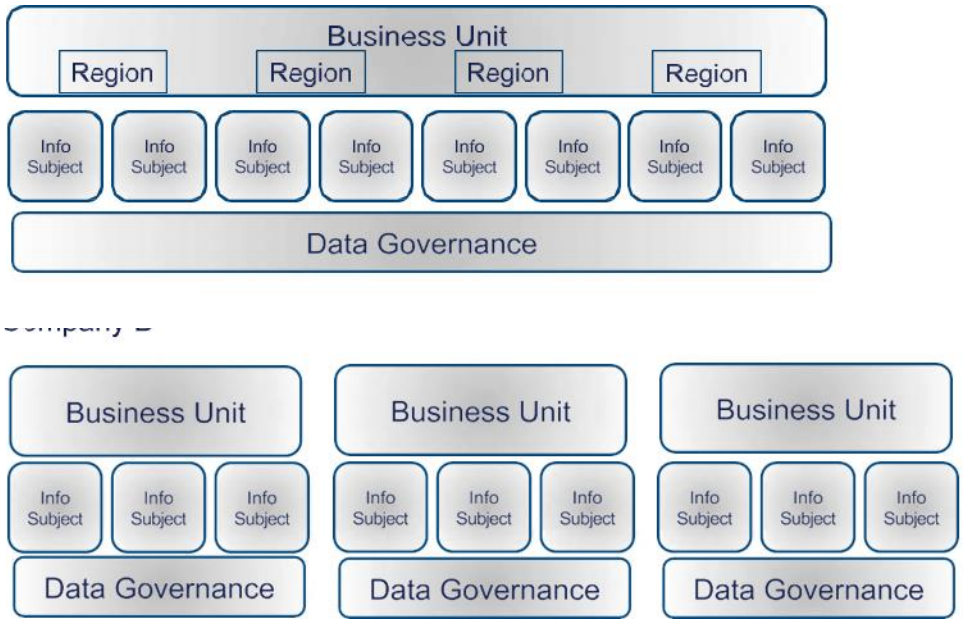
2.6.2 Στάδιο 2 – Προκλήσεις

Στο δεύτερο στάδιο όταν ένας οργανισμός βρίσκεται στα αρχικά στάδια της εφαρμογής της Διακυβέρνησης Δεδομένων, το στάδιο αυτό αποτελεί βήμα επικύρωσης με τους συμμετέχοντες

που έχουν ενταχθεί στο πρόγραμμα, όπως οι Κύριοι Κάτοχοι Δεδομένων. Η επικύρωση αυτή συμβαίνει κατά τον ορισμό του προγράμματος. Ανάλογα με το πεδίο εφαρμογής της Διακυβέρνησης Δεδομένων, ο Κύριος Κάτοχος Δεδομένων μπορεί να αποφασίσει ποιες προκλήσεις χρειάζεται να αντιμετωπιστούν εντός του πλαισίου του δικού του τομέα, δηλαδή θέματα που ενδεχομένως να μην επηρεάζουν ολόκληρη την επιχείρηση.

Με την επανάληψη του κύκλου, είναι σημαντικό να επαναξιολογηθούν ποιοι νέοι τομείς εστίασης πρέπει να προσδιοριστούν μέσω των προκλήσεων και των καθορισμένων προτεραιοτήτων. Αιτήματα, ερωτήσεις, νέα έργα και ζητήματα θα εμφανίζονται πάντα. Η συνέπεια στις προτεραιότητες πρέπει να διατηρηθεί. [2]

Ακόμα, σημαντική πρόκληση αποτελεί και η επιλογή του είδους εφαρμογής του μοντέλου που θα ακολουθηθεί, όπως αποτυπώνεται στην παρακάτω εικόνα:



Εικόνα 6: Διαφορές επιλογής Framework

2.6.3 Στάδιο 3 – Δημιουργία Policies

Η ανάγκη για δημιουργία συγκεκριμένων πολιτικών διαχείρισης δεδομένων είναι κρίσιμη για την επιτυχία οποιουδήποτε προγράμματος διακυβέρνησης δεδομένων. Πολιτικές αυτού του

είδους καθορίζουν μια συγκεκριμένη προσέγγιση για τη διαχείριση των δεδομένων και στοχεύουν σε συγκεκριμένα αποτελέσματα. Οι πολιτικές αυτές πρέπει να αναπτυχθούν με τέτοιο τρόπο ώστε να λύνουν προκλήσεις που αφορούν τους ορισμούς, την ποιότητα των δεδομένων, τα κυρίαρχα δεδομένα, την ασφάλεια των δεδομένων, την μοντελοποίηση, την ονοματοδοσία, ή την ενσωμάτωση δεδομένων.

Τα οφέλη από την καθιέρωση συνεκτικών και ευρύτερα αποδεκτών πολιτικών είναι πολυδιάστατα. Καταρχάς, διασφαλίζουν ότι όλοι οι συμμετέχοντες — από τους διαχειριστές δεδομένων έως τους τελικούς χρήστες — κατανοούν τις προσδοκίες και τις απαιτήσεις που συνοδεύουν τη διαχείριση των δεδομένων. Επίσης, η ενιαία προσέγγιση στην τεκμηρίωση και στη δομή των πολιτικών διασφαλίζει ότι δεν υπάρχει σύγχυση ή ανακολουθία στο πώς εφαρμόζονται οι διάφορες διατάξεις στα διαφορετικά δεδομένα ή διαμερίσματα.

Επιπλέον, η στρατηγική εστίαση της πολιτικής μπορεί να είναι είτε ευρεία, ώστε να αφορά θέματα σε επίπεδο επιχείρησης, είτε πιο ειδική, ώστε να αντιμετωπίζει συγκεκριμένες ανάγκες σε επίπεδο τμήματος. Αυτό επιτρέπει την ευελιξία και την προσαρμοστικότητα στις εκάστοτε επιχειρησιακές ανάγκες, όπως επίσης και την άμεση ανταπόκριση σε αλλαγές ή νέες προκλήσεις που μπορεί να προκύψουν.

Οι διαδικασίες ανάπτυξης, επικύρωσης και εφαρμογής των πολιτικών πρέπει να είναι σαφώς ορισμένες και να περιλαμβάνουν τη συμμετοχή όλων των σχετικών μερών, όπως οι διαχειριστές δεδομένων και οι ειδικοί των διαδικασιών επιχείρησης. Τέλος, η δημιουργία μιας πολιτικής δεν πρέπει να αντιμετωπίζεται ως αυτοσκοπός, αλλά ως ένα μέσο για την επίτευξη μετρήσιμων και συγκεκριμένων αποτελεσμάτων που ενισχύουν τη συνολική στρατηγική και τις λειτουργικές αποδόσεις της επιχείρησης.

2.6.4 Στάδιο 4 - Εφαρμογή της Πολιτικής

Στο στάδιο της εφαρμογής της πολιτικής, η ομάδα διαχείρισης δεδομένων, οι συνεργάτες ΤΠ και οι εμπλεκόμενοι τομείς της επιχείρησης αναλαμβάνουν να υλοποιήσουν λύσεις που διευκολύνουν τη συμμόρφωση με τις καθορισμένες πολιτικές και διαδικασίες. Η επίτευξη της συμμόρφωσης μπορεί να περιλαμβάνει πληθώρα αλλαγών, από την αναδιάρθρωση οργανωτικών δομών και την τροποποίηση επιχειρησιακών διαδικασιών μέχρι την εφαρμογή νέων τεχνολογιών ή ακόμη και την εισαγωγή εφαρμογών που συμβάλλουν στη διαχείριση των αλλαγών.

Παρά τη φαινομενικά συνοπτική περιγραφή της διαδικασίας, η προσπάθεια που απαιτείται για να κινηθεί η οργάνωση προς τη συμμόρφωση δεν πρέπει να υποτιμηθεί. Εκτός από τις πολιτικές που απλώς αντικατοπτρίζουν και επισημοποιούν τις ήδη υπάρχουσες λειτουργίες, οποιαδήποτε άλλη προσπάθεια συμμόρφωσης θα απαιτήσει μια διαδικασία διαχείρισης αλλαγών για τη συνεχή εφαρμογή τους. Οι εμπλεκόμενοι στη διακυβέρνηση δεδομένων, οι χορηγοί και οι υποστηρικτές της πρέπει επίσης να έχουν υπόψη τους ότι, ανάλογα με το εύρος των απαιτούμενων αλλαγών, η συμμόρφωση δεν θα επιτευχθεί από τη μία μέρα στην άλλη. Ένας επιπλέον παράγοντας είναι ο ανταγωνισμός με άλλα έργα και πρωτοβουλίες εντός της οργάνωσης. Το πρόγραμμα διακυβέρνησης δεδομένων ίσως χρειαστεί να δικαιολογήσει τις ανάγκες του όπως και οι άλλοι τομείς ή προγράμματα που διεκδικούν περιορισμένους πόρους. Γι' αυτό είναι τόσο σημαντική η ευθυγράμμιση με τους γενικότερους επιχειρησιακούς στόχους. Το κλειδί είναι η προγραμματισμένη αλλαγή, καθώς και η συνεχής παρακολούθηση και επικοινωνία της προόδου.

2.6.5 Στάδιο 5 - Παρακολούθηση Δεδομένων και Αναφορά

Η παρακολούθηση και η αναφορά είναι κρίσιμα στοιχεία στο πέμπτο στάδιο του κύκλου διαχείρισης δεδομένων, όπου η επίτευξη της συμμόρφωσης με τις πολιτικές και τα αποτελέσματα αυτών εξετάζονται εναντίον των επιδιωκόμενων στόχων. Η συνεχής παρακολούθηση διασφαλίζει ότι τα προγράμματα δεν μένουν απλά στο χαρτί αλλά φέρνουν τροποποιήσεις και βελτιώσεις στην πρακτική εφαρμογή των διαδικασιών.

- Παρακολούθηση σε Επίπεδο Πολιτικής

  Κάθε πολιτική οφείλει να καθορίζει σαφώς τι σημαίνει η συμμόρφωση και πώς αυτή πρέπει να παρακολουθείται. Οι δείκτες και οι μεθοδολογίες για την αξιολόγηση της συμμόρφωσης πρέπει να είναι ακριβείς και αντικειμενικοί, ενώ η παρακολούθηση αυτή πρέπει να ενσωματώνεται σε μηνιαία ή τριμηνιαία διαστήματα αναφορών, ανάλογα με την κρισιμότητα της πολιτικής.

- Παρακολούθηση σε Επίπεδο Προγράμματος

  Η μέτρηση της απόδοσης των προγραμμάτων έναντι των δηλωθέντων στόχων παρέχει μια ευκρινή εικόνα της αποτελεσματικότητας των εν λόγω πρωτοβουλιών. Η δημιουργία ενός "πίνακα αποτελεσμάτων" του προγράμματος, ο οποίος ανανεώνεται και αναφέρεται στην ηγεσία κατά κύριο λόγο σε τριμηνιαία βάση, βοηθά στη διαφάνεια και στην τακτική ενημέρωση των στόχων και των επιδόσεων.

- Επικοινωνία Αποτελεσμάτων

Η συχνή και έγκυρη επικοινωνία των εξελίξεων και των επιδόσεων είναι ουσιαστική. Η δημιουργία ενός ολοκληρωμένου σχεδίου επικοινωνίας που καθορίζει τα μέσα, τους στόχους και την περιοδικότητα της επικοινωνίας αποτελεί βασικό στοιχείο για την επιτυχία της διαχείρισης δεδομένων. Η τήρηση του σχεδίου επικοινωνίας και η διατήρηση της συνέπειας στις αναφορές ενισχύουν την εμπιστοσύνη των εμπλεκομένων και διασφαλίζουν τη συνεχή υποστήριξη των διαδικασιών διακυβέρνησης δεδομένων

2.7 Πολιτικές Διακυβέρνησης Δεδομένων

Κατά την ανάπτυξη μιας πολιτικής Διακυβέρνησης Δεδομένων, υπάρχουν πολλαπλές συνιστώσες που πρέπει να ληφθούν υπόψη προκειμένου να διασφαλιστεί ότι η πολιτική είναι αποτελεσματική, περιεκτική και εκτελεστή. Αυτές οι συνιστώσες παρουσιάζονται δομημένα σε αυτό που θα μπορούσε να αναφέρεται ως το πλαίσιο Διακυβέρνησης Δεδομένων. Κάθε τμήμα αυτού του πλαισίου έχει έναν μοναδικό ρόλο στη διαχείριση και χρήση των δεδομένων εντός μιας οργάνωσης.

Δήλωση Πολιτικής: Αποτελείται από μια επίσημη σειρά δηλώσεων που περιγράφουν τον τρόπο χρήσης και διαχείρισης των πόρων δεδομένων. Η σαφήνεια αυτών των δηλώσεων είναι κρίσιμη—πρέπει να είναι συνοπτικές και καθαρές ώστε όλοι οι ενδιαφερόμενοι, από τη διοίκηση μέχρι το επιχειρησιακό προσωπικό, να μπορούν εύκολα να κατανοήσουν τις προσδοκίες και τις απαιτήσεις. Οι πολιτικές πρέπει να δηλώνουν όχι μόνο τι πρέπει να γίνει αλλά και να τονίζουν τη σημασία αυτών των κανόνων, βοηθώντας έτσι τους ενδιαφερόμενους να καταλάβουν το λόγο πίσω από αυτούς. Οι στόχοι που περιγράφονται στη δήλωση της πολιτικής πρέπει να είναι συντονισμένοι με τους ευρύτερους στόχους του προγράμματος Διακυβέρνησης Δεδομένων της οργάνωσης. [2]

Διαδικασίες: Περιγράφουν λεπτομερώς πώς θα υλοποιηθεί η πολιτική. Οι διαδικασίες λειτουργούν ως βήμα-προς-βήμα οδηγοί για την εκτέλεση των πολιτικών και εξασφαλίζουν ότι υπάρχει μια τυποποιημένη προσέγγιση στη διαχείριση δεδομένων σε όλη την οργάνωση. Οι αποτελεσματικές διαδικασίες μειώνουν την ασάφεια και παρέχουν έναν σαφή οδικό χάρτη για την χειραφέτηση των δεδομένων, κρίσιμο για τη διατήρηση της συνέπειας και της αξιοπιστίας στις διαδικασίες δεδομένων.

Πρότυπα: Αυτά είναι οι καθορισμένες οδηγίες ή οι απαιτούμενες ρυθμίσεις που ορίζουν τα ελάχιστα αποδεκτά πρότυπα για τις πρακτικές διαχείρισης δεδομένων εντός της οργάνωσης. Τα

πρότυπα είναι κρίσιμα για τη διατήρηση της ποιότητας και της συνέπειας στη χειραφέτηση δεδομένων. Συχνά βασίζονται σε βέλτιστες πρακτικές του κλάδου και σε ρυθμιστικές απαιτήσεις, εξασφαλίζοντας ότι οι πρακτικές διακυβέρνησης δεδομένων της οργάνωσης συναντούν εξωτερικά και εσωτερικά κριτήρια για την ποιότητα και την ασφάλεια των δεδομένων.

Βέλτιστες Πρακτικές: Η αναγνώριση και η εφαρμογή βέλτιστων πρακτικών αφορά την αναγνώριση και τη χρήση μεθόδων, διαδικασιών ή δραστηριοτήτων που έχουν αποδειχθεί πιο αποτελεσματικές στην επίτευξη συγκεκριμένων αποτελεσμάτων διαχείρισης δεδομένων. Οι βέλτιστες πρακτικές προέρχονται από πραγματικές εφαρμογές και επικυρώνονται μέσω της επιτυχίας τους στην παράδοση καλύτερων αποτελεσμάτων σε σύγκριση με άλλες μεθόδους. Εξελίσσονται με την πάροδο του χρόνου καθώς εμφανίζονται νέες τεχνολογίες και μεθοδολογίες.

Διαδικασίες: Διαχείρισης Δεδομένων: Αφορά την τακτική εκτέλεση και επιβολή των πολιτικών και των προτύπων διακυβέρνησης δεδομένων. Είναι η εφαρμογή στην πράξη των αρχών και των κανόνων που έχουν καθοριστεί από τις πολιτικές μέσω των καθημερινών δραστηριοτήτων διαχείρισης δεδομένων. Οι αποτελεσματικές διαδικασίες διαχείρισης δεδομένων διασφαλίζουν ότι τα δεδομένα χειρίζονται με τρόπο που υποστηρίζει τους στρατηγικούς στόχους της οργάνωσης, τη συμμόρφωση με τους κανονισμούς και τις επιχειρησιακές ανάγκες.

Συνοψίζοντας, κατά τη διαμόρφωση μιας πολιτικής Διακυβέρνησης Δεδομένων, είναι ουσιαστικό να ενσωματωθούν αρμονικά αυτές οι συνιστώσες για να δημιουργηθεί ένα ακέραιο πλαίσιο. Αυτό το πλαίσιο όχι μόνο καθοδηγεί την οργάνωση στην κατάλληλη διαχείριση δεδομένων αλλά υποστηρίζει και τους στρατηγικούς στόχους, διασφαλίζοντας ότι τα δεδομένα λειτουργούν ως κύριος ενισχυτής των επιχειρησιακών στόχων.
Οι διαδικασίες αποτελούν λεπτομερείς οδηγίες σχετικά με τον τρόπο εφαρμογής μιας πολιτικής. Μπορεί να υπάρχει μία ή περισσότερες διαδικασίες που συνθέτουν ένα εγχειρίδιο λειτουργίας για μια συγκεκριμένη πολιτική. Οι διαδικασίες αυτές, όπως και οι λειτουργικές διαδικασίες, έχουν συχνά καθοριστεί εν μέρει κατά τη διαδικασία ορισμού των δραστηριοτήτων και αποφάσεων σχετικά με τη Διακυβέρνηση Δεδομένων, καθώς και κατά την ανάθεση ρόλων και ευθυνών.

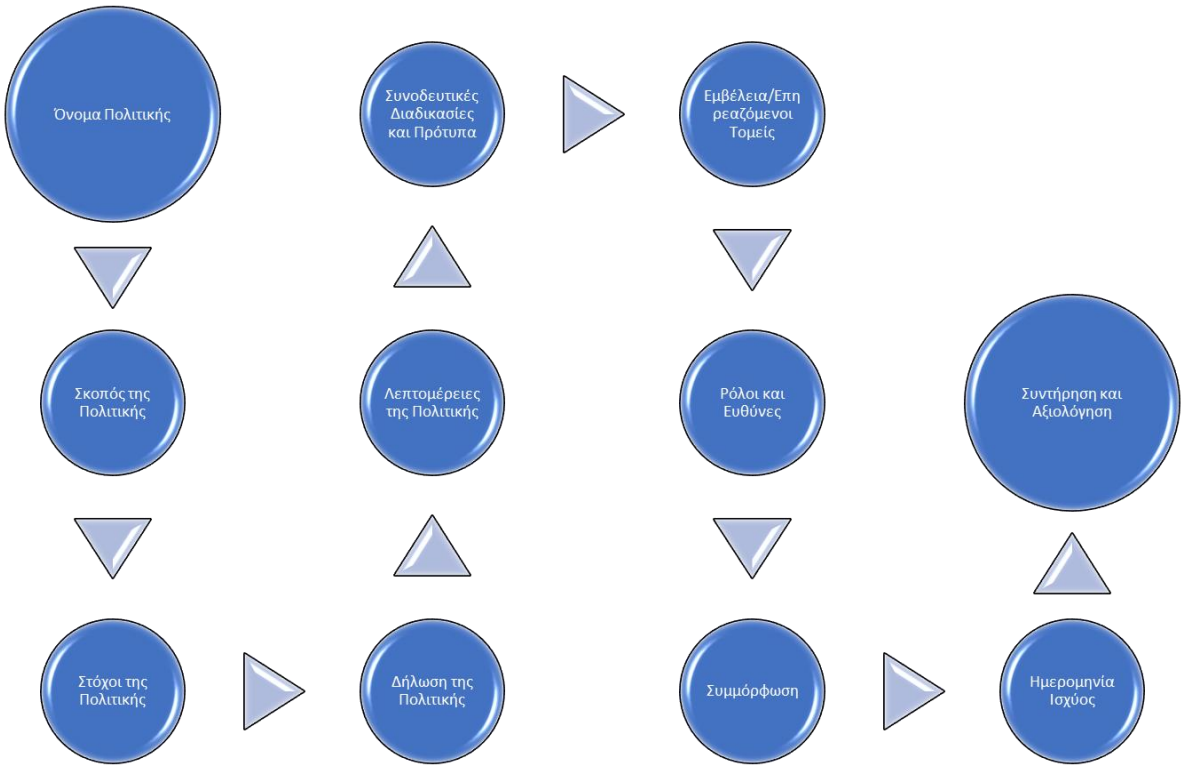
2.7.1 Τι πρέπει να περιλαμβάνεται σε μια Πολιτική

Η ανάπτυξη μιας πολιτικής απαιτεί τη διαμόρφωση ενός σαφούς πλαισίου που ορίζει το σκοπό, τους στόχους και τις λεπτομέρειες της εν λόγω πολιτικής. Ακολουθεί ένας κατάλογος με τα κύρια

στοιχεία που πρέπει να περιέχει μια πολιτική, είτε χρησιμοποιώντας ένα υπάρχον πρότυπο της οργάνωσης είτε αυτή τη λίστα ως αφετηρία.

2.7.2 Περιεχόμενα της Πολιτικής

- Όνομα: Το επίσημο όνομα της πολιτικής, το οποίο πρέπει να απεικονίζει σαφώς τον σκοπό της.
- Σκοπός της Πολιτικής: Μια σύντομη δήλωση που εξηγεί γιατί η πολιτική έχει αναπτυχθεί και τι επιδιώκει να επιτύχει.
- Στόχοι της Πολιτικής: Ειδικοί στόχοι που η πολιτική προσπαθεί να επιτύχει, απαριθμημένοι για σαφήνεια.
- Δήλωση της Πολιτικής: Η βασική αρχή ή οι κατευθύνσεις που καθορίζουν την πολιτική, προσδιορίζοντας τις δράσεις ή τις απαγορεύσεις που σχετίζονται με αυτή.
- Λεπτομέρειες της Πολιτικής: Επεκτείνει και εξηγεί τα σημεία που καλύπτονται στη δήλωση της πολιτικής, παρέχοντας περισσότερες λεπτομέρειες για την εφαρμογή.
- Συνοδευτικές Διαδικασίες και Πρότυπα: Οδηγίες και πρότυπα που πρέπει να ακολουθούνται για την εφαρμογή της πολιτικής.
- Εμβέλεια/Επηρεαζόμενοι Τομείς: Οι τομείς ή οι μονάδες της οργάνωσης στους οποίους εφαρμόζεται η πολιτική.
- Ρόλοι και Ευθύνες: Καθορισμός των ρόλων και των ατόμων ή τμημάτων που φέρουν ευθύνη για την εφαρμογή και συμμόρφωση με την πολιτική.
- Συμμόρφωση: Οι απαιτήσεις για την τήρηση και επαλήθευση της συμμόρφωσης με την πολιτική.
- Ημερομηνία Ισχύος: Η ημερομηνία από την οποία η πολιτική θα τεθεί σε ισχύ.
- Συντήρηση και Αξιολόγηση: Οι διαδικασίες για την τακτική αναθεώρηση και ενημέρωση της πολιτικής για να διασφαλιστεί η επικαιρότητα και η αποτελεσματικότητά της.



Εικόνα 7: Πολιτική

Η προσεκτική διαμόρφωση αυτών των στοιχείων εξασφαλίζει ότι η πολιτική είναι ολοκληρωμένη, κατανοητή και παρέχει σαφείς οδηγίες για την εφαρμογή της στην οργάνωση. [2]

Συμπέρασμα

Οι πολιτικές στη Διακυβέρνηση Δεδομένων αποτελούν την καρδιά του συστήματος διαχείρισης και προσφέρουν τα απαραίτητα εργαλεία για τη διασφάλιση της ακεραιότητας, της διαφάνειας και της αποτελεσματικότητας στο χειρισμό δεδομένων. Μέσω της διαρκούς επικαιροποίησης και βελτίωσης των πολιτικών, οι οργανισμοί μπορούν να ανταποκρίνονται στις εξελίξεις και να αξιοποιούν τις προκλήσεις ως ευκαιρίες για βελτίωση. Αυτή η διαδικασία ενισχύει την αξιοπιστία και τη σταθερότητα στη Διακυβέρνηση Δεδομένων, εξασφαλίζοντας μια ισχυρή βάση για το μέλλον της οργάνωσης στον ψηφιακό κόσμο.

3 Πολιτικές και Κανονισμοί στη Διακυβέρνηση Δεδομένων και Κυβερνοασφάλεια

3.1 Εισαγωγή

Στο παρόν κεφάλαιο αναλύεται η εξέλιξη των νομοθετικών και ρυθμιστικών πλαισίων που διέπουν την κυβερνοασφάλεια, με έμφαση στις πρόσφατες διατάξεις των ΗΠΑ, τις αντίστοιχες νομοθεσίες της Ευρωπαϊκής Ένωσης, και τη διεθνή απήχηση αυτών των προτύπων. Επικεντρώνεται στην ανάγκη για αυξημένη προστασία δεδομένων στην εποχή της ψηφιακής πληροφορίας και παρουσιάζει τις πολιτικές που στοχεύουν στην ενίσχυση της διαφάνειας και της ασφάλειας στον κυβερνοχώρο. Αναφέρονται επίσης τα πλαίσια που έχουν εφαρμοστεί σε διεθνές επίπεδο, εστιάζοντας στην επίδραση των κανονισμών στις πολυεθνικές συνεργασίες και στη διαχείριση κινδύνων. Η εισαγωγή αυτών των νεών προσεγγίσεων στην πρακτική εφαρμογή αποτελεί κρίσιμο στοιχείο για την κατανόηση των σύγχρονων προκλήσεων στην κυβερνοασφάλεια και τις απαντήσεις που αναπτύσσονται για την αντιμετώπισή τους. Με την παγκόσμια διάδοση της ψηφιακής τεχνολογίας και την αυξημένη εξάρτηση από τα ψηφιακά δεδομένα, οι κυβερνητικές και ιδιωτικές οργανώσεις βρίσκονται αντιμέτωπες με συνεχώς αυξανόμενες απειλές που επιτάσσουν ενισχυμένες και συνεκτικές κυβερνοασφαλιστικές πολιτικές.

Η Ευρωπαϊκή Ένωση, ανταποκρινόμενη στις προκλήσεις αυτές, έχει εισαγάγει σημαντικές διατάξεις μέσω του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), ο οποίος επικεντρώνεται στην ενίσχυση των δικαιωμάτων των υποκειμένων δεδομένων και στην επιβολή αυστηρότερων προτύπων για την επεξεργασία και την ασφάλεια των προσωπικών δεδομένων. Αυτές οι πολιτικές δεν επηρεάζουν μόνο τις εταιρείες εντός της Ε.Ε. αλλά και εκείνες που διακινούν δεδομένα μεταξύ της Ε.Ε. και άλλων περιοχών, διαμορφώνοντας μια παγκόσμια απήχηση.

Το κεφάλαιο συνεχίζει με την παρουσίαση των αναλυτικών εξελίξεων και των κρίσιμων ζητημάτων που περιλαμβάνουν οι διάφορες νομοθετικές και ρυθμιστικές προσεγγίσεις, αναδεικνύοντας παράλληλα τις διασυνδέσεις μεταξύ των διαφορετικών νομοθετικών πλαισίων και την ανάγκη για μια ενοποιημένη προσέγγιση που θα αντιμετωπίζει την κυβερνοασφάλεια ως μια κοινή πρόκληση σε παγκόσμιο επίπεδο. Τέλος, τονίζει τη σημασία της συνεχούς προσαρμογής και ενημέρωσης των πολιτικών ασφαλείας για να παραμείνουν επίκαιρες με τις τεχνολογικές εξελίξεις και τις εξελισσόμενες απειλές στον κυβερνοχώρο.

3.2 Κανονιστικό Πλαίσιο Κυβερνοασφάλειας στην Ευρωπαική Ένωση

3.2.1 Υπηρεσίες Ψηφιακής Διαμεσολάβησης (Digital Services Act)

Το DSA, ή η Οδηγία για τις Υπηρεσίες Ψηφιακής Διαμεσολάβησης (Digital Services Act), αποτελεί μια κεντρική νομοθετική πρωτοβουλία της Ευρωπαϊκής Ένωσης, σχεδιασμένη για να ρυθμίσει τον τρόπο λειτουργίας των πλατφορμών στο διαδίκτυο, εξασφαλίζοντας υψηλότερα επίπεδα διαφάνειας και ασφάλειας για τους χρήστες. Το DSA εφαρμόζεται σε μια ευρεία γκάμα διαμεσολαβητών στο διαδίκτυο, όπως οι πάροχοι υπηρεσιών διαδικτύου, οι πάροχοι υπηρεσιών cloud, πάροχοι υπηρεσιών μηνυμάτων, ψηφιακές αγορές και κοινωνικά δίκτυα. [13]

Μερικές από τις κυριότερες πτυχές του DSA περιλαμβάνουν:

1. **Ειδικές υποχρεώσεις**: Οι υπηρεσίες πλατφορμών όπως τα κοινωνικά δίκτυα και οι διαδικτυακές αγορές έχουν ειδικές υποχρεώσεις περί επιμέλειας, όπως η αναγνώριση και η απομάκρυνση παράνομου περιεχομένου.

2. **Προστασία χρηστών**: Οι κανόνες του DSA αποσκοπούν στην προστασία των χρηστών από παραπλανητικές διεπαφές και τη χρήση πληροφοριών που επηρεάζουν τις ελεύθερες αποφάσεις τους. Περιλαμβάνει επίσης απαιτήσεις για αυξημένη διαφάνεια στην διαδικτυακή διαφήμιση.

3. **Κατηγοριοποίηση των πλατφορμών**: Οι πλατφόρμες με πάνω από 45 εκατομμύρια ενεργούς χρήστες αναγνωρίζονται ως VLOPs (Very Large Online Platforms) και VLOSEs (Very Large Online Search Engines), οι οποίες υπόκεινται σε αυστηρότερους κανόνες.

4. **Εποπτεία και κυρώσεις**: Οι κανονιστικές αρχές σε κάθε κράτος μέλος, μαζί με την Ευρωπαϊκή Επιτροπή, επιβλέπουν τη συμμόρφωση των πλατφορμών με το DSA, με δυνατότητα επιβολής προστίμων σε περιπτώσεις μη συμμόρφωσης.

Το DSA τέθηκε σε ισχύ το Νοέμβριο του 2022, και η πλειονότητα των διατάξεών του άρχισαν να ισχύουν από τον Φεβρουάριο του 2024, καθορίζοντας ένα νέο πλαίσιο ασφάλειας και διαφάνειας για τις ψηφιακές υπηρεσίες στην ΕΕ.

Αναλυτικότερα, το DSA εφαρμόζεται σε μια ευρεία γκάμα διαμεσολαβητών στο διαδίκτυο (παρόχους υπηρεσιών πληροφοριακής κοινωνίας), συμπεριλαμβανομένων των παρόχων υπηρεσιών διαδικτύου, των παρόχων υπηρεσιών cloud, των παρόχων υπηρεσιών μηνυμάτων, των ψηφιακών αγορών και των κοινωνικών δικτύων. Ειδικές υποχρεώσεις επιμέλειας ισχύουν για τις υπηρεσίες πλατφορμών και ειδικότερα για τις διαδικτυακές πλατφόρμες, όπως τα

κοινωνικά δίκτυα, τις πλατφόρμες κοινής χρήσης περιεχομένου, τα καταστήματα εφαρμογών, τις διαδικτυακές αγορές και τις διαδικτυακές πλατφόρμες ταξιδιών και φιλοξενίας. Οι διαδικτυακές πλατφόρμες και οι διαδικτυακές μηχανές αναζήτησης με τουλάχιστον 45 εκατομμύρια ενεργούς χρήστες το μήνα στην ΕΕ (αντιπροσωπεύοντας το 10% του πληθυσμού της ΕΕ) κατηγοριοποιούνται αντίστοιχα ως VLOPs και VLOSEs. Οι πρώτοι VLOPs και VLOSEs ονοματίστηκαν στις 25 Απριλίου 2023, με την Επιτροπή να διακρίνει 17 VLOPs και 2 VLOSEs που επί του παρόντος πληρούν το σχετικό μηνιαίο κατώφλι χρηστών. Οι πιο εκτεταμένοι κανόνες στο DSA ισχύουν για τους VLOSEs και τους VLOPs. Αυτοί περιλαμβάνουν: απαιτήσεις για την αναγνώριση και απομάκρυνση παράνομου περιεχομένου, περιορισμούς στη χρήση παραπλανητικών διεπαφών χρήστη που εμποδίζουν τους χρήστες από το να λαμβάνουν ελεύθερες και ενημερωμένες αποφάσεις (για παράδειγμα, μέσω της χρήσης "σκοτεινών προτύπων" και τακτικών "ώθησης" που χειραγωγούν τις επιλογές των χρηστών), απαιτήσεις για την αύξηση της διαφάνειας της διαδικτυακής διαφήμισης (συμπεριλαμβανομένης της παροχής περισσότερων πληροφοριών στους χρήστες και της δυνατότητας εξαίρεσης από συστήματα αξιολόγησης βασισμένα σε προφίλ), αυξημένη προστασία για παιδιά που χρησιμοποιούν αυτές τις διαδικτυακές υπηρεσίες (συμπεριλαμβανομένης απαγόρευσης στη στοχευμένη διαφήμιση βάσει προφίλ), και απαιτήσεις για τη διεξαγωγή ετήσιων αξιολογήσεων κινδύνου και αναφορά αυτών στην Επιτροπή. Οι κράτη μέλη της ΕΕ απαιτείται να ορίσουν αρμόδιες (εθνικές) αρχές για την εποπτεία των παρόχων υπηρεσιών διαμεσολάβησης και να ενισχύσουν το DSA. Ωστόσο, η Ευρωπαϊκή Επιτροπή (Επιτροπή) είναι ο κύριος ρυθμιστής για τους VLOPs και τους VLOSEs. Οι ρυθμιστές που ορίζονται βάσει του DSA διαθέτουν εκτεταμένες ερευνητικές και επιβαλλόμενες εξουσίες, με την Επιτροπή να έχει το δικαίωμα να επιβάλλει πρόστιμα έως και 6% του ετήσιου παγκόσμιου τζίρου του παρόχου για το προηγούμενο οικονομικό έτος για μη συμμόρφωση με το DSA. Το DSA τέθηκε σε ισχύ στις 16 Νοεμβρίου 2022. Η πλειονότητα των διατάξεών του ισχύει για τους παρόχους υπηρεσιών από τις 17 Φεβρουαρίου 2024. Ωστόσο, όλες οι διαδικτυακές πλατφόρμες, εκτός από τις μικροσκοπικές και μικρές (που καθορίζονται από τον αριθμό των εργαζομένων και τον τζίρο), απαιτήθηκε να δημοσιεύσουν πληροφορίες σχετικά με τους μέσους ενεργούς αποδέκτες των υπηρεσιών τους έως τις 17 Φεβρουαρίου 2023. Αυτό έγινε για να επιτρέψει στην Επιτροπή να καθορίσει ποιοι πάροχοι υπηρεσιών θα έπρεπε να ονοματιστούν ως VLOPs και VLOSEs. Οι VLOPs και οι VLOSEs πρέπει να συμμορφωθούν με τις υποχρεώσεις τους βάσει του DSA εντός τεσσάρων μηνών από την ονομασία τους, δηλαδή έως τις 25 Αυγούστου 2023 για το πρώτο σύνολο ονομαζόμενων VLOPs και VLOSEs.

3.3 Κανονιστικό Πλαίσιο Κυβερνοασφάλειας στις ΗΠΑ

Η Αμερικανική Βουλή έχει υποβάλει προτάσεις νομοθεσίας που επεκτείνουν τις αρχές της κυβερνοασφάλειας. Ο Νόμος για την Ασφάλεια Δεδομένων Καταναλωτών και Ειδοποίηση τροποποιεί τον Νόμο Gramm-Leach-Bliley ώστε να απαιτεί την αποκάλυψη παραβιάσεων ασφάλειας από χρηματοοικονομικά ιδρύματα. Οι βουλευτές έχουν επίσης σχεδιάσει την "επέκταση του Gramm-Leach-Bliley σε όλους τους κλάδους που αφορούν οικονομικές πληροφορίες καταναλωτών, συμπεριλαμβανομένων οποιωνδήποτε εταιρειών που δέχονται πληρωμές με πιστωτική κάρτα." Η Βουλή έχει συζητήσει κανονισμούς κυβερνοασφάλειας παρόμοιους με τον Νόμο της Καλιφόρνια για την Ειδοποίηση Παραβίασης Ασφάλειας για εταιρείες που διατηρούν προσωπικά δεδομένα. Ο Νόμος για την Προστασία Πληροφοριών και Ασφάλεια απαιτεί από τους μεσίτες δεδομένων να "διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, να ελέγχουν και να παρακολουθούν τους χρήστες, να αποκαλύπτουν και να προλαμβάνουν παράνομες δραστηριότητες, και να μειώνουν τις πιθανές βλάβες στα άτομα."

Οι θεωρίες συμβάσεων μπορεί να καλύπτουν αξιώσεις για παραβίαση σύμβασης όταν υπάρχει μια ρητή συμφωνία μεταξύ του ενάγοντα και του εναγομένου που περιλαμβάνει μια ρητή υπόσχεση ειλικρινούς προστασίας πληροφοριών για τη διατήρηση των προσωπικών δεδομένων. Ακόμη και αν μια τέτοια ρήτρα δεν περιλαμβάνεται στη σύμβαση, πολλοί ενάγοντες θα δικαιολογήσουν μια αξίωση υπονοούμενης σύμβασης, υποστηρίζοντας ότι η μεταχείριση των προσωπικών δεδομένων ενός ενάγοντα υπονοεί μια δέσμευση για επαρκή προστασία αυτών των πληροφοριών. Οι θεωρίες αδικοπραγίας μπορεί να περιλαμβάνουν αμέλεια ή άλλες θεωρίες κοινού δικαίου όπως παραβίαση της ιδιωτικότητας, υπεκφυγή, παραβίαση ακινήτου, παραπλανητικές παραστάσεις ή άδικο εμπλουτισμό. Κάθε μία από αυτές τις θεωρίες μπορεί να αποδειχθεί πρόκληση για την προσαρμογή τους στο πλαίσιο της παραβίασης δεδομένων.

Ο Νόμος Πληροφορικής του 2008 εφαρμόζεται σε κάθε άτομο, εταιρεία ή οργανισμό (μεσάζοντες) που χρησιμοποιεί πόρους υπολογιστών, δίκτυα υπολογιστών ή άλλες τεχνολογίες επικοινωνίας στην Ινδία. Περιλαμβάνει επίσης παρόχους υπηρεσιών διαδικτύου, δικτύου και τηλεπικοινωνιών. Περιλαμβάνει επίσης ξένες οργανώσεις που έχουν παρουσία στην Ινδία και επιχειρήσεις εκτός της χώρας που έχουν λειτουργίες στην Ινδία.

Εκτός από τις γενικές απαιτήσεις λογικής προστασίας, κάποιοι νόμοι ή κανονισμοί κρατιδίων των ΗΠΑ είναι πιο συγκεκριμένοι. Για παράδειγμα, ο Κανονισμός Κυβερνοασφάλειας του Τμήματος Οικονομικών Υπηρεσιών της Νέας Υόρκης περιλαμβάνει συγκεκριμένες απαιτήσεις όπως ετήσιες δοκιμές αντοχής για καλυμμένες οντότητες. Ο αναθεωρημένος Κανόνας Προστασίας της FTC που ισχύει για ορισμένα χρηματοοικονομικά ιδρύματα καθορίζει συγκεκριμένα μέτρα για την

προστασία πληροφοριών καταναλωτών, συμπεριλαμβανομένου της κρυπτογράφησης και πολλαπλών παραγόντων ελέγχου πρόσβασης (ή ισοδύναμου δικαιολογημένου από έναν ορισμένο άτομο υπεύθυνο για την επιτήρηση του προγράμματος ασφάλειας του ιδρύματος).

4 Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Ο Κανονισμός (ΕΕ) 2016/679, γνωστός ως Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), είναι ένας νομοθετικός κανονισμός της Ευρωπαϊκής Ένωσης που στοχεύει στην προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των ατόμων στην ΕΕ και στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ). Ο κύριος σκοπός του GDPR είναι να ενδυναμώσει τους πολίτες σχετικά με τη διαχείριση των προσωπικών τους δεδομένων και να εναρμονίσει το ρυθμιστικό πλαίσιο για διεθνείς επιχειρήσεις εντός της ΕΕ.

Ο κανονισμός αντικαταστά την οδηγία 95/46/ΕΚ για την προστασία δεδομένων και καθορίζει τις απαιτήσεις για την επεξεργασία των προσωπικών δεδομένων εντός της Ευρωπαϊκής Ένωσης. Ισχύει για όλες τις επιχειρήσεις που ενεργούν στον Ευρωπαϊκό Οικονομικό Χώρο, ανεξαρτήτως της τοποθεσίας τους. Η επεξεργασία προσωπικών δεδομένων επιτρέπεται μόνο εφόσον βασίζεται σε νόμιμο λόγο ή με ρητή συγκατάθεση του ατόμου στο οποίο ανήκουν τα δεδομένα.

Οι υπεύθυνοι για την επεξεργασία δεδομένων πρέπει να κοινοποιούν σαφώς κάθε συλλογή δεδομένων, να επικαλούνται τη νομιμότητα της επεξεργασίας, τους σκοπούς και τη διάρκεια διατήρησης των δεδομένων. Επιπλέον, τα άτομα των οποίων επεξεργάζονται τα δεδομένα έχουν το δικαίωμα να λάβουν αντίγραφο των δεδομένων τους και να ζητήσουν τη διαγραφή τους υπό προϋποθέσεις.

4.1 Ποιος εφαρμόζει τον Γενικό Κανονισμό Προστασίας Δεδομένων

Οι υπεύθυνοι και οι επεξεργαστές των προσωπικών δεδομένων οφείλουν να λαμβάνουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εφαρμογή των αρχών προστασίας δεδομένων. Οι διαδικασίες επεξεργασίας προσωπικών δεδομένων πρέπει να είναι σχεδιασμένες και εκτελεσμένες με γνώμονα αυτές τις αρχές και να περιλαμβάνουν μηχανισμούς προστασίας, όπως ανωνυμοποίηση ή ψευδωνυμοποίηση των δεδομένων, όταν αυτό απαιτείται. Επιπρόσθετα, οι υπεύθυνοι επεξεργασίας πρέπει να εγγυώνται ότι οι επεξεργασίες δεδομένων γίνονται μόνο βάσει μίας από τις έξι νόμιμες βάσεις που ορίζει ο κανονισμός: συγκατάθεση, σύμβαση, δημόσιο έργο, ζωτικό συμφέρον, νόμιμο συμφέρον, ή νομική απαίτηση. Σε περίπτωση συγκατάθεσης, το άτομο έχει το δικαίωμα να την ανακαλέσει οποτεδήποτε.

Οι επιχειρήσεις πρέπει να αναφέρουν σαφώς τη συλλογή δεδομένων, τη νομική βάση και τον σκοπό της επεξεργασίας, τη διάρκεια διατήρησης των δεδομένων και εάν αυτά μοιράζονται με τρίτους ή μεταφέρονται εκτός ΕΟΧ. Πρέπει να εφαρμόζουν πολιτικές που διασφαλίζουν την

προστασία των δεδομένων με ελάχιστη επέμβαση στο απόρρητο των ατόμων. Επιπλέον, πρέπει να υπάρχουν εσωτερικοί ελέγχοι και κανονισμοί για την επιτήρηση των διαδικασιών.

Οι δημόσιες αρχές και οι επιχειρήσεις με βασικές δραστηριότητες στην επεξεργασία προσωπικών δεδομένων θα πρέπει να προσλαμβάνουν έναν υπεύθυνο προστασίας δεδομένων, που θα είναι υπεύθυνος για την τήρηση του GDPR. Οι παραβιάσεις δεδομένων πρέπει να αναφέρονται στις εθνικές αρχές εποπτείας εντός 72 ωρών αν έχουν αρνητικές συνέπειες στο απόρρητο των ατόμων. Σοβαρές παραβάσεις μπορεί να επιφέρουν σημαντικά πρόστιμα, ενδεχομένως μέχρι και 20 εκατομμύρια ευρώ ή 4% του παγκόσμιου κύκλου εργασιών της προηγούμενης χρήσης.

4.2 Εξαιρέσεις

Ορισμένες περιπτώσεις δεν αντιμετωπίζονται ειδικά στο GDPR, και επομένως αντιμετωπίζονται ως εξαιρέσεις. Αυτές είναι οι εξής:

- Προσωπικές ή οικιακές δραστηριότητες
- Επιβολή του νόμου
- Εθνική ασφάλεια

Όταν δημιουργήθηκε ο GDPR, δημιουργήθηκε αυστηρά για τη ρύθμιση των προσωπικών δεδομένων που πηγαίνει στα χέρια των εταιρειών. Αυτό που δεν καλύπτεται από τον GDPR είναι οι μη εμπορικές πληροφορίες ή οι οικιακές δραστηριότητες. Ένα παράδειγμα αυτών των οικιακών δραστηριοτήτων μπορεί να είναι μηνύματα ηλεκτρονικού ταχυδρομείου μεταξύ δύο φίλων γυμνασίου.

Επιπλέον, ο GDPR δεν ισχύει όταν τα δεδομένα συνδέονται ενδεχομένως με αστυνομική έρευνα. Παρόλο που δεν καλύπτεται από τον GDPR, ο νόμος για την προστασία δεδομένων του 2018, το Μέρος 3 καλύπτει ρητά αυτούς τους λόγους.

Τέλος, όταν τα δεδομένα αφορούν την εθνική ασφάλεια, είναι εκτός των ορίων του GPDR, οπότε καλύπτεται από τον Νόμο για την Προστασία Δεδομένων του 2018, Μέρος 2 Κεφάλαιο 3.

Αντίθετα, μια οντότητα ή πιο συγκεκριμένα μια «επιχείρηση» πρέπει να συμμετέχει σε «οικονομική δραστηριότητα» για να καλύπτεται από τον GPDR. Η οικονομική δραστηριότητα ορίζεται ευρέως στο δίκαιο ανταγωνισμού της Ευρωπαϊκής Ένωσης (Lawspot/GDPR: Ενσωματώθηκε στη Συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο, 2018).

4.3 Εφαρμογή εκτός της Ευρωπαϊκης Ένωσης

Ο GDPR επεκτείνεται και σε υπεύθυνους επεξεργασίας και επεξεργαστές δεδομένων που βρίσκονται εκτός Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ), αν αυτοί δραστηριοποιούνται στην προσφορά αγαθών ή υπηρεσιών (είτε απαιτείται πληρωμή είτε όχι) προς άτομα που βρίσκονται εντός του ΕΟΧ ή παρακολουθούν τη συμπεριφορά τους εντός της ΕΕ (άρθρο 3, παράγραφος 2). Ο κανονισμός ισχύει ανεξαρτήτως του τόπου που γίνεται η επεξεργασία των δεδομένων, προσδίδοντας έτσι εξωεδαφική δικαιοδοσία στο GDPR για οντότητες εκτός ΕΕ που αλληλεπιδρούν με κατοίκους της ΕΕ.

Εκπρόσωπος της ΕΕ

Σύμφωνα με το άρθρο 27, οι οντότητες εκτός ΕΕ που εμπλέκονται στην επεξεργασία δεδομένων υπό την εφαρμογή του GDPR, υποχρεούνται να ορίσουν έναν εκπρόσωπο εντός της Ευρωπαϊκής Ένωσης. Αυτός ο «εκπρόσωπος της ΕΕ» λειτουργεί ως κύριο σημείο επικοινωνίας με τις ευρωπαϊκές αρχές εποπτείας και τα υποκείμενα των δεδομένων σχετικά με όλες τις διαδικασίες επεξεργασίας, εξασφαλίζοντας τη συμμόρφωση με τον κανονισμό. Ο εκπρόσωπος μπορεί να είναι φυσικό ή νομικό πρόσωπο και πρέπει να οριστεί μέσω γραπτού εγγράφου.

Η μη ορισμός εκπροσώπου εντός της ΕΕ θεωρείται σοβαρή παράβαση του GDPR, με δυνατότητα επιβολής προστίμων έως και 10 εκατομμύρια ευρώ ή έως 2% του ετήσιου παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι μεγαλύτερο. Ο σκόπιμος ή αμελής χαρακτήρας της παράβασης μπορεί να θεωρηθεί επιβαρυντικός παράγοντας. Ωστόσο, δεν απαιτείται η ορισμός εκπροσώπου αν η επεξεργασία είναι περιστασιακή, δεν περιλαμβάνει εκτεταμένη επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων σχετικών με ποινικές καταδίκες και δεν είναι πιθανό να δημιουργήσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, σύμφωνα με το άρθρο 9 και 10 του GDPR. Δημόσιες αρχές και οργανισμοί εκτός ΕΕ επίσης εξαιρούνται.

4.4 Πεδίο Εφαρμογής Γενικού Κανονισμού Προστασίας Δεδομένων

Ο κανονισμός GDPR εφαρμόζεται τόσο από τους υπεύθυνους επεξεργασίας δεδομένων (οργανισμοί που συλλέγουν δεδομένα από κατοίκους της ΕΕ) όσο και από τους επεξεργαστές (οργανισμοί που επεξεργάζονται δεδομένα για λογαριασμό των υπεύθυνων, όπως οι πάροχοι υπηρεσιών cloud computing) και τα πρόσωπα στα οποία αναφέρονται τα δεδομένα. Ο κανονισμός επεκτείνεται επίσης σε οργανισμούς που βρίσκονται εκτός ΕΕ, αν συλλέγουν ή επεξεργάζονται προσωπικά δεδομένα ατόμων εντός της ΕΕ.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, προσωπικά δεδομένα αποτελούν οποιαδήποτε πληροφορία που αφορά ένα άτομο, είτε αφορά την ιδιωτική, επαγγελματική ή δημόσια ζωή του, όπως όνομα, διεύθυνση, φωτογραφία, τραπεζικές λεπτομέρειες, ιατρικά στοιχεία, ή IP διεύθυνση.

Ο GDPR δεν εφαρμόζεται στην επεξεργασία δεδομένων που αφορούν εθνική ασφάλεια ή δραστηριότητες επιβολής του νόμου στην ΕΕ. Το άρθρο 48 ορίζει ότι αποφάσεις δικαστηρίων ή διοικητικών αρχών από τρίτες χώρες, που απαιτούν μεταβίβαση ή αποκάλυψη προσωπικών δεδομένων, δεν αναγνωρίζονται ή εκτελούνται εκτός και αν βασίζονται σε διεθνή συμφωνία, όπως μια συνθήκη αμοιβαίας δικαστικής συνδρομής μεταξύ της αιτούσας τρίτης χώρας και της ΕΕ ή ενός κράτους μέλους.

Υπάρχει επίσης μια ξεχωριστή οδηγία για την προστασία δεδομένων στον τομέα της αστυνομίας και της ποινικής δικαιοσύνης, η οποία καθορίζει τους κανόνες για την ανταλλαγή προσωπικών δεδομένων σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) συντονίζει τις εποπτικές αρχές (ΑΕΑ) σε όλα τα κράτη μέλη, οι οποίες είναι υπεύθυνες για την εξέταση καταγγελιών και την επιβολή διοικητικών ποινών. Αυτές οι αρχές συνεργάζονται, παρέχοντας αμοιβαία βοήθεια και διοργανώνοντας κοινές επιχειρήσεις, ενώ η κυρίαρχη αρχή λειτουργεί ως "μονοαπευθυντική θυρίδα" για την εποπτεία δραστηριοτήτων επεξεργασίας σε ολόκληρη την ΕΕ.

4.5 Νομική Βάση του Γενικού Κανονισμού Προστασίας Δεδομένων

Εάν ένα υποκείμενο δεδομένων έχει δώσει συγκατάθεση για την επεξεργασία των δεδομένων του για έναν ή περισσότερους συγκεκριμένους σκοπούς, η επεξεργασία των δεδομένων δεν μπορεί να πραγματοποιηθεί εκτός και αν υπάρχει τουλάχιστον μία νομική βάση για την επεξεργασία αυτή. Οι νομικές βάσεις περιλαμβάνουν:

- Νόμιμα συμφέροντα του υπεύθυνου επεξεργασίας ή τρίτου, εκτός εάν υπερισχύουν τα δικαιώματα του υποκειμένου, ιδιαίτερα αν πρόκειται για παιδιά.
- Εκτέλεση καθήκοντος που υπηρετεί το δημόσιο συμφέρον ή άσκηση εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.
- Συμμόρφωση με νομική υποχρέωση του υπεύθυνου επεξεργασίας.
- Εκπλήρωση συμβατικών υποχρεώσεων με το υποκείμενο των δεδομένων.
- Εκτέλεση καθηκόντων στο πλαίσιο της σύναψης συμβάσεων από αίτηση του υποκειμένου δεδομένων.

- Προστασία ζωτικών συμφερόντων του υποκειμένου δεδομένων ή άλλου προσώπου.

Εάν η συγκατάθεση χρησιμοποιηθεί ως νομική βάση για την επεξεργασία, αυτή πρέπει να είναι συγκεκριμένη και ρητή για τα δεδομένα που συλλέγονται και χρησιμοποιούνται για κάθε σκοπό. Οι υπεύθυνοι επεξεργασίας πρέπει να είναι σε θέση να αποδείξουν ότι η συγκατάθεση έχει χορηγηθεί ενεργά («opt-in»), και η συγκατάθεση μπορεί να ανακληθεί ανά πάσα στιγμή. Όταν πρόκειται για παιδιά κάτω των 16 ετών, η συγκατάθεση πρέπει να δίνεται από τον γονέα ή τον κηδεμόνα τους.

Η παροχή υπηρεσίας δεν πρέπει να εξαρτάται από τη συγκατάθεση για την επεξεργασία δεδομένων που δεν είναι απαραίτητη για τη χρήση αυτής της υπηρεσίας. Εάν έχει χορηγηθεί ήδη συγκατάθεση σύμφωνα με προηγούμενη νομοθεσία, ο υπεύθυνος επεξεργασίας δεν απαιτείται να λάβει νέα ή ανανεωμένη συγκατάθεση εφόσον η επεξεργασία συνάδει με τους κανόνες του GDPR.

4.6 Θέματα που χρίζουν περαιτέρω ανάλυσης σχετικά με το Γενικό Κανονισμό Προστασίας Δεδομένων

Η εισαγωγή του GDPR αποτέλεσε έναν σημαντικό βήμα προς την εναρμόνιση των πολιτικών προστασίας δεδομένων στην Ευρωπαϊκή Ένωση. Η ιδέα της ενιαίας θυρίδας, ενώ φαινομενικά απλή, αποδείχθηκε πολύπλοκη στην εφαρμογή της. Αυτή η πολυπλοκότητα επικεντρώνεται κυρίως στη δυνατότητα των υποκειμένων των δεδομένων να προσφεύγουν αποτελεσματικά στις αρμόδιες αρχές, καθώς οι εποπτικές αρχές της κύριας εγκατάστασης του υπεύθυνου επεξεργασίας ή του μεταποιητή είναι αρμόδιες για την εποπτεία σε όλα τα κράτη μέλη.

Αρχικά, το άρθρο 15 του GDPR προέβλεπε μια οργανωμένη διαδικασία όπου ο επικεφαλής εποπτικής αρχής θα είχε την κύρια ευθύνη για την εποπτεία των δραστηριοτήτων επεξεργασίας των εταιρειών που δραστηριοποιούνται σε πολλά κράτη μέλη. Ωστόσο, μετά από τις ανησυχίες που εκφράστηκαν από το Ευρωπαϊκό Κοινοβούλιο, η τελική διατύπωση στο άρθρο 54 τροποποιήθηκε ώστε να ενθαρρύνει τη συνεργασία μεταξύ όλων των αρμόδιων εποπτικών αρχών και να διευκολύνει την καταγγελία σε τοπικό επίπεδο.

Το Συμβούλιο παρουσίασε μια εκδοχή της ενιαίας θυρίδας που αποδυναμώνει την κεντρική εξουσία της κύριας εποπτικής αρχής, δίνοντας στις τοπικές εποπτικές αρχές την δυνατότητα να παρέμβουν και να ασκήσουν εποπτεία στην επικράτειά τους. Αυτό εισήγαγε μια περισσότερο διαχειριστική προσέγγιση, αυξάνοντας τη γραφειοκρατία και τις διαδικαστικές δυσκολίες, κάτι που ενδεχομένως να αποθαρρύνει την αρχική πρόθεση για απλοποίηση και εναρμόνιση.

Τέλος, η διαμόρφωση και η εφαρμογή του GDPR προκάλεσαν ένα σημαντικό κύμα αλλαγών στη διαχείριση δεδομένων σε διεθνές επίπεδο, με εταιρείες και οργανισμούς να προσαρμόζονται σε μια νέα εποχή προστασίας της προσωπικής πληροφορίας. Αυτή η προσαρμογή περιελάμβανε την αναθεώρηση πολιτικών, τη βελτίωση μέτρων ασφαλείας και τη διασφάλιση δικαιωμάτων πρόσβασης και ελέγχου για τους χρήστες, επιβεβαιώνοντας την αυξημένη ενημέρωση και εμπλοκή τους στη διαχείριση των προσωπικών τους δεδομένων.

4.7 Επίδραση του Γενικού Κανονισμού Προστασίας Δεδομένων στη διεθνή νομοθεσία

Η ευρεία υιοθέτηση των κανόνων απορρήτου που εισήγαγε το GDPR έχει προκαλέσει αυτό που συχνά αποκαλείται ως «φαινόμενο των Βρυξελλών», όπου οι ευρωπαϊκές ρυθμίσεις αποτελούν πρότυπο για τη διαμόρφωση παγκόσμιων πρακτικών. Αυτός ο σημαντικός αντίκτυπος του GDPR έχει διεθνείς επιπτώσεις, καθώς εταιρείες πέρα από τα ευρωπαϊκά σύνορα προσαρμόζουν τις πολιτικές τους για να συμμορφώνονται με τις αυστηρές απαιτήσεις του.

Ένας από τους πιο εμφανείς νόμους που επηρεάστηκαν από το GDPR είναι ο νόμος περί απορρήτου των καταναλωτών της Καλιφόρνια στις ΗΠΑ, ο οποίος υιοθετήθηκε στις 28 Ιουνίου 2018 και έλαβε ισχύ την 1η Ιανουαρίου 2020. Αυτός ο νόμος παρέχει δικαιώματα διαφάνειας και ελέγχου παρόμοια με αυτά του GDPR, όσον αφορά τη συλλογή προσωπικών πληροφοριών από εταιρείες. Οι επικριτές του νόμου προτείνουν ότι για μεγαλύτερη αποτελεσματικότητα, τέτοιες ρυθμίσεις θα έπρεπε να εφαρμόζονται σε ομοσπονδιακό επίπεδο, καθώς η διατήρηση διαφορετικών προτύπων σε κρατικό επίπεδο μπορεί να δυσκολεύει τη συμμόρφωση των εταιρειών.

Επιπλέον, η Τουρκία, ως υποψήφια χώρα για ένταξη στην Ευρωπαϊκή Ένωση, ενέκρινε τον νόμο για την προστασία των προσωπικών δεδομένων στις 24 Μαρτίου 2016, συμμορφούμενη με τα πρότυπα του GDPR. Αυτή η κίνηση αντανακλά την επιρροή της Ευρωπαϊκής Ένωσης στη διαμόρφωση νομοθεσίας πέρα από τα άμεσα μέλη της και ενισχύει την παγκόσμια διάδοση των προτύπων προστασίας δεδομένων που εισήγαγε το GDPR.

Οι διεθνείς επιπτώσεις του GDPR υπογραμμίζουν τη δύναμη των ευρωπαϊκών κανονιστικών προτύπων να λειτουργούν ως παγκόσμια βάση για τη διαμόρφωση παρόμοιων νομοθετικών προσεγγίσεων στην προστασία των δεδομένων παγκοσμίως, αναδεικνύοντας την ανάγκη για παγκόσμια συνεργασία και εναρμόνιση στο πεδίο της πληροφοριακής ασφάλειας και της προσωπικής ιδιωτικότητας.

4.8 Διαδίκτυο των πραγμάτων (IOT) και Γενικός Κανονισμός Προστασίας Δεδομένων

Στο Διαδίκτυο των Πραγμάτων (IoT), τεχνολογίες αναγνώρισης και ελέγχου πρόσβασης διαδραματίζουν κεντρικό ρόλο, καθώς επιτρέπουν τη σύνδεση διαφορετικών συσκευών με μοναδικές ταυτότητες, παρέχοντας έτσι συνεχείς και αδιάλειπτες υπηρεσίες. Παρ' όλα αυτά, οι μέθοδοι δημιουργίας προφίλ μέσω συνδεδεμένων δεδομένων μπορεί να αποκαλύψουν λεπτομέρειες για την ταυτότητα και την ιδιωτική ζωή των χρηστών, κάτι που ενδέχεται να οδηγήσει σε διακρίσεις και άλλες αρνητικές συνέπειες.

Είναι απαραίτητο να επιτευχθεί ένας κατάλληλος συμβιβασμός μεταξύ των απαιτήσεων για αναγνώριση και ελέγχου πρόσβασης στο IoT και των δικαιωμάτων των χρηστών για προστασία της ιδιωτικότητας και της ταυτότητάς τους. Η επίτευξη αυτού του συμβιβασμού παρουσιάζει σημαντικές προκλήσεις λόγω των αδυναμιών στις τεχνικές ασφαλείας και των περιορισμών των τεχνικών ανωνυμοποίησης.

4.9 Επιχειρήσεις και Γενικός Κανονισμός Προστασίας Δεδομένων

Στη μελέτη του Colin Tankard το 2016, αναδεικνύεται η σημασία του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) για τις επιχειρήσεις. Ο GDPR, ένας κανονισμός που προβλέπει ουσιαστικές αλλαγές στη διαχείριση προσωπικών δεδομένων, εγκρίθηκε προσωρινά τον Δεκέμβριο του 2015 και τελικοποιήθηκε τον Ιούλιο του 2016. Ακολούθησε μια διετής περίοδος προσαρμογής, κατά την οποία οι επιχειρήσεις προετοιμάστηκαν για πλήρη συμμόρφωση με τον κανονισμό από τον Μάιο του 2018.

Διαφορετικά από τις οδηγίες, οι κανονισμοί όπως ο GDPR απαιτούν άμεση εφαρμογή σε όλα τα κράτη μέλη της ΕΕ, επιβάλλοντας έτσι ομοιομορφία στην προστασία δεδομένων σε όλη την Ευρώπη. Ο GDPR επεκτείνει το πεδίο εφαρμογής της προστασίας σε οποιονδήποτε οργανισμό, εντός ή εκτός ΕΕ, που συλλέγει ή επεξεργάζεται δεδομένα πολιτών της ΕΕ. Αυτό σημαίνει ότι οποιαδήποτε επιχείρηση που ασχολείται με δεδομένα που αφορούν πολίτες της ΕΕ πρέπει να διασφαλίζει ότι οι πρακτικές της συμμορφώνονται με τα υψηλά πρότυπα ασφαλείας και διαφάνειας που ορίζει ο κανονισμός.

Ο Tankard επισημαίνει ότι η εισαγωγή του GDPR συνέβαλε σημαντικά στην αναβάθμιση των μεθόδων διαχείρισης και προστασίας δεδομένων στις επιχειρήσεις. Η υποχρέωση της συμμόρφωσης δημιούργησε νέες ανάγκες για εσωτερικές πολιτικές και συστήματα που ενισχύουν τη διαφάνεια και την ασφάλεια, ενώ παράλληλα προστατεύουν τα δικαιώματα των υποκειμένων των δεδομένων.

Η εφαρμογή του GDPR έχει ως αποτέλεσμα όχι μόνο την ενίσχυση της προστασίας του απορρήτου και της ασφάλειας στο ψηφιακό χώρο αλλά και την ενίσχυση της νομικής και επιχειρηματικής εμπιστοσύνης, καθώς οι εταιρείες που συμμορφώνονται είναι πιο πιθανό να θεωρούνται αξιόπιστες από καταναλωτές και επιχειρηματικούς εταίρους. Η συμμόρφωση με το GDPR θεωρείται επίσης κρίσιμος παράγοντας για τη διασφάλιση της εμπορικής επιτυχίας στην παγκόσμια αγορά, καθώς η προστασία δεδομένων αποτελεί πλέον βασικό κριτήριο για τους καταναλωτές και τους ρυθμιστικούς φορείς ανά τον κόσμο.

Οι επιχειρήσεις, σύμφωνα με το GDPR, έχουν την υποχρέωση να διασφαλίσουν ότι όλα τα προσωπικά δεδομένα που συλλέγονται πραγματοποιούνται νόμιμα και αυστηρά. Επίσης, πρέπει να προστατεύουν τα δεδομένα από την εκμετάλλευση, αλλά και να σέβονται τα δικαιώματα των κατόχων των δεδομένων. Τέλος, χρειάζεται η αντιμετώπιση κάποιων πολύ σοβαρών κυρώσεων εφόσον αποτύχει η προστασία των δεδομένων.

Είναι αξιοσημείωτο το γεγονός ότι το GDPR εφαρμόζεται σε επιχειρήσεις και επαγγελματίες οι οποίοι εργάζονται και διαμένουν στην ΕΕ, αλλά και για επιχειρήσεις εκτός της ΕΕ εάν προσφέρουν υπηρεσίες ή αγαθά σε πελάτες στην ΕΕ. Ουσιαστικά το GDPR πρόκειται για μια νομοθεσία που εξαπλώνεται σε όλο τον κόσμο, διότι οι εταιρείες που εδρεύουν εκτός ΕΕ θα εξακολουθούν να συμμορφώνονται.

Η Ευρωπαϊκή Επιτροπή όσον αφορά το πώς θα επηρεάσει το GDPR τις επιχειρήσεις, υποστηρίζει ότι με την ενοποίηση των κανόνων της Ευρώπης όσον αφορά την προστασία των δεδομένων, οι νομοθέτες δημιουργούν μια επιχειρηματική ευκαιρία και στηρίζουν την καινοτομία. Επίσης, με την ύπαρξη μιας αρχής για ολόκληρη την ΕΕ, θα δημιουργηθεί μια πιο απλή και πιο φθηνή διαδικασία για επιχειρήσεις που κινούνται στην περιοχή. Αυτό θα συμβεί με προϊόντα και τεχνολογίες που θα προσφέρουν ουσιαστικά «προστασία δεδομένων από τον σχεδιασμό και από προεπιλογή

4.10 Μεταφορά δεδομένων και Γενικός Κανονισμός Προστασίας Δεδομένων

Το δικαίωμα στη φορητότητα δεδομένων αναγνωρίζεται ως μία από τις κυριότερες καινοτομίες στο πλαίσιο του Γενικού Κανονισμού της ΕΕ για την Προστασία Δεδομένων (GDPR). Αυτό το δικαίωμα ενδυναμώνει τα άτομα παρέχοντάς τους την εξουσία να ελέγχουν τα προσωπικά τους δεδομένα και να τα μεταφέρουν ελεύθερα από έναν ελεγκτή δεδομένων σε άλλον, χωρίς εμπόδια, ενισχύοντας έτσι τον ανταγωνισμό μεταξύ των ψηφιακών υπηρεσιών και τη διαλειτουργικότητα των πλατφορμών.

Το δικαίωμα αυτό επιτρέπει στους χρήστες να απολαμβάνουν τα οφέλη του "άυλου πλούτου" των προσωπικών τους δεδομένων, και υποστηρίζει την ανάπτυξη τεχνολογιών που προστατεύουν την ιδιωτικότητα, ενώ επίσης ενισχύει την ελεγκτική λειτουργία των ατόμων επί των δεδομένων τους. Αυτό καθιστά το δικαίωμα στη φορητότητα δεδομένων ένα ισχυρό εργαλείο για την προάσπιση των δικαιωμάτων των ατόμων σε μια ψηφιακά διασυνδεδεμένη εποχή.

Ωστόσο, η πρακτική εφαρμογή του δικαιώματος στη φορητότητα δεδομένων χρήζει περαιτέρω διευκρινίσεων. Το άρθρο του GDPR που διέπει αυτό το δικαίωμα είναι ανοιχτό σε πολλαπλές ερμηνείες, ιδιαίτερα σχετικά με το αντικείμενο του δικαιώματος και τις σχέσεις του με άλλα δικαιώματα, όπως τα δικαιώματα πνευματικής ιδιοκτησίας και την προστασία καταναλωτών. Αυτό θέτει σημαντικές προκλήσεις στην αποτελεσματική εφαρμογή του δικαιώματος, καθώς οι οργανισμοί πρέπει να προσαρμόζουν τις τεχνολογικές και διοικητικές τους δομές για να διασφαλίσουν την πλήρη συμμόρφωση με τον κανονισμό.

4.11 Πολίτες και Γενικός Κανονισμός Προστασίας Δεδομένων

Ο τρόπος με τον οποίο οι πολίτες είναι τώρα εξασφαλισμένοι με το δικαίωμα να γνωρίζουν πότε έχουν παραβιαστεί τα δεδομένα τους είναι μία από τις μεγαλύτερες αλλαγές που επέφερε το GDPR. Οι εταιρίες υποχρεούνται από το νόμο να ειδοποιούν τους καθορισμένους αρμόδιους εθνικούς οργανισμούς στην περίπτωση που εντοπιστεί παράβαση στα συστήματα τους, προκειμένου να διασφαλιστεί ότι τα δεδομένα των πελατών που διατηρούν δεν έχουν καταχραστεί. Με τον τρόπο αυτό, οι πελάτες θα έχουν μια πιο διαφανή εικόνα του τρόπου επεξεργασίας των δεδομένων τους.

Ήδη πολλές εταιρίες έχουν προοδεύσει προς αυτή τη διαφάνεια μεταξύ αυτών και των πελατών τους. Αυτό γίνεται με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου από εταιρείες που δίνουν πολύ περισσότερες πληροφορίες σχετικά με τον τρόπο χρήσης των δεδομένων. Ακόμα, πολλοί οργανισμοί συνομιλούν με τους πελάτες για να διαπιστώσουν εάν επιθυμούν ή όχι να είναι μέρος της βάσης δεδομένων τους, καθιστώντας έτσι το ίδιο εύκολο για τον πελάτη να αποχωρήσει από την ύπαρξη του σε λίστες αλληλογραφίας

4.12 Η ασφάλεια στον κυβερνοχώρο ως στρατηγική επιχειρηματική προτεραιότητα

Η ασφάλεια στον κυβερνοχώρο έχει εξελιχθεί σε μία από τις κυρίαρχες στρατηγικές επιχειρηματικές προτεραιότητες. Αντίθετα με το παρελθόν, όπου οι εταιρείες συχνά υιοθετούσαν μια αμυντική στάση έναντι των κυβερνοαπειλών, χωρίς να ενσωματώνουν ουσιαστικά την κυβερνοασφάλεια στις καθημερινές τους επιχειρηματικές πρακτικές, πλέον αυτή η προσέγγιση έχει αλλάξει δραστικά.

Σήμερα, η ασφάλεια στον κυβερνοχώρο αντιμετωπίζεται ως ουσιαστικό στοιχείο της επιχειρηματικής στρατηγικής, το οποίο ενσωματώνεται ενεργά στη διαδικασία λήψης αποφάσεων από την ανώτερη διοίκηση. Οι οργανισμοί πρέπει να εξασφαλίσουν ότι οι αμυντικές τους τακτικές είναι αποτελεσματικές και συνεχώς αξιολογούνται, για να προσαρμόζονται στο διαρκώς μεταβαλλόμενο τοπίο των απειλών.

Είναι κρίσιμης σημασίας οι επιχειρήσεις να υιοθετούν τις πιο σύγχρονες τεχνολογίες ασφαλείας και να διαθέτουν την απαραίτητη τεχνογνωσία, ώστε να προστατεύουν επαρκώς τα δεδομένα και τα συστήματά τους. Η συνεχής εκπαίδευση και η ενημέρωση του προσωπικού σχετικά με τις καλύτερες πρακτικές κυβερνοασφάλειας αποτελούν επίσης κεντρικό στοιχείο για τη διασφάλιση της εταιρικής ασφάλειας.

Αυτή η νέα προσέγγιση αντικατοπτρίζει μια στρατηγική αλλαγή: η κυβερνοασφάλεια δεν είναι πλέον απλώς ένας τομέας τεχνικής διαχείρισης κινδύνου, αλλά μια βασική επιχειρηματική λειτουργία που απαιτεί διαρκή επενδύσεις και στρατηγική σκέψη για την ενίσχυση της εταιρικής ανθεκτικότητας στον ψηφιακό κόσμο.

4.13 Η επίδραση του Γενικού Κανονισμού Προστασίας Δεδομένων στην ασφάλεια

Η επεξεργασία των προσωπικών δεδομένων αποτελεί πρωταρχικό μέσο για την παροχή υπηρεσιών και τη διευκόλυνση της ανθρώπινης δραστηριότητας σε πολλούς τομείς, όπως η υγεία, η εκπαίδευση, η έρευνα και πολλοί άλλοι. Ωστόσο, παράλληλα με την αξία που φέρνει στην κοινωνία, η επεξεργασία αυτών των δεδομένων εγείρει σημαντικά ηθικά και νομικά ζητήματα. Η ανάγκη για προστασία των προσωπικών δεδομένων αναδεικνύεται ως βασική αρχή, που πρέπει να ισορροπεί με άλλες αναγκαιότητες της κοινωνίας, όπως η ασφάλεια και η ελευθερία.

Οι τεχνολογικές εξελίξεις και η παγκοσμιοποίηση έχουν επιταχύνει τη ροή των προσωπικών δεδομένων σε παγκόσμιο επίπεδο. Αυτό έχει δημιουργήσει νέες προκλήσεις σχετικά με τον

έλεγχο, την προστασία και τη διαχείριση αυτών των δεδομένων. Ταυτόχρονα, οι ιδιωτικές επιχειρήσεις και οι δημόσιες αρχές εκμεταλλεύονται αυτές τις εξελίξεις για να αναπτύξουν νέες υπηρεσίες και προϊόντα που στηρίζονται στα δεδομένα των χρηστών.

Ωστόσο, η συλλογή και η χρήση των προσωπικών δεδομένων πρέπει να γίνεται με διαφάνεια και σεβασμό προς τα δικαιώματα των ατόμων. Η ασφάλεια των δεδομένων και η προστασία της ιδιωτικής ζωής πρέπει να είναι προτεραιότητες. Επίσης, η ενίσχυση της νομικής ασφάλειας και η επιβολή αυστηρών κανονισμών είναι απαραίτητες για τη δημιουργία εμπιστοσύνης στις ψηφιακές υπηρεσίες και την προστασία των ατόμων από τυχόν καταχρήσεις.

Το δικαίωμα των ατόμων να έχουν έλεγχο επί των προσωπικών τους δεδομένων είναι θεμελιώδες και πρέπει να ενισχυθεί μέσω διαφανών και εύκολα προσβάσιμων μηχανισμών. Επιπλέον, η διασφάλιση της προστασίας των δεδομένων δεν πρέπει να αποτελεί εμπόδιο για την ελεύθερη κυκλοφορία των δεδομένων εντός της Ένωσης και προς τρίτες χώρες, αλλά πρέπει να συμβιβάζεται με την ανάγκη για ελεύθερη ανταλλαγή πληροφοριών για την οικονομική ανάπτυξη και την καινοτομία.

Σε τελική ανάλυση, η διαχείριση των προσωπικών δεδομένων απαιτεί ένα ισορροπημένο πλαίσιο που να λαμβάνει υπόψη τις ανάγκες και τα δικαιώματα των ατόμων, τις τεχνολογικές εξελίξεις και τις κοινωνικοοικονομικές ανάγκες της εποχής μας. Μόνο με αυτόν τον τρόπο μπορούμε να διασφαλίσουμε μια δίκαιη και αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα στην εποχή της ψηφιακής επανάστασης.

4.14 Συμπέρασμα

Ο Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation / GDPR) αποτελεί ένα σημαντικό μέσο για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων των πολιτών της ΕΕ σε μια εποχή διαρκούς ψηφιοποίησης και διασύνδεσης. Έχοντας ως βάση την προηγούμενη οδηγία 95/46/ΕΚ, ο GDPR επιδιώκει να ενισχύσει τα δικαιώματα των ατόμων σε σχέση με την επεξεργασία των προσωπικών τους δεδομένων και να επιβάλει αυστηρότερες υποχρεώσεις στις επιχειρήσεις που διαχειρίζονται αυτά τα δεδομένα.

Ένα από τα κύρια χαρακτηριστικά του GDPR είναι η εκτεταμένη εφαρμογή του, καθώς ισχύει για όλες τις επιχειρήσεις που επεξεργάζονται προσωπικά δεδομένα των πολιτών της ΕΕ, ανεξάρτητα από την τοποθεσία της εταιρείας. Η επιβολή αυτής της κανονιστικής προσέγγισης αντικατοπτρίζει την ανάγκη για ολοκληρωμένη προστασία των δεδομένων σε έναν ψηφιακά διασυνδεδεμένο κόσμο.

Ένα από τα κύρια οφέλη του GDPR είναι η ενίσχυση της διαφάνειας και του έλεγχου που έχουν οι χρήστες επί των προσωπικών τους δεδομένων. Μέσω του δικαιώματος της πρόσβασης, του δικαιώματος της διόρθωσης και του δικαιώματος της διαγραφής, οι χρήστες έχουν περισσότερο έλεγχο επί της προσωπικής τους πληροφορίας. Επιπλέον, ο "Δικαίωμα να ξεχαστεί" δίνει στους χρήστες το δικαίωμα να ζητήσουν τη διαγραφή των προσωπικών τους δεδομένων σε συγκεκριμένες περιπτώσεις.

Μια άλλη σημαντική πτυχή του GDPR είναι η υποχρέωση για τις επιχειρήσεις να εφαρμόζουν τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων. Αυτό περιλαμβάνει την ανάπτυξη πολιτικών ασφαλείας, την ψευδωνυμοποίηση και κρυπτογράφηση των δεδομένων, και την εφαρμογή μέτρων για τη διατήρηση της διαθεσιμότητας, της ακεραιότητας και της αξιοπιστίας των δεδομένων.

Το GDPR αναμένεται να δημιουργήσει ένα περιβάλλον όπου οι πολίτες θα έχουν περισσότερη εμπιστοσύνη στην επεξεργασία των προσωπικών τους δεδομένων και οι επιχειρήσεις θα επωφεληθούν από την ενίσχυση της εμπιστοσύνης των πελατών τους και την ανάπτυξη ανταγωνιστικού πλεονεκτήματος μέσω της συμμόρφωσης με τους κανονισμούς προστασίας δεδομένων.

5 Επισκόπηση ενός προγράμματος Διακυβέρνησης Δεδομένων

Ένα πρόγραμμα διακυβέρνησης δεδομένων έχει ως απώτερο στόχο την αυτοκατάργησή του. Παρόλο που αυτή η ιδέα μπορεί να ακούγεται παράδοξη, εντούτοις, είναι ακριβής. Στην ουσία, ένα πρόγραμμα διακυβέρνησης δεδομένων αναπτύσσει ένα νέο σύνολο αρχών για τη διαχείριση ενός πολύτιμου περιουσιακού στοιχείου με βελτιωμένο τρόπο. Στην τελική ανάλυση, το πραγματικό δείγμα επιτυχίας είναι όταν ο οργανισμός αντιμετωπίζει τα δεδομένα του με τον ίδιο τρόπο που αντιμετωπίζει τα εργοστάσια, τις αλυσίδες εφοδιασμού, τους προμηθευτές και τους πελάτες του. Στον εικοστό πρώτο αιώνα, κανένας διευθυντής δεν διαφωνεί με τα πρότυπα για το χειρισμό των υλικών, τους κανόνες απόσβεσης ή το απόρρητο των πελατών. Αυτές είναι αποδεκτές επιχειρηματικές πρακτικές. Δεν υπάρχει συζήτηση για το αν πρέπει να έχετε πρότυπα ή ελέγχους. Ωστόσο, είναι εύκολο να εξαπλωθούν τα δεδομένα σε όλο τον οργανισμό σε σημείο που η διαχείρισή τους να είναι υπερβολικά δαπανηρή και η εύρεση ή κατανόησή τους να μην είναι δυνατή.

Η διασφάλιση της καλής κατανόησης του τρόπου με τον οποίο ένα πρόγραμμα διακυβέρνησης δεδομένων μοιάζει και λειτουργεί είναι απαραίτητη για την εμπλοκή των συμμετεχόντων. Η έννοια της αφομοίωσης της διακυβέρνησης δεδομένων στην καθημερινή εταιρική ζωή προσθέτει πρόσθετη πρόκληση, δεδομένου ότι δεν καθορίζεται και υλοποιείται μόνο ένα διακριτό πρόγραμμα- επιχειρείται επίσης να αλλάξει η συμπεριφορά σε σημείο που το μακροπρόθεσμο πρόγραμμα να είναι ορατό μόνο μέσω της επαλήθευσης και της προσαρμογής.

Ανεξάρτητα από το αν η διακυβέρνηση δεδομένων είναι καινούργια ή αν έχει ενδημήσει και θεσμοθετηθεί, υπάρχει μια συλλογή στοιχείων που χαρακτηρίζουν και περιγράφουν ένα πρόγραμμα διακυβέρνησης δεδομένων. Η κατανόηση του τρόπου με τον οποίο αυτά συνεργάζονται βοηθά στην κατανόηση της «μεγάλης εικόνας». Το παρόν κεφάλαιο εξετάζει το πεδίο εφαρμογής, το περιεχόμενο αυτών των στοιχείων και την αλληλεπίδρασή τους

5.1 Πεδίο Εφαρμογής

Αναφέραμε ήδη ότι η διακυβέρνηση δεδομένων (ΔΔ) είναι μια επιχειρησιακή έννοια. Πρέπει να αναγνωριστεί ότι ο οργανισμός θα υιοθετήσει μια νοοτροπία που απαιτεί μεγαλύτερη αυστηρότητα όσον αφορά τον χειρισμό των δεδομένων και των πληροφοριών του. Ωστόσο, η δήλωση του πεδίου εφαρμογής της διακυβέρνησης δεδομένων είναι λίγο πιο περίπλοκη από το να πούμε: «Κυβερνούμε τα πάντα». Σημαίνει ότι πρέπει να ληφθούν υπόψη ορισμένοι βασικοί παράγοντες που επηρεάζουν το πεδίο εφαρμογής και στη συνέχεια να βεβαιωθείτε ότι είστε

πολύ σαφείς ως προς τον ορισμό της εμβέλειας και του εύρους της διακυβέρνησης δεδομένων υπό το πρίσμα αυτών των παραγόντων. Οι τρεις παράγοντες που πρέπει να λάβετε υπόψη σας και επηρεάζουν το πεδίο εφαρμογής της Διακυβέρνηση δεδομένων είναι οι εξής

- Επιχειρηματικό μοντέλο: Ο τύπος του οργανισμού, η εταιρική του ιεραρχία και το περιβάλλον λειτουργίας του.
- Περιεχόμενο που ρυθμίζεται: Ο τύπος του περιεχομένου (δεδομένα, πληροφορίες, έγγραφα κ.λπ.), η τοποθεσία του και η επιχειρηματική του σημασία.
- Βαθμός ομοσπονδιοποίησης: Η έκταση ή η ένταση με την οποία ρυθμίζεται το διαφορετικό περιεχόμενο.

5.2 Επιχειρησιακό μοντέλο

Για παράδειγμα, μια μεγάλη πολυεθνική εταιρεία δεν χρειάζεται να αναπτύξει ένα παγκόσμιο πρόγραμμα Διακυβέρνηση δεδομένων από την αρχική αναφορά της λέξης διακυβέρνηση. Το πεδίο εφαρμογής μπορεί να είναι ένας αυτοτελής επιχειρηματικός τομέας. Ας υποθέσουμε ότι είστε μια μεγάλη διεθνής εταιρεία χημικών προϊόντων. Το επιχειρηματικό σας μοντέλο μπορεί να περιλαμβάνει φαρμακευτικά, γεωργικά και διυλιστικά τμήματα. Όλα αυτά θα λειτουργούσαν σε μια περισσότερο ή λιγότερο αυτοτελή βάση. Μπορεί τότε να υπάρχουν τρία «προγράμματα» Διακυβέρνηση δεδομένων που το καθένα είναι παρόμοιο στη σύνθεση, αλλά ξεχωριστά υπόλογα.

5.3 Περιεχόμενο

Πρόκειται για φιλοσοφικές και σημασιολογικές διακρίσεις που προκαλούν σημαντική σύγχυση και δεν έχουν σχέση με την παρούσα συζήτηση. Επίσης, δεν κυβερνάμε διαφορετικά τους διαφορετικούς τύπους περιεχομένου. Στο τέλος της ημέρας, η δραστηριότητα για τη διακυβέρνηση των δεδομένων επιχειρηματικής ευφυΐας, των επιχειρησιακών δεδομένων, των ηλεκτρονικών μηνυμάτων, των συμβάσεων, των εγγράφων ή ακόμη και των μέσων ενημέρωσης, καθοδηγείται από τους ίδιους λόγους και συνεπάγεται τις ίδιες δραστηριότητες.

Παρόλο που δεν κάνουμε διάκριση στον τρόπο με τον οποίο ρυθμίζεται το διαφορετικό περιεχόμενο, πρέπει να είμαστε σαφείς στο πλαίσιο ενός συγκεκριμένου οργανισμού για το ποιοι τύποι περιεχομένου υπόκεινται σε Διακυβέρνηση δεδομένων. Σίγουρα, τα κύρια δεδομένα, τα δεδομένα BI και άλλες μορφές δομημένων δεδομένων πιθανότατα διέπονται.

Ωστόσο, μια έντονα ρυθμιζόμενη εταιρεία μπορεί επίσης να χρειάζεται να διέπει τα μηνύματα ηλεκτρονικού ταχυδρομείου και τις συμβάσεις.

Μια εταιρεία στην οποία η ασφάλεια αποτελεί μείζον ζήτημα μπορεί να χρειαστεί να επικεντρώσει τη διακυβέρνηση της στις κατευθυντήριες γραμμές και τις διαδικασίες. Ένας κυβερνητικός φορέας μπορεί να χρειαστεί να επικεντρωθεί στη διακυβέρνηση της πρόσβασης σε δημόσια έγγραφα, προστατεύοντας παράλληλα την ιδιωτική ζωή των ατόμων.

Οι τύποι περιεχομένου που υπόκεινται σε Διακυβέρνηση δεδομένων θα επηρεάσουν σε μεγάλο βαθμό το πού βρίσκεται το πρόγραμμα Διακυβέρνηση δεδομένων, ποιος φέρει την ευθύνη και πώς ο οργανισμός αναπτύσσει το πρόγραμμα Διακυβέρνηση δεδομένων. Θα επηρεάσει επίσης τους τύπους εργαλείων και πολιτικών που πρέπει να καθορίσει ο οργανισμός Διακυβέρνηση δεδομένων.

Οι τύποι περιεχομένου είναι επίσης σημαντικοί επειδή, ενώ τα προγράμματα Διακυβέρνηση δεδομένων περιέχουν τα ίδια στοιχεία ανεξάρτητα από το περιεχόμενο που διέπεται, πολύ συχνά οι τύποι περιεχομένου θα επηρεάσουν τις λεπτομερείς διαδικασίες διακυβέρνησης. Οι διαφορετικοί τύποι περιεχομένου θα έχουν μοναδικούς κύκλους ζωής. Για παράδειγμα, το περιεχόμενο που είναι ένας δομημένος τύπος δεδομένων, όπως μια συναλλαγή, μπορεί να έρχεται και να φεύγει μέσα σε ένα οικονομικό έτος και η διακυβέρνηση θα τείνει να εστιάζει στη χρήση των δεδομένων αυτών εντός της χρονικής περιόδου. Ένας μη δομημένος τύπος δεδομένων, όπως οι συμβάσεις και τα μηνύματα ηλεκτρονικού ταχυδρομείου, μπορεί να χρειάζεται να διατηρούνται για δεκαετίες και μπορεί να υπόκεινται σε νομική ανακάλυψη ή σε αυστηρές ταξινομήσεις απορρήτου ή προνομίων. Προφανώς, θα πρέπει να εξεταστούν οι λεπτομέρειες της διακυβέρνησης αυτών των διαφορετικών τύπων.

Η ανάπτυξη και η συντήρηση εφαρμογών και συστημάτων θα πρέπει επίσης να λαμβάνεται υπόψη στον τύπο διακυβέρνησης. Πολλοί από τους πελάτες μας έχουν καθορισμένη διαδικασία ανάπτυξης ή κύκλο ζωής ανάπτυξης συστημάτων (SDLC) για τον καθορισμό και την ανάπτυξη αυτοματοποιημένων συστημάτων. Λίγοι από αυτούς έχουν δημιουργήσει οποιοδήποτε είδος εξέτασης για το σχεδιασμό γύρω από τις πολιτικές και τα πρότυπα της Διακυβέρνηση δεδομένων. Πολύ συχνά, καταλήγουμε να γράφουμε βελτιώσεις στις μεθοδολογίες SDLC των εταιρικών τμημάτων πληροφορικής όταν οι δομημένες πληροφορίες είναι

ρυθμίζονται. Οι βελτιώσεις παίρνουν τη μορφή επιπλέον αντικειμένων και διακλαδίζονται σε πρόσθετες εργασίες ή νέες εγκρίσεις και σημεία ελέγχου. Όταν οι μη δομημένες πληροφορίες υπόκεινται σε Διακυβέρνηση δεδομένων, πρέπει συχνά να τροποποιούμε τις διαδικασίες ροής εργασιών και διαχείρισης εγγράφων

5.4 Ομοσπονδία

Μία από τις σημαντικότερες έννοιες που επηρεάζουν τη φύση και το πεδίο εφαρμογής της διακυβέρνησης δεδομένων είναι αυτή της «ομοσπονδίας». Ο ορισμός της ομοσπονδίας στο λεξικό Webster προσφέρει κάποια εικόνα:

1. Μια περιεκτική πολιτική ή κοινωνική οντότητα που σχηματίζεται με τη συνένωση μικρότερων ή πιο εντοπισμένων οντοτήτων: όπως α : μια ομοσπονδιακή κυβέρνηση, β : μια ένωση οργανισμών
2. Η πράξη της δημιουργίας ή της μετατροπής σε ομοσπονδία, ιδίως : η δημιουργία μιας ομοσπονδιακής ένωσης

Για τη διακυβέρνηση δεδομένων, αυτό σημαίνει τον ορισμό μιας οντότητας (το πρόγραμμα Διακυβέρνηση δεδομένων) που αποτελεί ένα ξεχωριστό μείγμα λειτουργιών διακυβέρνησης, όπου οι διάφορες πτυχές της Διακυβέρνηση δεδομένων αγγίζουν τον οργανισμό. Η ομοσπονδία ενός προγράμματος διακυβέρνησης δεδομένων είναι ο ορισμός του πού και πώς θα εφαρμοστούν τα πρότυπα σε διάφορα επίπεδα και τμήματα ενός οργανισμού. Αυτό γίνεται καλύτερα κατανοητό εξετάζοντας έναν άλλο ομοσπονδιακό οργανισμό, την κυβέρνηση των Ηνωμένων Πολιτειών. Πολιτικά, οι Ηνωμένες Πολιτείες είναι μια ομοσπονδία, μια οργάνωση πολιτειών με ένα ομοσπονδιακό επίπεδο εποπτείας. Στις Ηνωμένες Πολιτείες, ορισμένες δραστηριότητες της κυβέρνησης είναι κεντρικές. Υπάρχει ένας κεντρικός στρατός και ένα αποθεματικό τραπεζικό σύστημα. Άλλες λειτουργίες της κυβέρνησης λειτουργούν σε πολιτειακό ή τοπικό επίπεδο, όπως η ιατρική περίθαλψη και η επιβολή του νόμου. Ένα πρόγραμμα διακυβέρνησης δεδομένων θα απαιτήσει τον ίδιο τύπο ορισμού των απαιτούμενων επιπέδων λειτουργιών διακυβέρνησης.1 Ο ορισμός της ομοσπονδίας θα επηρεάσει το πεδίο εφαρμογής της οργάνωσης της Διακυβέρνηση δεδομένων σας, τις διαδικασίες και τις αρχές της.

Η ομοσπονδία επηρεάζει τον χαρακτήρα και τη λειτουργία του προγράμματος Διακυβέρνηση δεδομένων. Σημειώστε στο Σχήμα 3-2, παρουσιάζουμε έναν χάρτη θερμότητας όπου παρόμοια περιουσιακά στοιχεία δεδομένων μπορούν να κυβερνώνται αυστηρά (στο κέντρο ή στην καυτή ζώνη) ή πιο χαλαρά (στο περιθώριο ή στην ψυχρή ζώνη). Οι συμπαγείς περιοχές υποδεικνύουν μια κυβερνημένη περιοχή που ονομάζεται «στοιχείο», όπου υπάρχει αυστηρός έλεγχος των παγκόσμιων στοιχείων, ελαφρώς χαλαρότερος έλεγχος στα περιφερειακά στοιχεία και τα τοπικά στοιχεία κυβερνώνται ελάχιστα. Οι διακεκομμένες περιοχές υποδεικνύουν ένα άλλο αντικείμενο, τον «πελάτη». Εξακολουθεί να υπάρχει ο αυστηρός έλεγχος για το περιεχόμενο πελατών που χρησιμοποιείται κεντρικά, αλλά το περιφερειακό και το τοπικό αντιμετωπίζονται με τον ίδιο τρόπο. Έτσι, η ομοσπονδιακή ένταση της Διακυβέρνηση δεδομένων διαφέρει ανά τύπο περιεχομένου

Οι παράγοντες του πεδίου εφαρμογής που επηρεάζουν τα ομοσπονδιακά επίπεδα και τις δραστηριότητες είναι

- Μέγεθος επιχείρησης: Προφανώς, οι τεράστιοι οργανισμοί θα πρέπει να ομοσπονδιοποιήσουν τα προγράμματα DG τους και να επιλέξουν προσεκτικά τους κρίσιμους τομείς όπου η DG προσθέτει τη μεγαλύτερη αξία.
- Επωνυμίες: Οι οργανισμοί με ισχυρές εμπορικές επωνυμίες μπορεί να θελήσουν να το λάβουν υπόψη τους κατά την άσκηση οριοθέτησης της Διακυβέρνηση δεδομένων. Ένα εμπορικό σήμα μπορεί να χρειάζεται ένα πιο κεντρικά διαχειριζόμενο χαρτοφυλάκιο δεδομένων από ένα άλλο.
- Τομείς: Ένας τομέας μπορεί να είναι περισσότερο ρυθμιζόμενος και, ως εκ τούτου, να απαιτεί διαφορετική ένταση της Διακυβέρνηση δεδομένων.
- Χώρες: Διάφορα έθνη έχουν διαφορετικούς κανονισμούς και έθιμα, επηρεάζοντας έτσι τον τρόπο με τον οποίο μπορείτε να διαχειριστείτε ορισμένους τύπους πληροφοριών.
- Κατάσταση χαρτοφυλακίου : Όταν ξεκινά μια προσπάθεια Διακυβέρνηση δεδομένων, συνήθως γίνεται κατανοητή σε κάποιο διαισθητικό επίπεδο, η φύση και η κατάσταση του υφιστάμενου χαρτοφυλακίου τεχνολογίας πληροφοριών. Ένας οργανισμός που ξεκινά μια μαζική αναμόρφωση των εφαρμογών (συνήθως μέσω της υλοποίησης μιας μεγάλης εταιρικής σουίτας SAP ή Oracle) θα έχει συγκεκριμένες και συγκεκριμένες απαιτήσεις ομοσπονδιοποίησης Διακυβέρνηση δεδομένων.

- Η ικανότητα ενός οργανισμού να χρησιμοποιεί τις πληροφορίες και τα δεδομένα αναφέρεται ως η ωριμότητα διαχείρισης των πληροφοριών ή ΔΟΠ. Ο τρόπος με τον οποίο ένας οργανισμός κάνει τη δουλειά του ονομάζεται συνήθως κουλτούρα. Σε συνδυασμό, η συγκεκριμένη ΔΟΠ και η κουλτούρα ενός οργανισμού θα επηρεάσουν το πεδίο εφαρμογής και το σχεδιασμό του προγράμματος Διακυβέρνηση δεδομένων. Για παράδειγμα, ένας οργανισμός που έχει άκαμπτο τρόπο σκέψης και χαμηλό επίπεδο ωριμότητας θα απαιτήσει περισσότερο συγκεντρωτικό έλεγχο στο πρόγραμμα Διακυβέρνηση δεδομένων του, καθώς και πιο σημαντικά ζητήματα διαχείρισης αλλαγών.

5.5 Στοιχεία των προγραμμάτων Διακυβέρνησης Δεδομένων

Από πολλές απόψεις, ένα πρόγραμμα διακυβέρνησης δεδομένων μοιάζει με οποιοδήποτε άλλο επιχειρηματικό πρόγραμμα. Πολλά στοιχεία της διακυβέρνησης δεδομένων είναι απολύτως λογικά για τους επιχειρηματίες όταν εξετάζουν για πρώτη φορά τη Διακυβέρνηση δεδομένων. Για κάποιο λόγο, οι άνθρωποι στην τεχνολογική πλευρά της εξίσωσης της διαχείρισης

πληροφοριών και της διακυβέρνησης δεδομένων ζαλίζονται και μπερδεύονται. Όπως και να έχει, η παρούσα ενότητα θα καλύψει αυτά τα βασικά στοιχεία του προγράμματος στο πλαίσιο της Διακυβέρνηση δεδομένων.

5.6 Οργανισμός

Όπως κάθε άλλη δραστηριότητα σε μια εταιρεία ή μια κυβερνητική οντότητα, πρέπει να υπάρχει μια επίσημη δήλωση ρόλων. Ο επίσημος καθορισμός της υπευθυνότητας και της ευθύνης είναι βασικοί παράγοντες για την επιβίωση της Διακυβέρνηση δεδομένων. Το πιο σημαντικό για τα νέα προγράμματα Διακυβέρνηση δεδομένων είναι η έννοια της λογοδοσίας για τα δεδομένα. Αυτός είναι πιθανότατα ένας πολύ νέος ρόλος. Για να είμαστε σαφείς, θα φανεί πολύ νέο και διαφορετικό να θεωρηθεί κάποιος υπεύθυνος για την ποιότητα των δεδομένων, ειδικά όταν η υπευθυνότητα σημαίνει άμεση επίδραση στα μπόνους ή στις προαγωγές. Θα υπάρχει επίσης η αντίληψη ότι το πρόγραμμα της Διακυβέρνηση δεδομένων είναι μάλλον ισχυρό ή τολμηρό για να κάνει αυτούς τους διορισμούς. Η ανάθεση ευθυνών θα είναι επίσης μια σημαντική δραστηριότητα. Σε πολλούς οργανισμούς, τα υπεύθυνα μέρη έχουν επίσημο ρόλο ως καθορισμένοι «διαχειριστές» ή «θεματοφύλακες». Σε άλλες εφαρμογές της Διακυβέρνηση δεδομένων μπορεί να τοποθετούνται όλοι κάτω από την ετικέτα του διαχειριστή και τα υπεύθυνα μέρη θα είναι οι άμεσοι προϊστάμενοι. Όπως και να έχει, μπορείτε να δείτε ότι χρειάζεται κάποιος επίσημος οργανωτικός σχεδιασμός.

Η οργάνωση γύρω από τη Διακυβέρνηση δεδομένων απαιτεί επίσης κάποιου είδους ιεραρχία για να καταστεί δυνατή η επίλυση προβλημάτων, η παρακολούθηση και ο καθορισμός κατευθύνσεων. Σπάνια αυτή η ιεραρχία της Διακυβέρνηση δεδομένων γίνεται ένας αυτόνομος τομέας (δηλαδή, σπάνια υπάρχει ένα «τμήμα» διακυβέρνησης δεδομένων). Τις περισσότερες φορές, η οργάνωση της Διακυβέρνηση δεδομένων είναι ένας εικονικός οργανισμός που αποτελείται από προσωπικό των επιχειρήσεων και της πληροφορικής

Καθώς αναπτύσσετε τη Διακυβέρνηση δεδομένων, θα πρέπει να επανεξετάζετε και να επαναλαμβάνετε τις αρχές σας σε επίπεδο επιχείρησης. Όχι να αναθεωρήσετε, αλλά να επαναλάβετε. Δεδομένου ότι είναι θεμελιώδεις και αντιπροσωπεύουν πεποιθήσεις, η επανάληψη θα είναι απαραίτητη. Στο Σχήμα 3-4 παρατίθενται ορισμένα δείγματα αρχών που έχουμε συλλέξει.

5.7 Εργαλεία και Τεχνολογίες

Το τελευταίο στοιχείο που απαιτεί εξέταση υψηλού επιπέδου είναι η τεχνολογία. Δεν υπάρχει μια ξεκάθαρη κατηγορία ή αγορά για καθαρή τεχνολογία Διακυβέρνηση δεδομένων. Οι περισσότερες προσπάθειες που έχουν καταγραφεί έχουν συγκεντρώσει διάφορες τεχνολογίες για την υποστήριξη της Διακυβέρνησης δεδομένων, χρησιμοποιώντας το SharePoint, το Word και το Excel, καθώς και την προσαρμογή εργαλείων από άλλους κλάδους, όπως εργαλεία μοντέλων δεδομένων ή λεξικών δεδομένων. Τα εξειδικευμένα εργαλεία εξελίσσονται και, σε γενικές γραμμές, θα πρέπει να εξετάσετε τις ακόλουθες δυνατότητες, αλλά το κεφάλαιο 14 θα καλύψει την εφαρμογή των εργαλείων με περισσότερες λεπτομέρειες. Μια πτυχή των εργαλείων που πρέπει να κατανοήσετε σε αυτό το σημείο είναι ότι δεν πρέπει να αισθάνεστε υποχρεωμένοι να αγοράσετε εργαλεία διακυβέρνησης δεδομένων μόνο και μόνο επειδή ασχολείστε με τη διακυβέρνηση δεδομένων. Εξ ορισμού, ένα εργαλείο υπάρχει για να βελτιώσει κάτι που ήδη κάνετε. Εάν δεν εφαρμόζετε ακόμη επίσημη διακυβέρνηση δεδομένων ή εάν την εφαρμόζετε ανεπαρκώς, τότε η αναζήτηση ενός εργαλείου που θα σας βοηθήσει να αναπτύξετε τη Διακυβέρνηση δεδομένων είναι χάσιμο χρόνου. Αυτό έρχεται σε αντίθεση με την τυπική φιλοσοφία της πληροφορικής, όπου το εργαλείο συνήθως αποκτάται πρώτα. Αυτό είναι ένα πασίγνωστο ανόητο πράγμα που πρέπει να κάνετε. Ωστόσο, η δουλειά μας μας βάζει πάντα φρένο σε ένα έργο επιλογής εργαλείων. Είναι εύκολο να αγοράσετε ένα εργαλείο και να το εγκαταστήσετε. Ωστόσο, τις περισσότερες φορές γινόμαστε μάρτυρες νέων εργαλείων για τη διαχείριση δεδομένων που κάθονται αχρησιμοποίητα ή ανεπαρκώς ανεπτυγμένα. Αυτό συμβαίνει επειδή η διαδικασία που υποστηρίζει το εργαλείο δεν έχει γίνει πλήρως κατανοητή.

Ορισμένα χαρακτηριστικά των εργαλείων Διακυβέρνησης δεδομένων που μπορούν να εξεταστούν είναι τα εξής:

- Διαχείριση αρχών και πολιτικών
- Διαχείριση επιχειρηματικών κανόνων και προτύπων
- Διαχείριση οργανισμών
- Ροή εργασιών για θέματα και ελέγχους
- Λεξικό δεδομένων
- Επιχειρησιακή αναζήτηση
- Διαχείριση εγγράφων
- Συγκέντρωση, σύνθεση και παρουσίαση δεδομένων μετρήσεων
- Διασυνδέσεις με άλλες ροές εργασίας και μεθοδολογίες
- Εγκαταστάσεις κατάρτισης και συνεργασίας

5.7.1 Οι ΚΠΕ για τη Διακυβερνηση των Δεδομενων

Συνήθως, οι κρίσιμοι παράγοντες επιτυχίας αφήνονται για το τέλος. Επειδή η Διακυβέρνηση δεδομένων είναι ένα επιχειρηματικό πρόγραμμα από ορισμένες απόψεις, αλλά μοναδικό από άλλες, πρέπει να επισημάνουμε τα ΚΠΕ.

1. Η διακυβέρνηση δεδομένων είναι υποχρεωτική για την επιτυχή υλοποίηση κάθε έργου ή πρωτοβουλίας που χρησιμοποιεί πληροφορίες. Κάθε έργο που απαιτεί αναφορές, επιχειρηματική ευφυΐα, καθαρισμό δεδομένων ή ανάπτυξη μιας «ενιαίας πηγής αλήθειας» απαιτεί Διακυβέρνηση δεδομένων για να είναι βιώσιμο και επιτυχημένο.
2. Η διακυβέρνηση δεδομένων πρέπει να δείχνει ρητά την αξία της. Αυτό σημαίνει ότι δεν μπορείτε να κάνετε διακυβέρνηση δεδομένων στο κενό. Κάτι πρέπει να ρυθμίζεται, ακόμη και αν πρόκειται για την ποιότητα των δεδομένων και εφαρμόζετε τη διακυβέρνηση δεδομένων ως μέσο για τη βελτίωση της ποιότητας των δεδομένων. Αμέτρητα καταστήματα πληροφορικής ανέπτυξαν μοντέλα, πρότυπα και πολιτικές στις δεκαετίες του 1980 και του 1990 και στη συνέχεια έψαχναν για ένα έργο για να τα μεταφέρουν. Πρέπει να δείξετε όφελος, και αυτό σημαίνει ότι πρέπει να συνδέσετε την προσπάθεια της Διακυβέρνησης δεδομένων με μια ορατή πρωτοβουλία.
3. Πρέπει να διαχειριστείτε την αλλαγή της οργανωτικής κουλτούρας. Με τον κίνδυνο να επαναλαμβάνομαι, κάνετε Διακυβέρνηση δεδομένων επειδή ΔΕΝ κάνετε κάτι σωστά. Ως εκ τούτου, κάτι πρέπει να αλλάξει. Έχουμε ασχοληθεί με πολυάριθμους οργανισμούς που ήθελαν να διορθώσουν όλα τα δεδομένα τους, αλλά δεν ήθελαν να αλλάξουν τις απόψεις τους ή τις συμπεριφορές ή τις διαδικασίες που δημιούργησαν το χάος. Επομένως, θα πρέπει να προσανατολίσετε, να εκπαιδεύσετε, να εκπαιδεύσετε, να επικοινωνήσετε, να κρατήσετε το χέρι σας, να ενθαρρύνετε και να προσφέρετε κίνητρα. Στη συνέχεια, να τα επαναλάβετε όλα αυτά ξανά.
4. Η διακυβέρνηση των δεδομένων πρέπει να αντιμετωπίζεται ως μια επιχειρησιακή προσπάθεια. Μπορείτε να την εφαρμόσετε τμηματικά, αλλά πρέπει πάντα να έχει μια επιχειρησιακή προοπτική. Διαφορετικά, θα καταλήξετε με αντικρουόμενα πρότυπα και υπευθυνότητες.

6 Διακυβέρνηση Δεδομένων ως Επιχειρηματικό πρόγραμμα

Η διακυβέρνηση δεδομένων είναι ένα επιχειρηματικό πρόγραμμα- ως εκ τούτου, πρέπει να προσθέτει αξία στην επιχείρηση. Ωστόσο, δεδομένου ότι η διακυβέρνηση δεδομένων είναι ένα πρόγραμμα που ασχολείται με αφηρημένες έννοιες (τα δεδομένα ως περιουσιακό στοιχείο), είναι παρόμοιο με άλλα προγράμματα όπου τα απτά αποτελέσματα είναι δύσκολο να φανούν, όπως το μάρκετινγκ ή τα οικονομικά. Ο Διευθύνων Σύμβουλος θα αναγνωρίσει την ανάγκη για μάρκετινγκ και σίγουρα την ανάγκη για έναν τομέα χρηματοδότησης, αλλά μια λεπτομερής, σκληρή αιτιολόγηση για αυτούς τους τομείς (όπως και για τη Διακυβέρνηση δεδομένω) συνήθως δεν βρίσκεται σε έναν φάκελο κάπου στο γραφείο.

Απαιτείται καν επιχειρηματική μελέτη για τη Διακυβέρνηση Δεδομένων; . Ας υποθέσουμε ότι ο διευθύνων σύμβουλος λέει: «Ξέρω ότι το χρειαζόμαστε πραγματικά αυτό, και είναι όπως το μάρκετινγκ, οπότε προχωρήστε χωρίς επιχειρηματική μελέτη». Θα πρέπει να υπάρχει μια εγγενής κατανόηση ότι η αντιμετώπιση της πληροφορίας ως περιουσιακού στοιχείου οδηγεί σε μια στενά συνδεδεμένη επιχείρηση, επομένως, μια πρόταση αξίας της πληροφορίας δεν είναι αρκετή. Στην πραγματικότητα, απαιτείται επιχειρηματική υπόθεση ακόμη και αν δεν ζητηθεί. Υπάρχουν διάφοροι λόγοι για αυτό:

- Η Διακυβέρνηση Δεδομένων είναι μια ολιστική προσπάθεια που απαιτεί την προσοχή της επιχείρησης. Όμως θα υπάρξουν αρνητές και πρέπει να είστε σε θέση να τους χειριστείτε. Μια συνηθισμένη μορφή αντίστασης είναι να δηλώνει ένας προϊστάμενος τμήματος ότι δεν υπάρχει χρόνος να συμμετάσχει σε μια νέα επιτροπή ή να μάθει νέες διαδικασίες. Εξάλλου, υπάρχει μια επιχείρηση που πρέπει να διευθύνεται. Ωστόσο, γίνεται πιο δύσκολο να προβάλλει κανείς αντίσταση μπροστά σε μια επιχειρηματική υπόθεση που συνδέεται με τον στόχο της παραγωγής εκατοντάδων εκατομμυρίων δολαρίων για τον οργανισμό.

- Η Διακυβέρνηση Δεδομένων δεν θα πετύχει αν δεν μπορεί να μετρηθεί, και τα μέτρα επιτυχίας πρέπει να προέρχονται από ένα σύνολο μετρήσεων με επιχειρηματικό προσανατολισμό.

- Μπορεί να υπάρχει μια de facto επιχειρηματική υπόθεση για τη Διακυβέρνηση Δεδομένων συνδεδεμένη με μια μεγάλη πρωτοβουλία. Μπορεί να υπάρχουν συντριπτικά ζητήματα ποιότητας δεδομένων ή ισχυρή πίεση από τις ρυθμιστικές αρχές. Μπορεί να έχει προγραμματιστεί μια μεγάλη εφαρμογή ενός πακέτου ERP. Η Διακυβέρνηση Δεδομένων γίνεται απαραίτητο μέρος αυτών των έργων, επομένως μπορεί να δρομολογηθεί ως μέρος ενός μεγαλύτερου έργου. Ένα άλλο συνηθισμένο παράδειγμα έχει τη μορφή μιας προσπάθειας για την ποιότητα των δεδομένων. Όλα αυτά τα σενάρια δημιουργούν τον κίνδυνο ανάπτυξης συνόλων παρόμοιων αλλά μη ενιαίων ομάδων Διακυβέρνησης Δεδομένων. Το συμπέρασμα

είναι ότι δεν αποκτάτε ένα βιώσιμο πρόγραμμα. Η Διακυβέρνηση Δεδομένων «αποβλακώνεται» από ένα επιχειρηματικό πρόγραμμα σε ένα επιχειρηματικό ενδιαφέρον που στη συνέχεια περνάει στην ΤΠ όπου γίνεται έργο. Αυτή η εξέλιξη, φυσικά, έρχεται σε άμεση σύγκρουση με την ουσιαστική πτυχή ότι η Διακυβέρνηση Δεδομένων είναι μια επιχειρησιακή προσπάθεια.

- Παραδόξως, υπάρχει ένα άλλο επίμονο εμπόδιο που αντιμετωπίζουν τα προγράμματα DG. Είναι η επιμονή πολλών οργανισμών να αναπτύσσουν μια σκληρή και γρήγορη επιχειρηματική υπόθεση με «πραγματικά» οφέλη και ισχυρές οικονομικές αποδόσεις που βασίζονται σε παραδοσιακά οφέλη όπως η μείωση του προσωπικού ή η μείωση του επιχειρηματικού κόστους. Σε αυτή την περίπτωση, μια επιχειρηματική υπόθεση με απτές αποδόσεις φαίνεται αδύνατη, επειδή τα διαχειριζόμενα δεδομένα και το περιεχόμενο είναι «άυλα». Έτσι, για άλλη μια φορά, η επιχειρηματική υπόθεση υποβαθμίζεται ή κατασκευάζουμε ψεύτικα οφέλη με βάση την τεχνολογική αποτελεσματικότητα. Ωστόσο, σύντομα θα δούμε ότι τα «σκληρά» οφέλη μπορούν να προκύψουν.

6.1 Στόχοι επιχειρηματικής υπόθεσης για τη Διακυβέρνηση Δεδομένων

Προφανώς, η επιχειρηματική υπόθεση για τη Διακυβέρνηση δεδομένων πρέπει να δείξει αξία. Αυτό επιτυγχάνεται με δύο τρόπους. Πρώτον, η αξία παρουσιάζεται με τη μορφή ενός απτού άμεσου οφέλους, όπου μπορείτε να συνδέσετε τη Διακυβέρνηση Δεδομένων με οφέλη που προέρχονται από μία από τρεις κατευθύνσεις:

- Βελτίωση της αποδοτικότητας (π.χ. ολοκλήρωση, ταχύτερη παράδοση πληροφοριών)
- Αύξηση σε άμεσους επιχειρηματικούς συντελεστές, όπως έσοδα, πελάτες ή μερίδιο αγοράς (π.χ. οικονομίες κλίμακας μετά τη συγχώνευση, αποτελεσματικές αλυσίδες εφοδιασμού, αποτελεσματικές προωθητικές ενέργειες)
- Μείωση του κινδύνου, είτε μέσω λιγότερων προστίμων, χαμηλότερων αποθεματικών, απώλειας μεριδίου αγοράς ή μειωμένου κόστους διαχείρισης κινδύνου, όπως τα ασφάλιστρα (π.χ. συμμόρφωση με τον νόμο Sarbanes-Oxley, βελτίωση του απορρήτου των πληροφοριών, βελτίωση της ποιότητας των δεδομένων)

Σε πολλούς οργανισμούς, το ευκολότερο άμεσο όφελος προκύπτει από τη μείωση του κινδύνου. Η εκρηκτική αύξηση των αποθηκευμένων δεδομένων και εγγράφων εδώ και τρεις ή τέσσερις δεκαετίες έχει δημιουργήσει τεράστιες ποσότητες κινδύνου. Μερικά παραδείγματα αυτού του γεγονότος είναι τα εξής:

- Παραβίαση της ιδιωτικής ζωής

- Ασφάλεια δεδομένων
- Αστική ευθύνη που προκαλείται από την κακή διαχείριση πληροφοριών σχετικά με την ασφάλεια ή την εγγύηση
- Λανθασμένες αποφάσεις που προκαλούνται από ανακριβή ή ασυνεπή δεδομένα σε πολυάριθμα αντίγραφα (π.χ. δημιουργία πολύ χαμηλών αποθεμάτων ή απώλεια της παρακολούθησης του τόπου απόκτησης στοιχείων)
- Ρυθμιστική ευθύνη από την αποτυχία παρακολούθησης βασικών εγγράφων ή από την αδυναμία ανταπόκρισης σε αίτημα για έγγραφα
- Υπερβολικό κόστος διατήρησης δεδομένων ROT (περιττά, παρωχημένα και ασήμαντα), συμπεριλαμβανομένων εγγράφων, αντιγράφων ασφαλείας, SharePoint και ηλεκτρονικού ταχυδρομείου

Η δεύτερη μορφή απτής αξίας είναι έμμεση, με τον ίδιο περίπου τρόπο όπως ένα πρόγραμμα μάρκετινγκ (δηλαδή, το πρόγραμμα μάρκετινγκ θα υποστηρίξει άλλες πρωτοβουλίες που διαφορετικά θα αποτύγχαναν ή θα παραπαίουν χωρίς το πρόγραμμα). Στην περίπτωση του μάρκετινγκ, η αξία προσδιορίζεται από την πρόβλεψη και την επιβεβαίωση της αύξησης του μεριδίου αγοράς ή των περισσότερων προοπτικών. Το μάρκετινγκ προσπαθεί να βελτιώσει την προβολή ενός προϊόντος που, για παράδειγμα, υποστηρίζει περισσότερες πωλήσεις. Με παρόμοιο τρόπο, η αξία των έργων πληροφόρησης προκύπτει από το πού χρησιμοποιούνται οι πληροφορίες. Ως εκ τούτου, η επιχειρηματική υπόθεση της Διακυβέρνησης Δεδομένων πρέπει να υποστηρίζει τη δραστηριότητα που διασφαλίζει τη διαθεσιμότητα καλών δεδομένων και πληροφοριών για την επίτευξη των επιχειρησιακών στόχων, χωρίς να αναλαμβάνεται αδικαιολόγητος κίνδυνος ή κόστος. Πρέπει να αναζητήσετε ευκαιρίες όπου η διακυβέρνηση δεδομένων υποστηρίζει επιχειρηματικά προγράμματα που θέλουν να αυξήσουν τα έσοδα, να μειώσουν το κόστος και να μειώσουν τον κίνδυνο. Αφού εντοπίσετε τις ευκαιρίες που θα βοηθήσουν στην επίτευξη των επιχειρηματικών στόχων, τότε είναι καιρός να ποσοτικοποιήσετε συγκεκριμένα τα επιχειρηματικά οφέλη και να τα ευθυγραμμίσετε, λεπτομερώς, με τα δεδομένα και το περιεχόμενο που θα εποπτεύει η διακυβέρνηση δεδομένων.

Ένας άλλος στόχος της επιχειρησιακής υπόθεσης της Διακυβέρνηση Δεδομένων είναι να οικοδομήσει μια απάντηση στις ιστορικές ελλείψεις των έργων τεχνολογίας πληροφοριών. Αυτές είναι οι εξής:

- Η αντίληψη ότι οι πρωτοβουλίες δεδομένων και πληροφοριών αποτυγχάνουν πάντα
- Η αντίληψη ότι οι δαπάνες για «καθαρά» έργα διαχείρισης πληροφοριών είναι σπατάλες
- Η ιστορική κριτική στον τομέα της τεχνολογίας πληροφοριών (ΤΠ)
- Συνεχείς καταγγελίες ότι τα δεδομένα της ΤΠ δεν είναι «σωστά», οπότε οι επιχειρησιακές περιοχές πρέπει να δημιουργήσουν «σωστά» δεδομένα

- Ανάπτυξη της «κρυφής» ή σκιώδους ΤΠ ως αντίδραση στην κακή αντίληψη για την ΤΠ.
- Λίστες έργων που «θα αρχίσουμε να τρέχουμε με αυτές τις ελλείψεις και θα τις διορθώσουμε αργότερα». Φυσικά, το αργότερα δεν συμβαίνει ποτέ.i

Η επιχειρηματική υπόθεση για τη Διακυβέρνηση δεδομένων πρέπει να αντιμετωπίσει αυτές τις απόψεις κατά μέτωπο. Για να ανακεφαλαιώσουμε, η επιχειρηματική υπόθεση της Διακυβέρνηση δεδομένων πρέπει να επιτύχει τα εξής:

- Να προσδιορίσει πού μπορεί να υποστηρίξει άμεσα την επιχείρηση (όπως η αποφυγή κινδύνων).
- Προσδιορισμός των σημείων όπου οι πληροφορίες χρησιμοποιούνται για την προώθηση της επιχείρησης.
- Σύνδεση της Διακυβέρνηση Δεδομένων με τις εν λόγω δραστηριότητες (MDM, BI, κ.λπ.).
- Αντιμετώπιση των ιστορικών ελλείψεων των έργων ΤΠ.

Η επίτευξη αυτών των στόχων θα παράσχει μια πολυδιάστατη επιχειρηματική υπόθεση που θα καταστήσει τη Διακυβέρνηση Δεδομένων ένα βιώσιμο πρόγραμμα.

Εάν τα λεπτομερή, συγκεκριμένα επιχειρηματικά οφέλη δεν μπορούν να ποσοτικοποιηθούν εύκολα, μπορείτε να χρησιμοποιήσετε βιομηχανικά πρότυπα, σημεία αναφοράς και έγγραφα για να παράσχετε τις μετρήσεις για την επιχειρηματική υπόθεση.

6.1.1 Περιεχόμενα της επιχειρηματικής υπόθεσης

Απαιτούνται διάφορα βασικά στοιχεία για την οικοδόμηση μιας επιχειρηματικής υπόθεσης για τη διακυβέρνηση δεδομένων. Επειδή η Διακυβέρνηση Δεδομένων αποτελεί συστατικό στοιχείο της EIM, υπάρχουν ομοιότητες στις δύο επιχειρηματικές περιπτώσεις.

6.1.2 Όραμα

Το όραμα είναι ίσως ο πιο καταχρηστικός όρος στις επιχειρήσεις, αλλά η «μεγάλη εικόνα» είναι απίστευτα σημαντική για την αποδοχή της Διακυβέρνησης Δεδομένων. Να θυμάστε ότι θα πείτε σε ένα μεγάλο μέρος του οργανισμού να αλλάξει. Η αλλαγή δεν συμβαίνει μεταξύ των ανθρώπων χωρίς κάποια άποψη της μεγάλης εικόνας. Στην πραγματικότητα, είναι μάλλον αγένεια να ζητάτε από τους ανθρώπους να αλλάξουν χωρίς κάποιου είδους εξήγηση.

Μία από τις μεγάλες εκπλήξεις κατά την ανάπτυξη της Διακυβέρνησης Δεδομένων συμβαίνει όταν οι επιχειρηματικοί τομείς αρχίζουν να κατανοούν ότι θα υπάρξει νέα υπευθυνότητα για τα δεδομένα. Πολύ συχνά θα εμφανιστεί ένα οξύμωρο. Οι ίδιες επιχειρηματικές μονάδες που επιμένουν στο δικό τους προσωπικό πληροφορικής και διατηρούν δεκάδες παλαιά λογιστικά φύλλα και βάσεις δεδομένων Access.

6.1.3 Κίνδυνοι προγράμματος

Ένα επιχειρηματικό σχέδιο είναι επίσης ένα όχημα για να παρουσιάσει τον τρόπο με τον οποίο ένα εγχείρημα θα διαχειριστεί τον κίνδυνο. Ενώ μέρος της επιχειρηματικής υπόθεσης για τη Διακυβέρνηση δεδομένων θα αφορά τους επιχειρηματικούς κινδύνους, πρέπει επίσης να εξετάσετε τους κινδύνους που μπορεί να δημιουργήσει το ίδιο το πρόγραμμα Διακυβέρνησης Δεδομένων:

1. Επιχειρηματικοί κίνδυνοι: Το πρόγραμμα Διακυβέρνησης Δεδομένων αποτυγχάνει να κάνει το καθήκον του για να αποτρέψει την απώλεια μεριδίου αγοράς και φήμης και αποτυγχάνει να πετύχει τους στόχους ή να αποφύγει την απάτη.
2. Ρυθμιστικοί κίνδυνοι: η Διακυβέρνηση Δεδομένων αποτυγχάνει να συνδεθεί με τις απαιτήσεις συμμόρφωσης και υπάρχουν παραβιάσεις των κανονισμών.
3. Πολιτισμικοί κίνδυνοι: Ο οργανισμός αποτυγχάνει να συμμετάσχει στη διαδικασία Διακυβέρνησης Δεδομένων και συνεχίζει τις κακές πρακτικές διαχείρισης περιουσιακών στοιχείων δεδομένων που οδήγησαν εξαρχής στην ανάγκη για Διακυβέρνηση Δεδομένων.

6.1.4 Επιχειρησιακή ευθυγράμμιση

Εάν το πρόγραμμα Διακυβέρνησης Δεδομένων πρόκειται να υποστηρίξει (άμεσα ή έμμεσα) επιχειρηματικές πρωτοβουλίες, αναφέρετε τα σημεία αξίας ή τα συγκεκριμένα σενάρια που θα επιτρέψει η Διακυβέρνηση δεδομένων. Τα πραγματικά επιχειρηματικά σας οφέλη θα προκύψουν από αυτούς τους τομείς, οπότε μην είστε άτολμοι στην αναζήτηση ευκαιριών.

6.1.5 Κόστος της ποιότητας δεδομένων

Τα ζητήματα ποιότητας δεδομένων καταναλώνουν ένα τεράστιο ποσό κόστους και πόρων. Είναι η πρωταρχική εκδήλωση και μέτρηση ενός λειτουργικού προγράμματος Διακυβέρνησης Δεδομένων. Ως εκ τούτου, είναι σημαντικό η επιχειρηματική σας υπόθεση να αναφέρει το τρέχον κόστος και τους κινδύνους που σχετίζονται με την ποιότητα των δεδομένων.

6.1.6 Κόστος των χαμένων ευκαιριών

Υπάρχει πάντα η ανάγκη να τονιστεί τι θα συμβεί, ή τι θα συνεχίσει να συμβαίνει, χωρίς Διακυβέρνηση Δεδομένων. Μπορεί να καλύπτετε κάποια από αυτά στον τομέα της ποιότητας δεδομένων, αλλά είναι καλό να υπενθυμίζετε τα υφιστάμενα προβλήματα με τα δεδομένα, την υποβολή εκθέσεων, την κακή διαχείριση περιεχομένου, τα τρομακτικά ζητήματα συμμόρφωσης ή το υψηλό κόστος ιδιοκτησίας λόγω του εκτεταμένου πλεονασμού. Ωστόσο, μπορεί να υπάρχουν επιχειρηματικές δράσεις και σενάρια που δεν μπορούν να συμβούν ή μπορεί να είναι πιο δύσκολα χωρίς Διακυβέρνηση Δεδομένων.

6.1.7 Εμπόδια, επιπτώσεις και αλλαγές

Είναι δίκαιο να καλυφθούν πιθανά πολιτιστικά και άλλα οργανωτικά ζητήματα. Εάν υπάρχει η πιθανότητα τεχνολογικών αλλαγών, αυτές μπορούν να αναφερθούν (δεν χρειάζονται λεπτομέρειες, αυτές έρχονται αργότερα). Τυχόν εμπόδια που είναι γνωστά πρέπει να παρουσιαστούν.

Παρουσίαση της υπόθεσης

Η επιχειρηματική υπόθεση για τη Διακυβέρνηση δεδομένων είναι ένα επιχειρηματικό έγγραφο. Ακόμα και αν το έργο αυτό το χειρίζεται ο CIO, πρέπει να αποφύγετε τα ακρωνύμια με τρία γράμματα, την τεχνοκρατική φλυαρία και τις εξωτικές και αφηρημένες εικόνες. Πουλάτε και κάθε πωλητής θα σας πει ότι πρέπει να είστε απόλυτα σαφής και συνοπτικός.

Μερικά θέματα πρέπει να κυριαρχούν στην επιχειρηματική υπόθεση:

- Η Διακυβέρνηση δεδομένων είναι ένα πρόγραμμα. (Ακόμη και αν ο απώτερος στόχος της Διακυβέρνησης Δεδομένων είναι να ενσωματωθεί στην επιχείρηση, εξακολουθεί να είναι προγραμματική στην ανάπτυξη και τη διάρκεια ζωής της). Χρηματοδοτείτε μια

μακροπρόθεσμη, μόνιμη αλλαγή στη νοοτροπία και τη συμπεριφορά, αλλά ο οργανισμός δεν θα ξεκινήσει αυτό το ταξίδι χωρίς κάποια μορφή απόδοσης ή αντιληπτού οφέλους.

- Η Διακυβέρνηση Δεδομένων υποστηρίζει πολλά έργα, αλλά, κυρίως, είναι η λειτουργία ελέγχου και λογιστικού ελέγχου για τη διαχείριση των πληροφοριακών περιουσιακών στοιχείων.
- Η διακυβέρνηση και η αλλαγή είναι υποχρεωτική για την αντιμετώπιση των ζητημάτων που δημιούργησαν την ανάγκη αυτής της συνάντησης. Βεβαιωθείτε ότι αυτά τα ζητήματα και το ιστορικό είναι κατανοητά.
- Στο υψηλότερο επίπεδο, απαιτείται μια σύντομη και περιεκτική παρουσίαση. Η δική μου κατευθυντήρια γραμμή για μια ενημέρωση σε επίπεδο CEO είναι δέκα διαφάνειες ή λιγότερες. Εάν η παρουσίαση γίνει καλά, η ομάδα της Διακυβέρνησης Δεδομένων θα περιμένει εκδήλωση ενδιαφέροντος, δέσμευση για τη συνέχιση και ανατροφοδότηση. Η ανατροφοδότηση πρέπει να αποτελεί αναγνώριση ή διόρθωση των στοιχείων επιχειρηματικής ευθυγράμμισης και να μεταφέρει την κατανόηση των κινδύνων και των επιπτώσεων. Εάν αυτό το προ-περιπτωσιολογικό υλικό παρουσιάζεται σε άτομα χαμηλότερων επιπέδων σε έναν οργανισμό, τότε προσθέστε λεπτομέρειες γύρω από τις επιπτώσεις, τα επιχειρηματικά οφέλη και τους κινδύνους.

6.1.8 Η διαδικασία για τη δημιουργία της περίπτωσης

Ακολουθεί ένα σύντομο περίγραμμα της διαδικασίας για την ανάπτυξη της επιχειρησιακής υπόθεσης για τη Διακυβέρνηση Δεδομένων.

6.1.9 Πλήρης κατανόηση της επιχειρηματικής κατεύθυνσης

Είτε έχετε ρητή πρόσβαση στην εταιρική στρατηγική είτε χρειάζεται να διαβάσετε την ετήσια έκθεση, πρέπει να διαμορφώσετε την επιχειρηματική υπόθεση της Διακυβέρνησης Δεδομένων στο πλαίσιο του οργανισμού σας. Αυτό σημαίνει ότι δεν πρέπει να δεχτείτε μια τυποποιημένη αιτιολόγηση από ένα φυλλάδιο συνεδρίου. Γιατί η Διακυβέρνηση δεδομένων είναι σημαντική για την επιχείρησή σας; Εάν διαμορφώνετε τη Διακυβέρνηση Δεδομένων ως μέρος μιας ευρύτερης προσπάθειας EIM μέσω MDM, BI ή και των δύο, τότε επιβεβαιώστε ότι η ομάδα Διακυβέρνησης Δεδομένων γνωρίζει πού θέλει να πάει η επιχείρηση.

6.1.10 Προσδιορισμός πιθανών ευκαιριών

Η επιχειρηματική στρατηγική γεννά ευκαιρίες πληροφόρησης. Και πάλι, αν υλοποιείται ένα πρόγραμμα EIM, μπορεί να έχετε αυτές τις πληροφορίες πρόχειρες. Ένα συνηθισμένο άμεσο όφελος της διακυβέρνησης είναι στους τομείς e-discovery και της διαχείρισης εγγράφων. Εκεί οι οργανισμοί μειώνουν δραστικά το κόστος και τον κίνδυνο διαχείρισης εγγράφων, εφαρμόζοντας απλώς καλύτερη διακυβέρνηση.

6.1.11 Προσδιορισμός ευκαιριών χρήσης

Τα έμμεσα οφέλη προέρχονται από προσπάθειες όπου οι πληροφορίες χρησιμοποιούνται ως μέσο για την επίτευξη ενός επιχειρηματικού αποτελέσματος, όπως μια αποθήκη δεδομένων. Σε αυτές τις περιπτώσεις, η Διακυβέρνηση Δεδομένων μπορεί να συμβάλει στη διασφάλιση ενός συνεπούς και σχετικού αποτελέσματος. Εάν υπάρχει μια μεγάλη προσπάθεια MDM πελατών που συνδέεται με κάποιο είδος προγράμματος πελατών, τότε η προσπάθεια της Διακυβέρνησης Δεδομένων σας παρέχει την απαιτούμενη διακυβέρνηση στις νέες πολιτικές, πρότυπα και διαδικασίες MDM.

6.1.12 Καθορισμός επιχειρηματικών οφελών και οφελών διαχείρισης κινδύνων

Εξειδικεύστε τα δυνητικά οφέλη όχι μόνο ως προς έναν αντιληπτό αριθμό υψηλού επιπέδου, αλλά και ως προς την αύξηση των ταμειακών ροών ή των κερδών. Επιπλέον, περιγράψτε συγκεκριμένους κινδύνους. Αναζητήστε τους κινδύνους σε όλους τους τρεις τύπους κινδύνωνρυθμιστικούς, αστικούς και χρηματοοικονομικούς.

6.1.13 Επιβεβαίωση

Επιβεβαιώστε τα επιχειρηματικά οφέλη που έχετε εντοπίσει για να διασφαλίσετε ότι υποστηρίζονται από τη Διακυβέρνηση Δεδομένων. Βεβαιωθείτε ότι δεν επιχειρείτε να υποστηρίξετε κάτι που δεν είναι σχετικό.

6.1.14 Ποσοτικοποίηση του κόστους

Εξετάστε το τρέχον κόστος της ΤΠ καθώς και άλλα κόστη που σχετίζονται με τις πληροφορίες. Συμπεριλάβετε όλα τα κόστη κεφαλαίου, τις αποσβέσεις και τα γενικά έξοδα. Οποιαδήποτε ανάλυση του κόστους της κακής ποιότητας των δεδομένων θα πρέπει επίσης να συνυπολογιστεί εδώ. Συμπεριλάβετε το κόστος των τμηματικών βάσεων δεδομένων τελικής χρήσης, των υπολογιστικών φύλλων και των τμηματικών «μίνι τμημάτων πληροφορικής». Αυτός είναι ένας καλός αρχικός αριθμός κόστους. Επισημαίνει πόσα ξοδεύονται τώρα, χωρίς διακυβέρνηση. Το πραγματικό κόστος της διακυβέρνησης θα πρέπει να είναι ένα μικρό κλάσμα του σημερινού κόστους. Ιδανικά, θα χρησιμοποιήσετε εσωτερικούς πόρους. Τις περισσότερες φορές βλέπουμε αρχικά μια μικρή αύξηση του κόστους για κάποιους συμβούλους ή για εκπαίδευση, αλλά καθώς η Διακυβέρνηση δεδομένων γίνεται μέρος της επιχείρησης, το κόστος θα επιστρέψει στα προηγούμενα επίπεδα.

6.1.15 Προσεγγίσεις

Πολλές, αν όχι οι περισσότερες, εταιρείες κάνουν φρικτή δουλειά στη διάδοση των επιχειρηματικών τους σχεδίων, και αυτό προϋποθέτει ότι έχουν πράγματι ένα τέτοιο σχέδιο. Η εταιρεία μου έχει εκτελέσει δεκάδες δεσμεύσεις τύπου EIM τα τελευταία 20 χρόνια. Λίγες από αυτές τις εταιρείες είχαν ένα επιχειρηματικό όραμα ή μια στρατηγική που ήταν άμεσα διαθέσιμη στους ανθρώπους των οποίων η δουλειά ήταν να διασφαλίσουν ότι αυτά τα σχέδια θα μπορούσαν να μετρηθούν. Συχνά η προσπάθεια της EIM προκαλούσε μια αμήχανη αμηχανία σε ένα γραφείο κατά τη διάρκεια μιας συνέντευξης και παρήγαγε ένα στρατηγικό σχέδιο. Οι οργανισμοί που δημοσιοποιούν τις στρατηγικές τους και προωθούν αυτές τις πληροφορίες σε όλα τα επίπεδα τείνουν να έχουν πολύ λιγότερο δύσκολες ανάγκες πληροφόρησης και περιεχομένου. Αυτό δεν είναι σύμπτωση. Εάν οι επιχειρηματικοί οδηγοί και στόχοι είναι ενδημικοί, πόσο δύσκολο είναι πραγματικά να ταιριάξει το χαρτοφυλάκιο εφαρμογών και οι προσπάθειες επιχειρηματικής ευφυΐας με την επιχειρηματική κατεύθυνση;

6.2 Μελέτη Περίπτωσης: Εφαρμογή πλαισίου Διακυβέρνησης Δεδομένων από την Uber

Το WorkflowGuard αποτελεί ένα πρωτοποριακό σύστημα διακυβέρνησης και παρατηρησιμότητας ροών εργασίας, που αναπτύχθηκε από την ομάδα Data Workflow Platform (DWP) της Uber. Η αυξανόμενη ανάγκη για διαχείριση και βελτιστοποίηση των ροών εργασίας οδήγησε στην ανάπτυξη αυτού του συστήματος, το οποίο διαχειρίζεται πάνω από 120.000 ροές εργασίας και εξυπηρετεί περισσότερους από 3.000 χρήστες. Ο βασικός στόχος του

WorkflowGuard είναι η βελτίωση της αξιοπιστίας, της αποδοτικότητας και της εμπειρίας των χρηστών, με ταυτόχρονη μείωση των κοστών υποδομής. [14]

Προκλήσεις

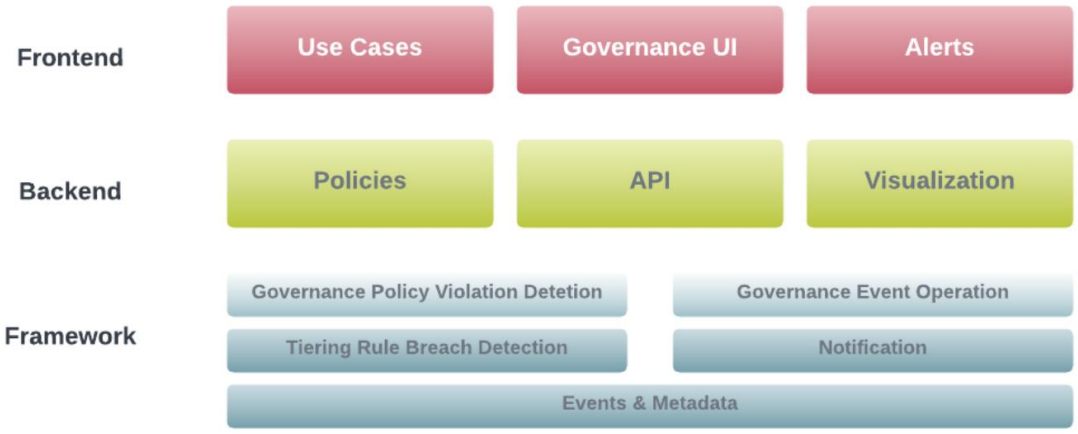
Η Uber αντιμετώπισε πολλές προκλήσεις στη διαχείριση των ροών εργασίας της. Η συνεχής αύξηση του όγκου των δεδομένων και των ροών εργασίας οδήγησε σε αυξημένες απαιτήσεις για πόρους υπολογισμού. Χαρακτηριστικό είναι το παράδειγμα των Presto queries, οι οποίες αυξήθηκαν κατά 4% εβδομαδιαίως το 2021. Επιπλέον, η ταυτόχρονη εκτέλεση πολλών εργασιών προκάλεσε κυκλοφοριακή συμφόρηση και καθυστερήσεις, επηρεάζοντας την απόδοση και την αξιοπιστία του συστήματος. [14]

Λύση: WorkflowGuard

Το WorkflowGuard αναπτύχθηκε για να αντιμετωπίσει αυτές τις προκλήσεις. Το σύστημα παρέχει μηχανισμούς προτεραιοποίησης πόρων, ανακύκλωσης αναποτελεσματικών ροών εργασίας και αυτόματους ελέγχους παραμετροποίησης. Οι ροές εργασίας κατηγοριοποιούνται βάσει της σημασίας τους και προτεραιοποιούνται ανάλογα, επιτρέποντας την απομόνωση των κρίσιμων εκτελέσεων. Το σύστημα επίσης εντοπίζει και ανακυκλώνει ή διαγράφει απαρχαιωμένες ή αναποτελεσματικές ροές εργασίας, αποφεύγοντας την επιβάρυνση των πόρων. [14]

Αρχιτεκτονική του WorkflowGuard

Το WorkflowGuard αποτελείται από πέντε βασικά στοιχεία: τον ανιχνευτή συμβάντων, τον επικυρωτή πολιτικών, τον εκτελεστή διακυβέρνησης, την υπηρεσία ειδοποίησης και την υπηρεσία παρατηρησιμότητας. Ο ανιχνευτής συμβάντων συλλέγει και ανιχνεύει σημαντικά συμβάντα, όπως ενημερώσεις κατάστασης εκτέλεσης και αλλαγές στην κατηγορία. Ο επικυρωτής πολιτικών επικυρώνει τις ροές εργασίας βάσει των καθορισμένων πολιτικών, λαμβάνοντας αποφάσεις σχετικά με την αναστολή, διαγραφή ή υποβάθμιση των ροών. Ο εκτελεστής διακυβέρνησης εφαρμόζει τις αποφάσεις αυτές και ενημερώνει τη βάση δεδομένων των ροών εργασίας. Η υπηρεσία ειδοποίησης ενημερώνει τους χρήστες για αλλαγές κατάστασης μέσω email και άλλων μέσων, ενώ η υπηρεσία παρατηρησιμότητας συλλέγει και αναλύει δεδομένα απόδοσης για την παρακολούθηση των ροών εργασίας. [14]



Εικόνα 8: Αρχιτεκτονική του WorkflowGuard

Ανιχνευτής Συμβάντων:

Ο Ανιχνευτής Συμβάντων συλλέγει δεδομένα σχετικά με την κατάσταση των ροών εργασιών. Αυτά τα δεδομένα περιλαμβάνουν πληροφορίες για την έναρξη, την ολοκλήρωση και τυχόν σφάλματα που προκύπτουν κατά τη διάρκεια της εκτέλεσης των ροών εργασιών. [14]

Επικυρωτής Πολιτικής:

Ο Επικυρωτής Πολιτικής διασφαλίζει ότι οι ροές εργασιών συμμορφώνονται με τους καθορισμένους κανόνες διακυβέρνησης. Ελέγχει τις πολιτικές και αναλαμβάνει δράση σε περίπτωση παραβίασης, όπως η αναστολή ή η τροποποίηση των ροών. [14]

Εκτελεστής Διακυβέρνησης:

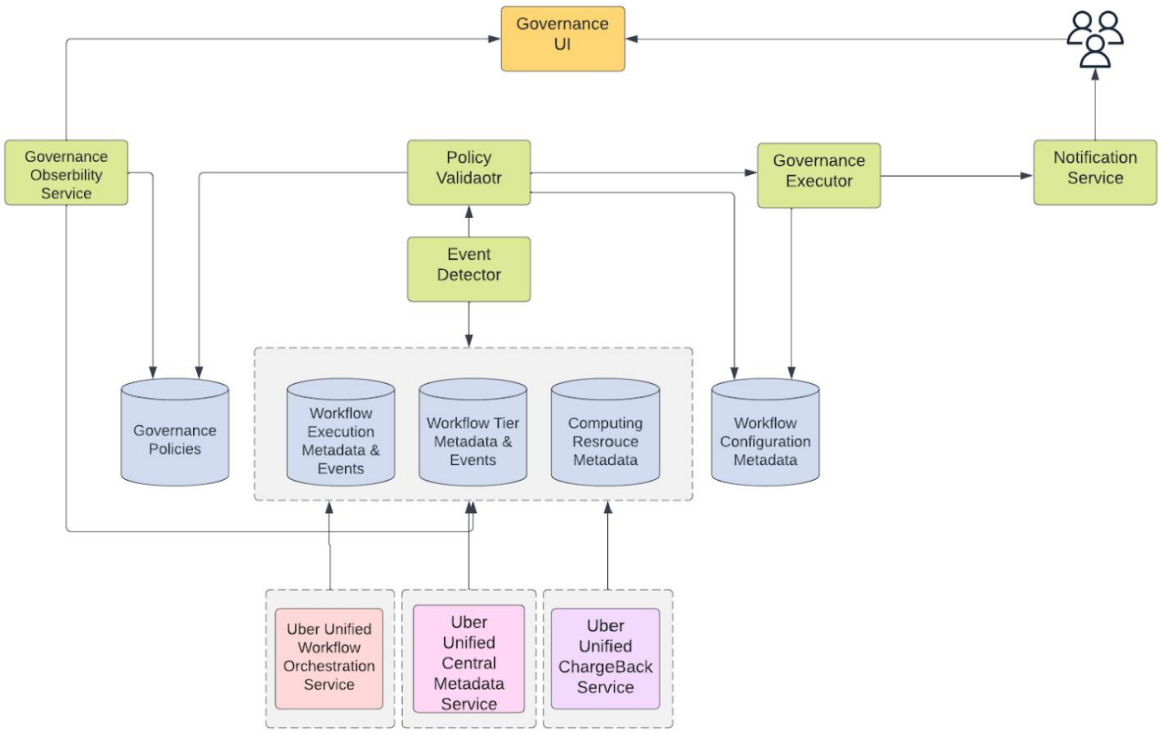
Ο Εκτελεστής Διακυβέρνησης ενημερώνει τις καταστάσεις των ροών εργασιών και επιβάλλει τις αποφάσεις που προκύπτουν από τον Επικυρωτή Πολιτικής. Εφαρμόζει τις εντολές για την τροποποίηση ή τη διακοπή των ροών που δεν συμμορφώνονται με τις πολιτικές. [14]

Υπηρεσία Ειδοποίησης:

Η Υπηρεσία Ειδοποίησης ενημερώνει τους χρήστες για οποιεσδήποτε αλλαγές στην κατάσταση των ροών εργασιών, καθώς και για παραβιάσεις πολιτικής. Οι ειδοποιήσεις αυτές βοηθούν τους διαχειριστές να παραμένουν ενήμεροι και να λαμβάνουν άμεσες δράσεις. [14]

Υπηρεσία Παρατηρησιμότητας:

Η Υπηρεσία Παρατηρησιμότητας παρακολουθεί και οπτικοποιεί τις μετρήσεις των ροών εργασιών. Παρέχει λεπτομερείς αναφορές και γραφικές παραστάσεις που επιτρέπουν στους διαχειριστές να αξιολογούν την απόδοση και τη χρήση πόρων, και να εντοπίζουν περιοχές που χρειάζονται βελτίωση. [14]



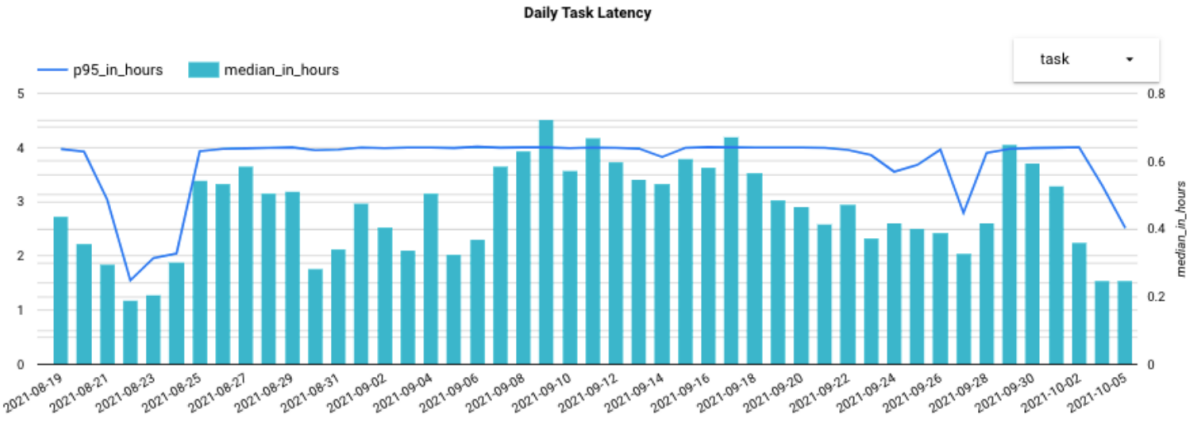
Εικόνα 9: Ροή εργασίας βασικών στοιχείων

Βελτιώσεις Απόδοσης

Η εισαγωγή του WorkflowGuard έφερε σημαντικές βελτιώσεις στην απόδοση του συστήματος. Μέσω της νέας πολιτικής, απενεργοποιήθηκαν πάνω από 9.000 ροές εργασίας Presto, μειώνοντας την εκτέλεση αναποτελεσματικών εργασιών κατά 66%. Το ποσοστό επιτυχίας των εκτελέσεων Presto αυξήθηκε από 69,28% σε 85,22%, ενώ ο συνολικός χρόνος αναμονής μειώθηκε από 40 σε 15 λεπτά. [14]

Εικόνα 10: Γενική εικόνα βαθμού επιτυχίας

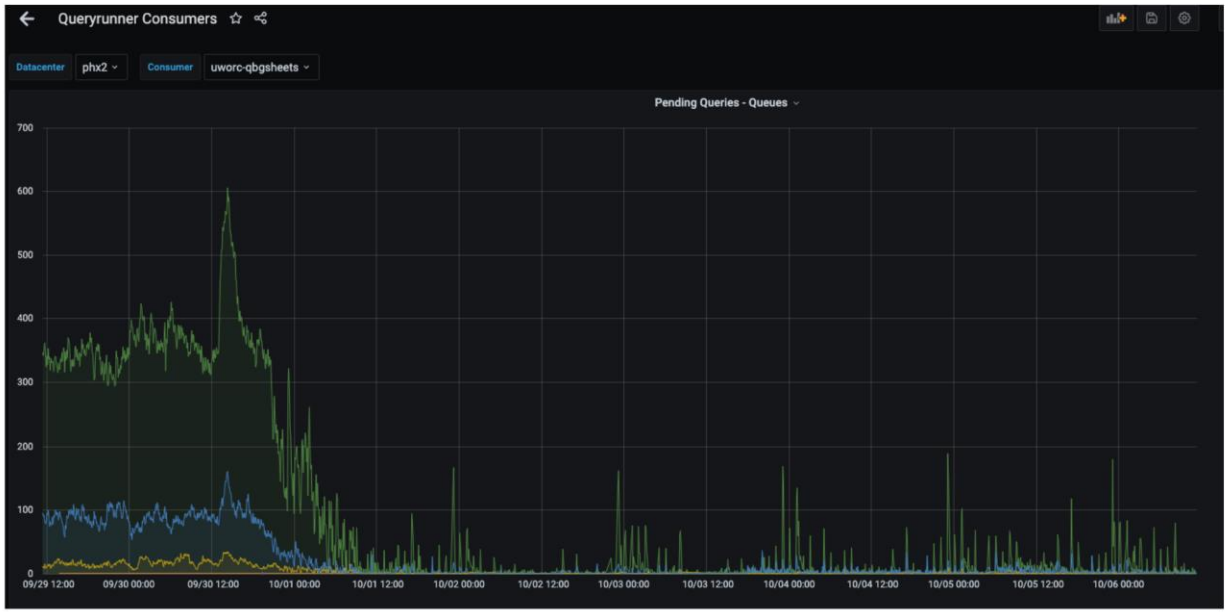
Επιπλέον, το DWP παρατήρησε αύξηση του συνολικού ποσοστού επιτυχίας των εκτελέσεων Presto από 69,28% σε 85,22% (Εικόνα 4). Αυτό συμβαίνει επειδή μια σειρά συνεχόμενων αποτυχημένων εκτελέσεων αποσύρθηκαν με τον καθαρισμό των παλαιών ροών εργασίας, που παλαιότερα μείωναν το συνολικό ποσοστό επιτυχίας. Επιπλέον, η υπολογιστική ισχύς απελευθερώθηκε σημαντικά, μειώνοντας τις πιθανότητες αποτυχίας λόγω υπέρβασης χρόνου.



Εικόνα 11: Γενική εικόνα καθυστέρησης εκτέλεσης εργασιών

Το WorkflowGuard παρέχει μια διαδραστική διεπαφή για τους χρήστες, προσφέροντας πληροφορίες για τις πολιτικές διακυβέρνησης και εργαλεία για τη διόρθωση παραβιάσεων. Οι χρήστες λαμβάνουν ειδοποιήσεις όταν υπάρχει παραβίαση και μπορούν να δουν τις λεπτομέρειες και να την διορθώσουν με ένα κλικ. Οι πίνακες ελέγχου του WorkflowGuard επιτρέπουν στους χρήστες να κατανοήσουν τις ροές εργασίας τους, μειώνοντας την ανάγκη για επικοινωνία. Παρέχουν λεπτομερείς πληροφορίες για την κατανάλωση πόρων, τους χρόνους

εκτέλεσης και άλλες σημαντικές μετρικές, διευκολύνοντας τον εντοπισμό και την επίλυση προβλημάτων.



Εικόνα 12: Συνολικός αριθμός εργασιών στην ουρά εργασιών

Οι ετήσιες εξοικονομήσεις από την υπολογιστική χρήση του Presto από αυτήν την πολιτική ανέρχονται σε περίπου 200.000 δολάρια. [14]

Μελλοντικές Κινήσεις

Η ομάδα της Uber σχεδιάζει να εισαγάγει μοντέλα προώθησης για συμβάντα διακυβέρνησης και να ενεργοποιήσει τον καθαρισμό κατηγοριοποιήσεων για τη διαχείριση ροών εργασίας και δεδομένων που έχουν φτάσει στο τέλος της ζωής τους.

Συμπεράσματα

Το WorkflowGuard βελτίωσε σημαντικά την αξιοπιστία, την αποδοτικότητα κόστους και την παρατηρησιμότητα των ροών εργασίας στην Uber. Επέτρεψε την αναστολή αναποτελεσματικών ροών, την ανακύκλωση πόρων υπολογισμού και την προτεραιοποίηση κρίσιμων εκτελέσεων, προσφέροντας μια καλύτερη εμπειρία στους χρήστες. Η επιτυχία του WorkflowGuard αποδεικνύεται από τις σημαντικές βελτιώσεις στην απόδοση και τη μείωση των καθυστερήσεων εκτέλεσης των εργασιών, καθιστώντας το ένα απαραίτητο εργαλείο για τη διαχείριση των δεδομένων και των πόρων στην Uber.

6.3 Σύνοψη

Ακόμη και αν ένας επιχειρηματικός ηγέτης επισημαίνει ξεκάθαρα την ανάγκη για «καλύτερα δεδομένα» και είναι πρόθυμος να πιέσει σκληρά και να χρησιμοποιήσει πολιτικό κεφάλαιο για να τα αποκτήσει, δεν προχωράτε χωρίς επιχειρηματική υπόθεση, διαφορετικά κινδυνεύετε να πέσετε στον κάδο απορριμμάτων των αποτυχημένων πρωτοβουλιών. Επομένως, υπάρχουν και κάποιες επιχειρηματικές εκτιμήσεις για την επιχειρηματική υπόθεση:

1. Η επιχειρηματική υπόθεση πρέπει να χαρακτηρίζεται από λογοδοσία. Εάν οι στόχοι δεν επιτευχθούν, ποιος είναι υπεύθυνος; Ιστορικά, ήταν πολύ εύκολο να επιρρίψετε την ευθύνη στην ΤΠ για την αποτυχία της επικοινωνίας. Μια σαφής επιχειρηματική υπόθεση θα χρησιμοποιεί επιχειρηματική ορολογία και θα επισημαίνει πού βρίσκεται η επιχειρηματική ευθύνη.
2. Οι ηγέτες των επιχειρήσεων έχουν ελάχιστα κίνητρα για να τα πάνε καλά σε έργα σχετικά με τις πληροφοριες. Η επιχειρηματική υπόθεση για τη Διακυβέρνηση δεδομένων πρέπει να υποστηρίζει την επιχειρηματική λογοδοσία και να ενσωματώνεται στους στόχους και τους προσωπικούς στόχους των χορηγών.
3. Μόλις ολοκληρωθούν τα έργα πληροφορικής, υπάρχει η τάση να μειώνεται το ενδιαφέρον, ακόμη και να επιστρέφεται στην παλιά εναλλακτική λύση. Οι επιχειρηματικοί τομείς πρέπει να κατανοήσουν ότι η επένδυση συνεχίζεται και μετά την ανάπτυξη και απαιτείται κάποια προσπάθεια και θέληση για τη διατήρηση των στόχων του έργου. Η επιχειρηματική υπόθεση πρέπει να αναγνωρίζει τον πολιτισμικό αντίκτυπο και να προσαρμόζει ακόμη και το κόστος και τα οφέλη της διατήρησης της προσπάθειας, διασφαλίζοντας παράλληλα ότι οι αλλαγές υιοθετούνται πλήρως και ενσωματώνονται στον ιστό της κουλτούρας.

Η ομάδα της Διακυβέρνησης Δεδομένων πρέπει να θυμάται ότι πρέπει να υπάρχει ένα είδος διαδικασίας πώλησης, ακόμη και αν δεν έχει ζητηθεί κάτι τέτοιο. Ένας χορηγός δεν κάνει ένα επιτυχημένο πρόγραμμα. Αυτό σημαίνει εξέταση των επιχειρηματικών ευκαιριών, εκπαίδευση σχετικά με τις επιπτώσεις της διαχείρισης των πληροφοριών ως περιουσιακό στοιχείο και αναγνώριση ότι η μακροχρόνια εχθρότητα μεταξύ του IT και των επιχειρηματικών τομέων πρέπει να αντιμετωπιστεί με ένα επιχειρηματικό πρόγραμμα. Μην ξεχνάτε ότι υπάρχουν αμφισβητίες και αρνητές εκεί έξω. Η παράθεση μιας υπόθεσης με σκληρά δολάρια θα επιβραδύνει την πρώιμη αντίσταση.

7 Συμπεράσματα

Η κυβερνοασφάλεια και η διακυβέρνηση δεδομένων έχουν αποδειχθεί ζωτικής σημασίας για την ασφαλή και αποτελεσματική λειτουργία των σύγχρονων ψηφιακών κοινωνιών και επιχειρήσεων. Η εργασία αυτή ανέδειξε μέσω εκτεταμένης ανάλυσης πώς οι εξελίξεις στις ψηφιακές τεχνολογίες και οι αλλαγές στο κανονιστικό περιβάλλον, όπως ο GDPR, έχουν επηρεάσει την προσέγγιση των οργανισμών προς την κυβερνοασφάλεια και τη διαχείριση των δεδομένων τους.

7.1 Τεχνολογική Εξέλιξη και Ασφάλεια Δεδομένων

Οι τεχνολογικές καινοτομίες, όπως η τεχνητή νοημοσύνη, το blockchain και το Internet of Things, ανοίγουν νέους δρόμους για την αυτοματοποίηση, την ανάλυση δεδομένων και τη βελτιωμένη επικοινωνία. Ωστόσο, αυτές οι ίδιες καινοτομίες αυξάνουν επίσης την ευπάθεια των συστημάτων σε κυβερνοεπιθέσεις και διαρροές δεδομένων. Η προστασία αυτών των τεχνολογικών υποδομών απαιτεί μια συνεχώς εξελισσόμενη στρατηγική κυβερνοασφάλειας που συνδυάζει τόσο τεχνολογικές όσο και οργανωτικές προσεγγίσεις.

7.2 Κανονιστικό Πλαίσιο και Συμμόρφωση

Ο GDPR και άλλες σχετικές νομοθεσίες έχουν αναδειχθεί ως καίρια εργαλεία για τη διασφάλιση ότι οι οργανισμοί διαχειρίζονται τα δεδομένα με τρόπο που σέβεται την ιδιωτικότητα και την ασφάλεια των χρηστών. Η εφαρμογή αυτών των κανονισμών έχει οδηγήσει σε αυξημένη διαφάνεια και έχει βελτιώσει τη δημόσια εμπιστοσύνη, προσφέροντας στους χρήστες καλύτερο έλεγχο των προσωπικών τους δεδομένων. Παράλληλα, αυτή η συμμόρφωση έχει παράσχει στις επιχειρήσεις ένα καθαρό πλαίσιο για το πώς πρέπει να διαχειρίζονται τις πληροφορίες, αυξάνοντας την ασφάλεια και μειώνοντας τις νομικές αβεβαιότητες.

7.3 Στρατηγικές Αντιμετώπισης και Πρόληψης

Οι διαρκώς αυξανόμενες κυβερνοαπειλές απαιτούν από τις επιχειρήσεις να εφαρμόζουν στρατηγικές που όχι μόνο αντιμετωπίζουν τις επιθέσεις όταν συμβούν, αλλά και προλαμβάνουν την εμφάνισή τους. Εκπαιδεύσεις περί κυβερνοασφάλειας, ισχυρές πολιτικές πρόσβασης και τεχνολογίες ανίχνευσης απειλών είναι ζωτικής σημασίας. Επιπρόσθετα, η διαρκής αναθεώρηση

και ενημέρωση των κυβερνητικών πρακτικών, η ενσωμάτωση τεχνολογικών καινοτομιών στα συστήματα ασφάλειας, και η συνεργασία με άλλους οργανισμούς και τις κυβερνήσεις, αναδεικνύονται ως κρίσιμα στοιχεία για την ενίσχυση της ψηφιακής ασφάλειας.

7.4 Μελλοντικές Προοπτικές

Η εξέλιξη των ψηφιακών τεχνολογιών και των κανονιστικών πλαισίων θα συνεχίσει να προκαλεί νέες προκλήσεις στην κυβερνοασφάλεια και τη διακυβέρνηση δεδομένων. Η δυναμική αντίδραση σε αυτές τις προκλήσεις, μέσω της διαρκούς ενημέρωσης, της τεχνολογικής προσαρμογής και της ενδυνάμωσης των πολιτικών και των διαδικασιών, θα καθορίσει την ικανότητα των οργανισμών να διατηρούν υψηλά επίπεδα ασφάλειας. Το μέλλον της κυβερνοασφάλειας και της διακυβέρνησης δεδομένων επιβάλλει μια ολιστική προσέγγιση, η οποία ενσωματώνει την καινοτομία, τη συμμόρφωση και τη διαρκή βελτίωση των τεχνολογικών και διαδικαστικών μηχανισμών ασφαλείας.

8 Βιβλιογραφία

8.1 Βιβλιογραφία

[1] Chunlei Tang, The Data Industry: The Business and Economics of Information and Big Data, 1st ed. Wiley, 2016.

[2] John Ladley, Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program, 1st ed. Morgan Kaufmann, 2012.

[3] Peter K. Ghavami, Big Data Governance: Modern Data Management Principles for Hadoop, NoSQL & Big Data Analytics, 1st ed. CreateSpace Independent Publishing Platform, 2016.

[4] Alex Gorelik, The Enterprise Big Data Lake: Delivering the Promise of Big Data and Data Science, 1st ed. O'Reilly Media, 2019.

[5] Bernard Marr, Big Data in Practice: How 45 Successful Companies Used Big Data Analytics to Deliver Extraordinary Results, 1st ed. Wiley, 2016.

[6] Alan Calder and Steve Watkins, IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002, 4th ed. Kogan Page, 2008.

[7] Evren Eryurek, Uri Gilad, Valliappa Lakshmanan, Anita Ibunguchy, and Jessi Ashdown, Data Governance: The Definitive Guide: People, Processes, and Tools to Operationalize Data Trustworthiness, 1st ed. O'Reilly Media, 2021.

[8] Mary Anne Hopper, Practitioner’s Guide to Operationalizing Data Governance, 1st ed. Technics Publications, 2023.

[9] Sunil Soares, Data Governance Tools: Evaluation Criteria, Big Data Governance, and Alignment with Enterprise Data Management, 1st ed. Technics Publications, 2014.

[10] Sunil Soares, The Chief Data Officer Handbook for Data Governance, 1st ed. Technics Publications, 2014.

[11] Steve Winterfeld and Jason Andress, The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice, 1st ed. Syngress, 2013.

[12] Elias G. Carayannis, David F.J. Campbell, and Marios Panagiotis Efthymiopoulos, Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice, 1st ed. Springer, 2014.

8.2 Παραπομπές

[13] Deloitte, "Cybersecurity," [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/gr/Documents/risk/gr_SEV_Deloitte_Cybersecurity_noexp.pdf.

[14] Uber, "Introducing WorkflowGuard," [Online]. Available: https://www.uber.com/en-GR/blog/introducing-workflowguard/.