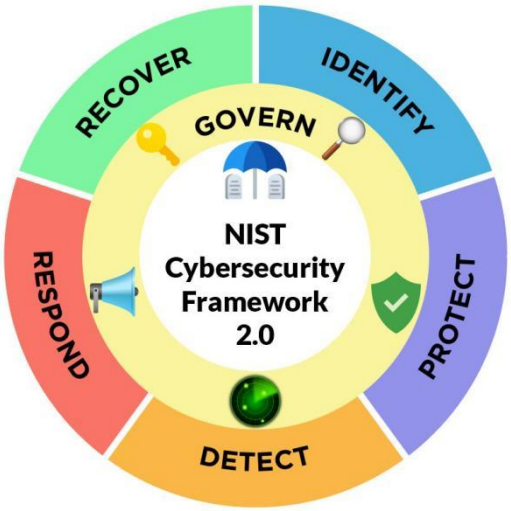
ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

« Εφαρμογή του NIST Cybersecurity framework 2.0 σε δημόσιους οργανισμούς »



Του φοιτητή
Πασχάλη Κωνσταντά
Αρ. Μητρώου: 144308

Επιβλέπων
Ονοματεπώνυμο: Χρήστος Ηλιούδης
Βαθμίδα: Καθηγητής

Ημερομηνία 10/9/2024

Τίτλος Δ.Ε.: Εφαρμογή του NIST Cybersecurity framework 2.0 σε δημόσιους οργανισμούς

Κωδικός Δ.Ε. 24167

Ονοματεπώνυμο φοιτητή: Πασχάλης Κωνσταντάς

Ονοματεπώνυμο εισηγητή: Χρήστος Ηλιούδης

Ημερομηνία ανάληψης Δ.Ε. 27/03/2024

Ημερομηνία περάτωσης Δ.Ε.: 10/09/2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

« Αφιερώνω αυτήν την εργασία στους γονείς μου, για την αμέριστη στήριξή τους, στην αγαπημένη μου, για την αγάπη και την ενθάρρυνσή της, και στους καθηγητές μου, για την πολύτιμη καθοδήγηση και έμπνευσή τους. »

Πρόλογος

Αποτελεί γεγονός πως, η ψηφιακή εποχή έχει εδραιώσει την κυβερνοασφάλεια κρίσιμη για τους οργανισμούς, εξαιτίας της ολοένα και μεγαλύτερης αύξησης των τεχνολογιών πληροφορικής. Το NIST Cybersecurity Framework (CSF) 2.0, το οποίο έχει αναπτυχθεί από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ, είναι πλέον από τα πιο διαδεδομένα και αναγνωρισμένα εργαλεία, για τη διαχείριση κινδύνων στην κυβερνοασφάλεια. Μπορεί να ειπωθεί, ότι προσφέρει μια μέθοδο για την αναγνώριση απειλών, για την προστασία, την ανίχνευση περιστατικών, και την αποκατάσταση των λειτουργιών μετά από επιθέσεις.

Η συγκεκριμένη εργασία μελετά την εφαρμογή του NIST CSF 2.0 σε δημόσιους οργανισμούς στην Ελλάδα, επικεντρώνοντας το ενδιαφέρον στα θετικά στοιχεία και τις μελλοντικές προοπτικές. Πιο συγκεκριμένα μελετά το πώς το πλαίσιο μπορεί να συμβάλει στη βελτίωση της κυβερνοασφάλειας, συγκρίνοντάς το με άλλες οδηγίες όπως το NIS 2 της Ευρωπαϊκής Ένωσης. Μέσα από μια μελέτη περίπτωσης, η εργασία αναδεικνύει τα πρακτικά οφέλη και τις δυσκολίες της εφαρμογής του σε έναν συγκεκριμένο ελληνικό δημόσιο οργανισμό. Τέλος, διατυπώνονται συμπεράσματα και προτάσεις για τη βελτίωση του πλαισίου, ώστε να ανταποκριθεί στις μελλοντικές προκλήσεις της κυβερνοασφάλειας στον δημόσιο τομέα της Ελλάδας.

Περίληψη

Η ψηφιακή εποχή έχει οδηγήσει σε αυξανόμενη εξάρτηση από τα πληροφοριακά συστήματα, καθιστώντας την κυβερνοασφάλεια ένα κρίσιμο ζήτημα για τους οργανισμούς, ιδιαίτερα στον δημόσιο τομέα. Η ανάγκη για ολοκληρωμένα πλαίσια διαχείρισης των κινδύνων κυβερνοασφάλειας έχει αναδειχθεί ως προτεραιότητα για τη διασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δεδομένων. Σε αυτό το πλαίσιο, το NIST Cybersecurity Framework (CSF) 2.0, που αναπτύχθηκε από το National Institute of Standards and Technology (NIST) των ΗΠΑ, προτείνεται ως ένα από τα πιο αξιόπιστα και ευρέως αναγνωρισμένα πλαίσια διαχείρισης της κυβερνοασφάλειας. Το πλαίσιο αυτό παρέχει μια δομημένη μεθοδολογία και εργαλεία που μπορούν να βοηθήσουν τους οργανισμούς να αντιμετωπίσουν τις σύγχρονες προκλήσεις της κυβερνοασφάλειας.

Η παρούσα πτυχιακή εργασία εξετάζει την εφαρμογή του NIST CSF 2.0 στους δημόσιους οργανισμούς της Ελλάδας. Αναλύει το πρόβλημα της κυβερνοασφάλειας στο δημόσιο τομέα, τους κινδύνους που αντιμετωπίζουν οι οργανισμοί και την ανάγκη για υιοθέτηση ενός ολοκληρωμένου πλαισίου διαχείρισης της ασφάλειας. Μέσα από την ανάλυση της ελληνικής πραγματικότητας, την παρουσίαση και τη σύγκριση του NIST CSF 2.0 με άλλες σχετικές οδηγίες, όπως το NIS 2 της Ευρωπαϊκής Ένωσης, και τη μελέτη περίπτωσης ενός συγκεκριμένου ελληνικού δημόσιου οργανισμού, η εργασία εξετάζει τις δυνατότητες, τα οφέλη και τις προκλήσεις που σχετίζονται με την εφαρμογή αυτού του πλαισίου.

Η μελέτη περίπτωσης εστιάζει στην εφαρμογή του NIST CSF 2.0 σε έναν ελληνικό δημόσιο οργανισμό και εξετάζει πρακτικά ζητήματα, όπως η προσαρμογή του πλαισίου στις ανάγκες του οργανισμού, οι προκλήσεις που αντιμετωπίστηκαν και τα οφέλη που προέκυψαν από την υιοθέτησή του. Η εργασία καταλήγει σε συμπεράσματα και προτάσεις για μελλοντικές επεκτάσεις, με στόχο τη βελτίωση της κυβερνοασφάλειας στον δημόσιο τομέα της Ελλάδας και την ενίσχυση της ανθεκτικότητας των δημόσιων οργανισμών στις κυβερνοαπειλές.

« Applying the NIST Cybersecurity framework 2.0 to public organizations »

« Paschalis Konstantas »

Abstract

The digital era has led to an increasing dependence on information systems, making cybersecurity a critical issue for organizations, especially in the public sector. The need for comprehensive frameworks to manage cybersecurity risks has emerged as a priority to ensure the integrity, availability, and confidentiality of data. In this context, the NIST Cybersecurity Framework (CSF) 2.0, developed by the National Institute of Standards and Technology (NIST) in the United States, is proposed as one of the most reliable and widely recognized cybersecurity management frameworks. This framework provides a structured methodology and tools that can help organizations address modern cybersecurity challenges.

This thesis examines the implementation of NIST CSF 2.0 in public organizations in Greece. It analyzes the problem of cybersecurity in the public sector, the risks faced by organizations, and the need to adopt a comprehensive security management framework. Through an analysis of the Greek cybersecurity landscape, a presentation and comparison of NIST CSF 2.0 with other relevant directives, such as the NIS 2 Directive of the European Union, and a case study of a specific Greek public organization, this thesis explores the possibilities, benefits, and challenges associated with the framework's implementation.

The case study focuses on the application of NIST CSF 2.0 in a Greek public organization and examines practical issues such as adapting the framework to the organization's needs, the challenges encountered, and the benefits that emerged from its adoption. The thesis concludes with findings and suggestions for future extensions, aiming to improve cybersecurity in Greece's public sector and enhance the resilience of public organizations against cyber threats.

Ευχαριστίες

Θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στους γονείς μου, για την αμέριστη στήριξη και αγάπη τους, που μου έδωσαν τη δύναμη να ολοκληρώσω αυτήν την εργασία. Επίσης, ένα μεγάλο ευχαριστώ στην αγαπημένη μου, για την υπομονή, την κατανόηση και την ενθάρρυνση που μου προσέφερε σε κάθε στάδιο της διαδικασίας.

Ευχαριστώ ιδιαίτερα τους καθηγητές μου για την πολύτιμη καθοδήγησή τους και τις γνώσεις που μου μετέδωσαν. Η συμβολή τους υπήρξε καθοριστική στην ολοκλήρωση αυτής της διπλωματικής εργασίας. Τέλος, ευχαριστώ όλους τους φίλους και συμφοιτητές μου για την ηθική υποστήριξη και τη βοήθειά τους κατά τη διάρκεια αυτής της πορείας.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συντομογραφίες

A.I.	Artificial Intelligence
C.OB.I.T.	Control Objectives for Information Technology
C.S.F.	Cybersecurity Framework
C.S.I.R.T.	Computer Security Incident Response Team
DE	Detect
GV	Govern
GV.OC	Organizational Context
GV.RM	Risk Management strategy
ID	Identify
I.o.t.	Internet of Things
M.F.A.	Multi Factor Authentication
N.I.S.	Network and Information Security
NIST	National Institute of Standards and Technology
PR	Protect
RC	Recover
RS	Respond
Z.T.A.	Zero Trust Architecture
Δ.Ε.	Διπλωματική Εργασία
ΔΙ.ΠΑ.Ε.	Διεθνές Πανεπιστήμιο Ελλάδος
Ε.Ε.	Ευρωπαϊκή Ένωση
Μ.Μ.Ε.	Μικρομεσαίες επιχειρήσεις
Ο.ΔΙ.Π.Σ.Ε.	Οργανισμός Διαχείρισης Πληροφοριακών Συστημάτων Ελλάδας

Κεφάλαιο 1ο: Η ερευνητική περιοχή της εργασίας

1.1 Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο αποτελεί έναν από τους σημαντικότερους τομείς προστασίας και διαχείρισης κινδύνων στους δημόσιους οργανισμούς, ιδίως σήμερα που η ψηφιακή τεχνολογία διαδραματίζει κεντρικό ρόλο σε όλες τις πτυχές των λειτουργιών. Οι δημόσιοι οργανισμοί διαχειρίζονται κρίσιμες πληροφορίες και δεδομένα πολιτών που είναι απαραίτητα για τη λήψη αποφάσεων, την παροχή υπηρεσιών και τη δημόσια ασφάλεια. Είναι ζωτικής σημασίας η προστασία αυτών των πληροφοριών από απειλές όπως οι επιθέσεις στον κυβερνοχώρο και οι παραβιάσεις δεδομένων. Το Πλαίσιο Κυβερνοασφάλειας NIST (CSF) είναι ένα πλαίσιο για τη διαχείριση κινδύνων και την ασφάλεια των πληροφοριακών συστημάτων που αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) στις ΗΠΑ. Παρέχει κατευθυντήριες γραμμές για την ασφάλεια. Το πλαίσιο σχεδιάστηκε αρχικά για τον ιδιωτικό τομέα, αλλά η ευελιξία και η προσαρμοστικότητά του το καθιστούν ιδανικό για τον δημόσιο τομέα (Pawlak et al., 2020).

Δεδομένου του αυξανόμενου αριθμού και της σοβαρότητας των επιθέσεων στον κυβερνοχώρο, η ανάγκη για μια στρατηγική και ολοκληρωμένη προσέγγιση της ασφάλειας στον κυβερνοχώρο γίνεται ακόμη πιο εμφανής. Οι δημόσιοι οργανισμοί αντιμετωπίζουν πολλές προκλήσεις στις προσπάθειές τους για την προστασία των δεδομένων, συμπεριλαμβανομένων των περιορισμένων πόρων, της έλλειψης εξειδικευμένου προσωπικού και της ανάγκης συμμόρφωσης με ένα συνεχώς εξελισσόμενο κανονιστικό πλαίσιο. Η συγκεκριμένη εργασία εξετάζει τον τρόπο με τον οποίο το NIST CSF 2.0 μπορεί να εφαρμοστεί αποτελεσματικά στους ελληνικούς δημόσιους οργανισμούς για την ενίσχυση της ανθεκτικότητάς τους απέναντι στις απειλές για την ασφάλεια στον κυβερνοχώρο. Περιλαμβάνει λεπτομερή ανάλυση των βασικών στοιχείων και λειτουργιών του πλαισίου, καθώς και συγκριτική ανάλυση με άλλες διεθνείς και ευρωπαϊκές προσεγγίσεις, όπως το NIS 2.0.

1.2 Στόχος της πτυχιακής εργασίας

Ο κύριος στόχος του παρόντος πονήματος είναι να αναλύσει και να αξιολογήσει την εφαρμογή του Πλαισίου Κυβερνοασφάλειας 2.0 του NIST σε ελληνικούς δημόσιους φορείς. Ειδικότερα, η εργασία αποσκοπεί σε:

- Παρουσίαση NIST Cybersecurity Framework 2.0: Παροχή μιας ολοκληρωμένης παρουσίασης των αρχών, των κατηγοριών και των λειτουργιών αυτού του πλαισίου και του τρόπου με τον οποίο μπορεί να βοηθήσει τους οργανισμούς να βελτιώσουν την κυβερνοασφάλειά τους.
- Σύγκριση με το NIS 2: Προσδιορίζει τις διαφορές και τις ομοιότητες συγκρίνοντας το NIST CSF 2.0 με την NIS 2 (Network and Information Systems Directive), τη δεύτερη έκδοση της οδηγίας της Ευρωπαϊκής Ένωσης για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Πρέπει να διευκρινιστεί.
- Ανάλυση Η πραγματικότητα στην Ελλάδα: εξετάζει την τρέχουσα κατάσταση της ασφάλειας στον κυβερνοχώρο στην Ελλάδα μέσω της ανάλυσης των υφιστάμενων πολιτικών και των σχετικών εγγράφων.
- Μελέτες περιπτώσεων: Αναλύει συγκεκριμένες εφαρμογές του NIST CSF 2.0 σε ελληνικούς δημόσιους φορείς και προσδιορίζει τις προκλήσεις, τις δυσκολίες και τα οφέλη που σχετίζονται με την εφαρμογή του εν λόγω πλαισίου.
- Συμπεράσματα και συστάσεις: Συνοψίζει τα κύρια ευρήματα της μελέτης και παρέχει συστάσεις για βελτιώσεις και μελλοντικές κατευθύνσεις για την περαιτέρω ανάπτυξη της κυβερνοασφάλειας σε δημόσιους οργανισμούς.

1.3 Δομή της μελέτης

Η μελέτη είναι δομημένη ως εξής:

- Εισαγωγή: Παρουσιάζεται το πρόβλημα που επιλύει η παρούσα εργασία, οι στόχοι και η δομή της.
- Παρουσιάσεις:

- Εισαγωγή στο NIST Cybersecurity Framework 2.0: αναλύονται τα βασικά στοιχεία και οι λειτουργίες του εν λόγω πλαισίου.
- Εισαγωγή στο NIS 2: Περιγράφεται η δεύτερη έκδοση της οδηγίας της Ευρωπαϊκής Ένωσης για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών.
  - Ελληνική πραγματικότητα: Αναλύεται η τρέχουσα κατάσταση της ασφάλειας στον κυβερνοχώρο στην Ελλάδα και οι τρέχουσες πολιτικές.
  - Μελέτη περίπτωσης: Παρουσιάζεται μια συγκεκριμένη εφαρμογή του NIST CSF 2.0 σε έναν ελληνικό δημόσιο οργανισμό.
  - Συμπεράσματα και μελλοντικές επεκτάσεις: Συνοψίζονται τα ευρήματα και προτείνονται βελτιώσεις και μελλοντικές κατευθύνσεις για την περαιτέρω ενίσχυση της ασφάλειας στον κυβερνοχώρο.

Κεφάλαιο 2ο: Παρουσιάσεις

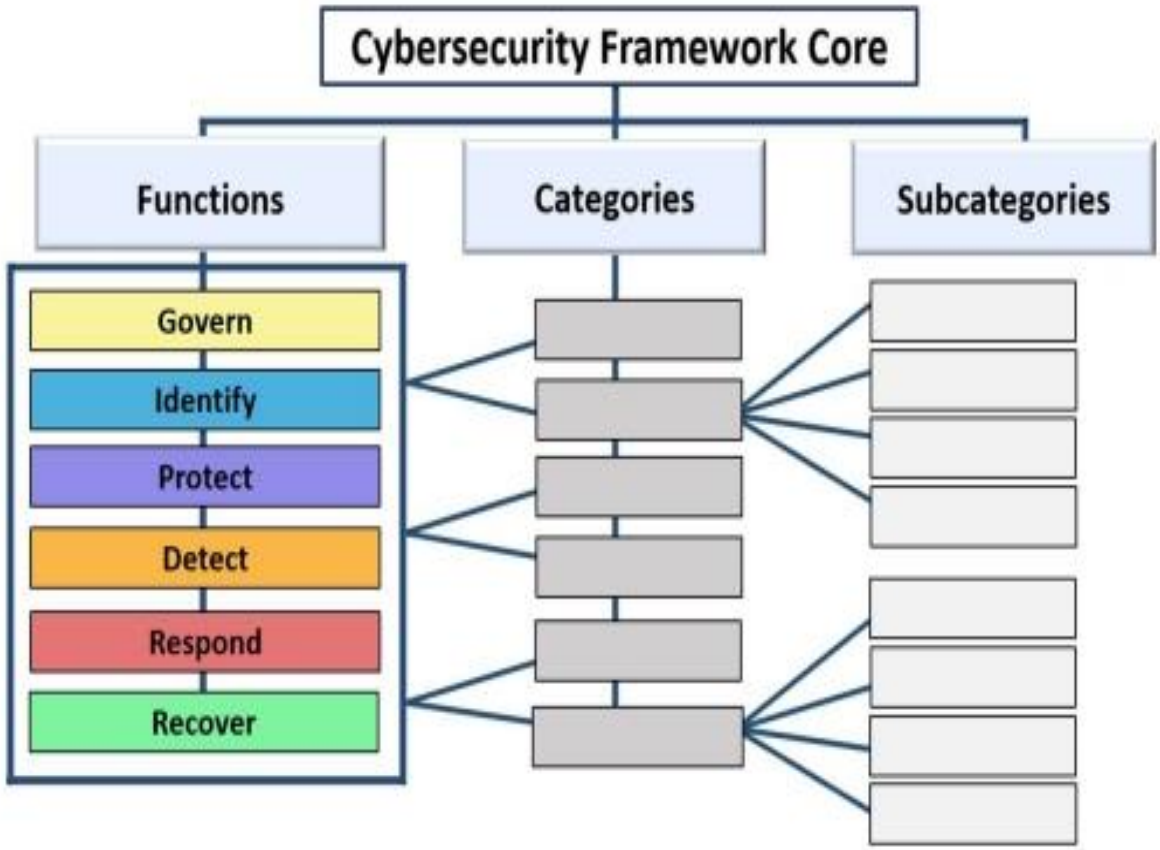
2.1 Παρουσίαση NIST Cybersecurity Framework 2.0

Το Πλαίσιο Κυβερνοασφάλειας NIST (CSF) 2.0 είναι ένα ολοκληρωμένο εργαλείο που αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) και παρέχει κατευθυντήριες γραμμές και βέλτιστες πρακτικές για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Το πλαίσιο μπορεί να προσαρμοστεί με ευελιξία στις ανάγκες και τους στόχους κάθε οργανισμού, ανεξάρτητα από το μέγεθος ή τον τομέα δραστηριότητάς του (Korff et al., 2021).

Το NIST Cybersecurity Framework 2.0 είναι μια αναθεωρημένη έκδοση του NIST Cybersecurity Framework, το οποίο έχει υιοθετηθεί ευρέως από οργανισμούς παγκοσμίως ως πρότυπο για τη διαχείριση κινδύνων στον κυβερνοχώρο. Η νέα έκδοση του πλαισίου ενσωματώνει τις εξελίξεις στην τεχνολογία και τις απειλές και παρέχει βελτιωμένες κατευθυντήριες γραμμές και πρακτικές για την ενίσχυση της ασφάλειας στον κυβερνοχώρο. Το Πλαίσιο NIST για την ασφάλεια στον κυβερνοχώρο αναπτύχθηκε αρχικά με τη συμμετοχή πολυάριθμων ενδιαφερομένων μερών, συμπεριλαμβανομένου του ιδιωτικού τομέα, των δημόσιων αρχών και της ακαδημαϊκής κοινότητας, προκειμένου να παρέχει ένα ευέλικτο, αποτελεσματικό και πρακτικό πλαίσιο για τη διαχείριση των κινδύνων στον κυβερνοχώρο. Είναι δομημένο γύρω από πέντε βασικές λειτουργίες - Προστασία, ανίχνευση, αντίδραση και ανάκτηση. Κάθε μία από αυτές τις λειτουργίες περιλαμβάνει κατηγορίες και υποκατηγορίες που παρέχουν λεπτομερείς οδηγίες για την εφαρμογή των μέτρων ασφαλείας (ENISA, 2022).

Το Πλαίσιο κυβερνοασφάλειας 2.0 του NIST είναι ένα πολύτιμο εργαλείο για τους οργανισμούς που επιδιώκουν να βελτιώσουν την ασφάλεια των συστημάτων και των δεδομένων τους. Η ευελιξία, η διεθνής αναγνώριση και η ολοκληρωμένη προσέγγιση του πλαισίου το καθιστούν ιδανικό για την αντιμετώπιση των σημερινών προκλήσεων της κυβερνοασφάλειας. Παρά τις προκλήσεις που ενδέχεται να προκύψουν κατά την εφαρμογή, τα οφέλη από την υιοθέτηση του NIST Cybersecurity Framework 2.0 είναι σημαντικά και συμβάλλουν στην ενίσχυση της ανθεκτικότητας ενός οργανισμού στις απειλές στον κυβερνοχώρο. Η έκδοση 2.0 εισάγει βελτιώσεις που καθιστούν το πλαίσιο πιο σύγχρονο και αποτελεσματικό, ενσωματώνουν τις τεχνολογικές εξελίξεις και ενισχύουν τις στρατηγικές διαχείρισης κινδύνων. Οι οργανισμοί που επιλέγουν να υιοθετήσουν το πλαίσιο μπορούν να διαχειριστούν τις απειλές στον κυβερνοχώρο με δομημένο και ολοκληρωμένο τρόπο και να βελτιώσουν την ασφάλεια και την αποτελεσματικότητα των επιχειρηματικών διαδικασιών (ENISA, 2021).

Εικόνα 1. Δομή CSF



Πηγή: The NIST Cybersecurity Framework (CSF) 2.0

2.1.1 Βασικά στοιχεία του NIST Cybersecurity Framework 2.0

- CSF Core

Το CSF Core αποτελεί τον βασικό πυλώνα του πλαισίου και περιλαμβάνει πέντε κύριες λειτουργίες (Functions) που ορίζουν τις βασικές δραστηριότητες για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Αυτές οι λειτουργίες είναι: Identify (Ταυτοποίηση), Protect (Προστασία), Detect (Ανίχνευση), Respond (Ανταπόκριση), και Recover (Αποκατάσταση). Κάθε λειτουργία περιλαμβάνει κατηγορίες και υποκατηγορίες που περιγράφουν συγκεκριμένα αποτελέσματα που πρέπει να επιτευχθούν (Maitland et al., 2021).

- CSF Profiles

Τα CSF Profiles παρέχουν τη δυνατότητα σε έναν οργανισμό να ορίσει την παρούσα και την ιδανική κατάσταση της κυβερνοασφάλειάς του. Με τον τρόπο αυτό βοηθά τους οργανισμούς να προσδιορίσουν τις προτεραιότητές τους και να σχεδιάσουν στρατηγικές για την επίτευξη των στόχων τους.

- CSF Tiers

Τα CSF Tiers ορίζουν τον βαθμό ωριμότητας των πρακτικών διαχείρισης κινδύνου ενός οργανισμού. Υπάρχουν τέσσερα επίπεδα (Partial, Risk Informed, Repeatable, Adaptive) που προσφέρουν ένα πλαίσιο για την αξιολόγηση και τη βελτίωση των συγκεκριμένων πρακτικών.

Η έκδοση 2.0 του Πλαισίου Κυβερνοασφάλειας του NIST εισάγει αρκετές βελτιώσεις και καινοτομίες για την αντιμετώπιση των σημερινών προκλήσεων της κυβερνοασφάλειας: Η έκδοση 2.0 ενισχύει τη σύνδεση μεταξύ της διαχείρισης κινδύνων και των επιχειρηματικών στόχων. Το Πλαίσιο ενισχύει τη σύνδεση μεταξύ της διαχείρισης κινδύνων και των επιχειρηματικών στόχων και ενσωματώνει τη διαδικασία διαχείρισης κινδύνων σε μια ευρύτερη επιχειρηματική στρατηγική, διασφαλίζοντας ότι οι αποφάσεις για την ασφάλεια στον κυβερνοχώρο λαμβάνονται με βάση τον αντίκτυπό τους στις επιχειρηματικές λειτουργίες. Το πλαίσιο αναγνωρίζει την ανάγκη ενσωμάτωσης καινοτόμων τεχνολογιών, όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση, για τον εντοπισμό και την αντιμετώπιση απειλών. Η έκδοση 2.0 παρέχει καθοδήγηση σχετικά με τον τρόπο ασφαλούς και αποτελεσματικής χρήσης αυτών των τεχνολογιών. Το αναθεωρημένο πλαίσιο υπογραμμίζει τη σημασία της συμμετοχής όλων των ενδιαφερόμενων μερών, συμπεριλαμβανομένων των ανώτερων διοικητικών στελεχών, των τεχνικών ομάδων και των τρίτων παρόχων υπηρεσιών, στην ανάπτυξη και εφαρμογή στρατηγικών κυβερνοασφάλειας. Η έκδοση 2.0 εμπεριέχει αναφορές σε άλλες κατευθυντήριες γραμμές και πρότυπα, όπως το ISO/IEC 27001 και το COBIT, προκειμένου να διευκολυνθεί η εφαρμογή ενός ολοκληρωμένου προγράμματος ασφάλειας στον κυβερνοχώρο με βάση τις βέλτιστες πρακτικές (Maitland et al., 2021).

Εικόνα 2. Λειτουργίες και περιγραφή

Function	Description
Govern	"Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy. The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations."
Identify	"Help determine the current cybersecurity risk to the organization. Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN."
Protect	"Use safeguards to prevent or reduce cybersecurity risk. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events."
Detect	"Find and analyze possible cybersecurity attacks and compromises. DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring."
Respond	"Take action regarding a detected cybersecurity incident. RESPOND supports the ability to contain the impact of cybersecurity incidents."
Recover	"Restore assets and operations that were impacted by a cybersecurity incident. RECOVER supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts."

Πηγή: Paper Title (use style: paper title) (esa.int)

2.1.2 Λειτουργίες του CSF Core

Εικόνα 3. Βασικές λειτουργίες, ονομασίες και αναγνωριστικά του CSF 2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Πηγή: The NIST Cybersecurity Framework (CSF) 2.0

- Identify (ID):

Η λειτουργία αυτή περιλαμβάνει την κατανόηση του περιβάλλοντος του οργανισμού και τον προσδιορισμό των περιουσιακών στοιχείων, των δεδομένων και των συναφών κινδύνων που πρέπει να διαχειριστούν. Οι βασικές κατηγορίες περιλαμβάνουν τη διαχείριση περιουσιακών στοιχείων, το επιχειρηματικό περιβάλλον, τη διακυβέρνηση, την αξιολόγηση κινδύνων και τις στρατηγικές διαχείρισης κινδύνων. Η λειτουργία Identify περιλαμβάνει κατηγορίες που βοηθούν τον οργανισμό να

κατανοήσει και να διαχειριστεί τους κινδύνους που σχετίζονται με τα συστήματά του. Οι βασικές κατηγορίες αυτής της λειτουργίας περιλαμβάνουν:

- «Διαχείριση πόρων»: προσδιορισμός και διαχείριση φυσικών και εικονικών πόρων.
- Επιχειρησιακό περιβάλλον: κατανόηση του ρόλου των συστημάτων και των διαδικασιών σε έναν οργανισμό.
- Διακυβέρνηση: ανάπτυξη πολιτικών και διαδικασιών ασφάλειας στον κυβερνοχώρο.
- Αξιολόγηση κινδύνου: αξιολόγηση πιθανών απειλών και τρωτών σημείων.
- Στρατηγική διαχείρισης κινδύνου: ανάπτυξη στρατηγικής για τη διαχείριση των κινδύνων (Maitland et al., 2021).

- Protect (PR):

Η λειτουργία αυτή περιλαμβάνει την ανάπτυξη και την εφαρμογή κατάλληλων μέτρων για τη συνεχή παροχή κρίσιμων υπηρεσιών. Οι κύριες κατηγορίες είναι η διαχείριση ταυτότητας και ο έλεγχος πρόσβασης, η ευαισθητοποίηση και η κατάρτιση, η ασφάλεια δεδομένων, οι διαδικασίες και οι διαδικασίες προστασίας πληροφοριών και η συντήρηση. Η λειτουργία Προστασίας επικεντρώνεται στην εφαρμογή μέτρων για την προστασία κρίσιμων υποδομών και δεδομένων. Συγκεκριμένα:

- ✓ Identity Management and Access Control (Διαχείριση ταυτότητας και έλεγχος πρόσβασης): Διασφαλίζει πως μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε συγκεκριμένα συστήματα.
- ✓ Awareness and Training (Ευαισθητοποίηση και εκπαίδευση): Εκπαίδευση των εργαζομένων για την αναγνώριση και την αντιμετώπιση των απειλών.
- ✓ Data Security (Ασφάλεια δεδομένων): Εφαρμογή μέτρων προστασίας των δεδομένων από μη εξουσιοδοτημένη πρόσβαση.
- ✓ Information Protection Processes and Procedures (Διαδικασίες προστασίας πληροφοριών): Δημιουργία και συντήρηση πολιτικών για την προστασία των πληροφοριών.
- ✓ Maintenance (Συντήρηση): Τακτική συντήρηση των συστημάτων για την αποτροπή των ευπαθειών.
- ✓ Protective Technology (Προστατευτική τεχνολογία): Χρήση τεχνολογικών λύσεων για την προστασία των συστημάτων (Stallings, 2020).

- Detect (DE):

Η συγκεκριμένη λειτουργία αφορά την ανάπτυξη και την εφαρμογή κατάλληλων δραστηριοτήτων για τον εντοπισμό απειλών και περιστατικών στον κυβερνοχώρο. Οι κύριες κατηγορίες είναι οι ανωμαλίες και τα περιστατικά, η συνεχής παρακολούθηση της ασφάλειας και οι διαδικασίες ανίχνευσης. Η λειτουργία ανίχνευσης αφορά την ανάπτυξη και τη διατήρηση της ικανότητας έγκαιρης ανίχνευσης απειλών. Οι βασικές κατηγορίες περιλαμβάνουν:

- ✓ Anomalies and Events (Ανωμαλίες και συμβάντα): Αναγνώριση δυσλειτουργιών και συμβάντων που πιθανώς υποδηλώνουν παραβίαση ασφάλειας.
- ✓ Security Continuous Monitoring (Συνεχής παρακολούθηση ασφάλειας): Συνεχής παρακολούθηση των συστημάτων για ανίχνευση και αξιολόγηση των απειλών.
- ✓ Detection Processes (Διαδικασίες ανίχνευσης): Δημιουργία και εφαρμογή διαδικασιών για την ανίχνευση απειλών (Maitland et al., 2021).

- Respond (RS):

Η συγκεκριμένη λειτουργία περιλαμβάνει την ανάπτυξη και την εφαρμογή κατάλληλων δραστηριοτήτων για την αντιμετώπιση των απειλών και περιστατικών στον κυβερνοχώρο που εντοπίζονται. Οι κύριες κατηγορίες είναι ο σχεδιασμός απόκρισης, η επικοινωνία, η ανάλυση, ο μετριασμός και η αποκατάσταση. Η λειτουργία απόκρισης επικεντρώνεται στη διαχείριση των περιστατικών ασφάλειας που συμβαίνουν. Οι βασικές κατηγορίες περιλαμβάνουν:

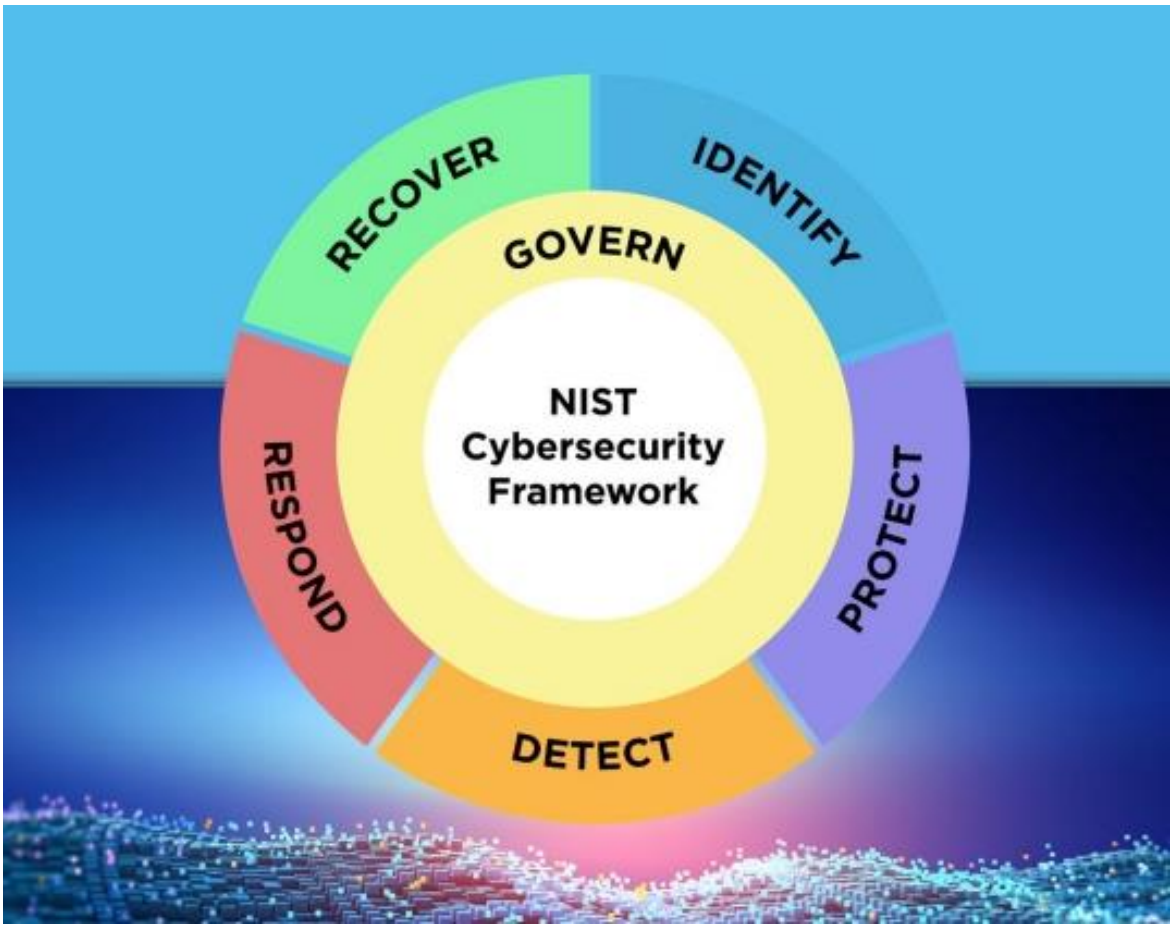
- ✓ Response Planning (Σχεδιασμός ανταπόκρισης): Ανάπτυξη και εφαρμογή σχεδίων ανταπόκρισης σε ζητήματα ασφάλειας.
- ✓ Communications (Επικοινωνίες): Διασφάλιση αποτελεσματικής επικοινωνίας κατά τη διάρκεια και μετά από ένα ζήτημα ασφάλειας.
- ✓ Analysis (Ανάλυση): Ανάλυση των περιστατικών για την κατανόηση της φύσης και της επίπτωσής τους.
- ✓ Mitigation (Μετριασμός): Εφαρμογή μέτρων για τον περιορισμό της επίπτωσης των περιστατικών ασφάλειας.
- ✓ Improvements (Βελτιώσεις): Ανασκόπηση των περιστατικών και βελτίωση των σχεδίων και των διαδικασιών ανταπόκρισης (Maitland et al., 2021).

- Recover (RC):

Η παρούσα λειτουργία περιλαμβάνει την ανάπτυξη και εφαρμογή κατάλληλων δραστηριοτήτων για την αποκατάσταση των υπηρεσιών και δυνατοτήτων που επηρεάζονται από απειλές και περιστατικά στον κυβερνοχώρο. Οι κύριες κατηγορίες είναι ο σχεδιασμός αποκατάστασης, η αποκατάσταση και η επικοινωνία. Η λειτουργία αποκατάστασης περιλαμβάνει δραστηριότητες για την αποκατάσταση υπηρεσιών και δυνατοτήτων που επηρεάζονται από περιστατικά ασφαλείας. Οι σημαντικότερες κατηγορίες είναι:

- ✓ Recovery Planning (Σχεδιασμός ανάκτησης): Ανάπτυξη και εφαρμογή σχεδίων για την αποκατάσταση των υπηρεσιών.
- ✓ Improvements (Βελτιώσεις): Βελτίωση των διαδικασιών ανάκτησης βάσει των εμπειριών από τα περιστατικά ασφάλειας.
- ✓ Communications (Επικοινωνίες): Επικοινωνία με τους μετόχους κατά τη διαδικασία της ανάκτησης (Peltier et al., 2005).

Εικόνα 4. Οι λειτουργίες του CSF



Πηγή: The NIST Cybersecurity Framework (CSF) 2.0

- Η λειτουργία Govern (Διακυβέρνηση)

Η λειτουργία της διακυβέρνησης προστέθηκε ως νέα κατηγορία στην έκδοση 2.0 του Πλαισίου Κυβερνοασφάλειας του NIST και αποτελεί σημαντικό στοιχείο της συνολικής διαχείρισης της κυβερνοασφάλειας ενός οργανισμού. Το υπόβαθρο της προσθήκης αυτής της λειτουργίας αντανακλά την ανάγκη για καλύτερη διακυβέρνηση και καθοδήγηση των διαδικασιών ασφάλειας από πάνω προς τα κάτω στη διοικητική δομή ενός οργανισμού. Η λειτουργία αυτή αποσκοπεί στη δημιουργία μιας δομής διακυβέρνησης της κυβερνοασφάλειας, συμπεριλαμβανομένης της ανάπτυξης πολιτικών, διαδικασιών και ελέγχων που ευθυγραμμίζονται με τους επιχειρηματικούς στόχους και τις κανονιστικές απαιτήσεις του οργανισμού (NIST, 2023).

Μία από τις βασικές λειτουργίες της διακυβέρνησης είναι η στρατηγική καθοδήγηση της διαχείρισης της ασφάλειας στον κυβερνοχώρο και η διασφάλιση ότι τα μέτρα ασφάλειας ενσωματώνονται στον πυρήνα της επιχειρηματικής στρατηγικής και των λειτουργιών διαχείρισης. Αυτό κατακτάται μέσα από την ανάπτυξη, της παρακολούθησης και της συνεχούς βελτίωσης των πολιτικών ασφάλειας, των στρατηγικών διαχείρισης κινδύνων και των προτύπων που εφαρμόζονται σε όλους τους τομείς του οργανισμού.

Ορισμένα από τα κύρια στοιχεία της λειτουργίας Govern περιλαμβάνουν:

1. **Ορισμός πολιτικής και κατευθυντήριων γραμμών:** Η λειτουργία αυτή υποστηρίζει την ανάπτυξη και εφαρμογή ενός πλαισίου πολιτικής ασφάλειας που ορίζει συγκεκριμένες κατευθυντήριες γραμμές για την προστασία των δεδομένων και των συστημάτων του οργανισμού. Οι πολιτικές αυτές θα πρέπει να διασφαλίζουν ότι οι συμπεριφορές και οι στρατηγικές διαχείρισης κινδύνων ευθυγραμμίζονται με τις επιχειρηματικές ανάγκες και τους στόχους του οργανισμού, ενώ παράλληλα διασφαλίζουν τη συμμόρφωση με τις νομικές απαιτήσεις.

2. **Εδραίωση της διακυβέρνησης της ασφάλειας στον κυβερνοχώρο στις επιχειρηματικές δραστηριότητες:** Ένας από τους κύριους στόχους της λειτουργίας διακυβέρνησης είναι η ενσωμάτωση της ασφάλειας στον κυβερνοχώρο ως αναπόσπαστο μέρος των καθημερινών επιχειρηματικών δραστηριοτήτων. Η ασφάλεια στον κυβερνοχώρο δεν πρέπει να αντιμετωπίζεται ως ξεχωριστό ή απομονωμένο ζήτημα. Σε άλλη περίπτωση, θα πρέπει να αποτελεί κεντρικό στοιχείο όλων των αποφάσεων και διαδικασιών που σχετίζονται με την προστασία των περιουσιακών στοιχείων, των δεδομένων και των πληροφοριακών συστημάτων.

3. **Διαχείριση ρόλων και αρμοδιοτήτων:** Οι επιχειρησιακοί διαχειριστές καθορίζουν τους ρόλους και τις αρμοδιότητες σε όλα τα επίπεδα του οργανισμού και διασφαλίζουν ότι ο εκάστοτε υπάλληλος αντιλαμβάνεται τις ευθύνες του για την προστασία των πληροφοριών και των συστημάτων. Αυτό

περιλαμβάνει την ανάθεση συγκεκριμένων ρόλων και αρμοδιοτήτων για τη διαχείριση κινδύνων και την εφαρμογή διαδικασιών υποβολής εκθέσεων.

4. **Παρατήρηση συμμόρφωσης και διαχείριση κινδύνων**: Η διακυβέρνηση στον τομέα της ασφάλειας στον κυβερνοχώρο εμπεριέχει επίσης την παρατήρηση της συμμόρφωσης με τα εσωτερικά πρότυπα ασφάλειας και τους κανονισμούς, καθώς και τη διαχείριση των κινδύνων που ενδέχεται να προκύψουν από εξωτερικές και εσωτερικές απειλές. Μέσα από αυτή τη διαδικασία, οι οργανισμοί εξασφαλίζουν πως τα συστήματά τους είναι ασφαλή και εναρμονισμένα με τις καλύτερες διεθνείς πρακτικές.

5. **Ανάλυση απειλών και προσαρμογή στρατηγικών:** Οι δραστηριότητες διακυβέρνησης απαιτούν συνεχή παρακολούθηση των τάσεων των απειλών στον κυβερνοχώρο και προσαρμογή των στρατηγικών για την αντιμετώπιση των αναδυόμενων κινδύνων. Αυτό σημαίνει ότι ο οργανισμός πρέπει να αναλύει τα δεδομένα που συλλέγει από τις απειλές και να επικαιροποιεί τα σχέδια ασφαλείας του με βάση τα αποτελέσματα της ανάλυσης αυτής.

6. **Διαφάνεια και λογοδοσία**: Οι δραστηριότητες διακυβέρνησης διασφαλίζουν τη διαφάνεια και τη λογοδοσία για την ασφάλεια σε όλα τα επίπεδα του οργανισμού. Αυτό περιλαμβάνει τη σαφή κοινοποίηση των πολιτικών και των διαδικασιών ασφάλειας στα ενδιαφερόμενα μέρη και την τακτική αναφορά της προόδου όσον αφορά τη συμμόρφωση και τη διαχείριση των κινδύνων (NIST, 2023).

Για την επιτυχή εφαρμογή της λειτουργίας Govern, είναι απαραίτητο να ακολουθούνται συγκεκριμένες πρακτικές:

- **Συμμετοχή της ανώτερης διοίκησης**: Η ανώτερη διοίκηση πρέπει να συμμετέχει ένθερμα στον καθορισμό της στρατηγικής ασφάλειας και να παρέχει την κατάλληλη καθοδήγηση και υποστήριξη. Η έλλειψη συμμετοχής της ανώτερης διοίκησης μπορεί να οδηγήσει σε αποτυχία της συνολικής στρατηγικής ασφάλειας στον κυβερνοχώρο.
- **Διασύνδεση σχέσης ανάμεσα στην επιχειρηματική στρατηγική και ασφάλεια στον κυβερνοχώρο**: Η ασφάλεια στον κυβερνοχώρο δεν μπορεί να λειτουργήσει ανεξάρτητα από τους επιχειρηματικούς στόχους ενός οργανισμού. Αντίθετα, πρέπει να είναι πλήρως ευθυγραμμισμένη με την ευρύτερη επιχειρηματική στρατηγική, ώστε η διαχείριση των κινδύνων να γίνεται στο πλαίσιο της επίτευξης των επιχειρηματικών στόχων.
- **Συνεχής εκπαίδευση και κατάρτιση**: Η εκπαίδευση του προσωπικού είναι απαραίτητη για την επιτυχή διακυβέρνηση. Το προσωπικό θα πρέπει να ενημερώνεται τακτικά για τις νέες πρακτικές ασφάλειας στον κυβερνοχώρο, τις τεχνολογικές εξελίξεις και τις μεταβαλλόμενες απειλές.
- **Συνεχής αναθεώρηση και βελτίωση των πολιτικών**: Οι πολιτικές διακυβέρνησης πρέπει να επανεξετάζονται και να βελτιώνονται τακτικά, ώστε να παραμένουν αποτελεσματικές και

σύμφωνες με τις τρέχουσες απαιτήσεις ασφαλείας. Η τακτική αναθεώρηση επιτρέπει στους οργανισμούς να προσαρμόζονται στις νέες προκλήσεις και να βελτιώνουν την ικανότητά τους να ανταποκρίνονται στις νέες απειλές.

Η λειτουργία της διακυβέρνησης είναι ζωτικής σημασίας για την αποτελεσματική διαχείριση των διαδικασιών ασφάλειας στον κυβερνοχώρο. Οι οργανισμοί του δημόσιου και του ιδιωτικού τομέα που εφαρμόζουν με επιτυχία αυτή τη λειτουργία μπορούν να βελτιώσουν σημαντικά την ικανότητά τους να ανταποκρίνονται στις απειλές, να διαχειρίζονται τους κινδύνους και να διασφαλίζουν την επιχειρησιακή συνέχεια κατά τη διάρκεια μιας κρίσης (NIST, 2023).

2.1.3 Πλεονεκτήματα του NIST CSF 2.0

Το NIST CSF 2.0 παρέχει πολλά οφέλη στον οργανισμό που το εφαρμόζει. Πρώτον, είναι ευέλικτο και προσαρμόσιμο: το πλαίσιο μπορεί να προσαρμοστεί στις ανάγκες και τα χαρακτηριστικά κάθε οργανισμού, ανεξάρτητα από το μέγεθος ή τον τομέα του. Εξίσου σημαντική είναι η διεθνής αναγνώριση και υιοθέτηση: Το Πλαίσιο Κυβερνοασφάλειας του NIST έχει αποκτήσει διεθνή αναγνώριση και έχει υιοθετηθεί από οργανισμούς σε όλο τον κόσμο. Η αναγνώριση αυτή καθιστά το Πλαίσιο μια αξιόπιστη βάση για την ανάπτυξη πολιτικών και διαδικασιών κυβερνοασφάλειας που συμμορφώνονται με τις παγκόσμιες κανονιστικές απαιτήσεις. Μπορεί επίσης να βελτιώσει την αποτελεσματικότητα στην αντιμετώπιση των απειλών. Η δομημένη προσέγγιση του Πλαισίου βοηθά τους οργανισμούς να εντοπίζουν, να προστατεύουν, να ανιχνεύουν, να αντιδρούν και να ανακάμπτουν αποτελεσματικότερα από περιστατικά ασφάλειας- οι πέντε βασικές λειτουργίες καλύπτουν όλο το φάσμα της ασφάλειας στον κυβερνοχώρο και ενισχύουν την ετοιμότητα για την αντιμετώπιση απειλών. Η διαχείριση κινδύνων μπορεί να προστεθεί σε αυτό το σημείο. Αυτή παρέχει μια συστηματική προσέγγιση για τη διαχείριση των κινδύνων κυβερνοασφάλειας και επιτρέπει στους οργανισμούς να εντοπίζουν, να αξιολογούν και να διαχειρίζονται τις απειλές. Μέσω της συνεχούς βελτίωσης δημιουργείται ένας μηχανισμός συνεχούς βελτίωσης που επιτρέπει στους οργανισμούς να προσαρμόζουν τις στρατηγικές τους καθώς εξελίσσονται οι απειλές. Τέλος, θα πρέπει να αναφερθεί η συμμόρφωση με τα διεθνή πρότυπα: Το NIST CSF 2.0 είναι ευθυγραμμισμένο με διεθνή πρότυπα και κανονισμούς, διευκολύνοντας τους οργανισμούς να συμμορφωθούν με τα κανονιστικά πλαίσια (Golling et al., 2021).

2.1.4 Προκλήσεις και περιορισμοί

Παρά το γεγονός, ότι παρουσιάζει θετικά στοιχεία, μέσα από την έρευνα προκύπτουν συγκεκριμένες προκλήσεις και περιορισμοί. Μερικοί από αυτούς είναι οι ακόλουθοι:

- **Πολυπλοκότητα της εφαρμογής**

Για ορισμένους οργανισμούς, η χρήση του NIST Cybersecurity Framework πιθανόν να είναι πολύπλοκη και να απαιτεί πολύ χρόνο, ιδιαίτερα για όσους δεν διαθέτουν εξειδικευμένο προσωπικό ή επαρκείς πόρους. Η ανάγκη για λεπτομερειακή ανάλυση και προσαρμογή των κατευθυντήριων γραμμών στις συγκεκριμένες ανάγκες του οργανισμού μπορεί να αποτελέσει σημαντική πρόκληση (Golling et al., 2021).

- **Συνεχής προσαρμογή στις νέες απειλές**

Η ταχεία εξέλιξη της τεχνολογίας και των απειλών στον κυβερνοχώρο απαιτεί από τους οργανισμούς να προσαρμόζουν συνεχώς τις στρατηγικές και τις πρακτικές τους. Η συνεχής ενημέρωση και η ανταπόκριση στις νέες απειλές μπορεί να είναι πρόκληση, ιδίως για οργανισμούς με περιορισμένους πόρους (Golling et al., 2021).

Το Πλαίσιο Κυβερνοασφάλειας (CSF) 2.0 του NIST αποτελεί εξέλιξη του αρχικού CSF του NIST που αναπτύχθηκε για να καθοδηγήσει τους οργανισμούς των ΗΠΑ στη βελτίωση της κυβερνοασφάλειας. Το πλαίσιο είναι αρκετά ευέλικτο ώστε να προσαρμόζεται σε διαφορετικές ανάγκες και μεγέθη οργανισμών, ενώ παρέχει δομή και καθοδήγηση για τη διαχείριση και τον μετριασμό των κινδύνων στον κυβερνοχώρο. Στο πλαίσιο αυτό, τα «σημεία ελέγχου» και τα λογιστικά φύλλα του NIST CSF 2.0 αποτελούν σημαντικά εργαλεία για την αξιολόγηση και την παρακολούθηση της συμμόρφωσης με το πλαίσιο και της προόδου της διαχείρισης της κυβερνοασφάλειας ενός οργανισμού.

Τα σημεία ελέγχου (λογιστικά φύλλα) του NIST CSF 2.0 χρησιμεύουν ως ένα σύνολο εργαλείων που βοηθούν τους οργανισμούς να αξιολογήσουν τη συμμόρφωσή τους με τις λειτουργίες, τις κατηγορίες και τις υποκατηγορίες του πλαισίου. Κάθε σημείο ελέγχου συνδέεται με ορισμένες δραστηριότητες και τακτικές οι οποίες είναι αναγκαίο να υιοθετηθούν για να επιτευχθεί το θεμιτό επίπεδο κυβερνοασφάλειας (Anderson, 2001).

Τα κύρια στοιχεία του λογιστικού φύλλου (speedsheet) εμπεριέχουν κατηγορίες και υποκατηγορίες και μπορούν να αξιολογήσουν τη συμμόρφωσή τους με τις κατηγορίες και τις υποκατηγορίες του πλαισίου. Το λογιστικό φύλλο επιτρέπει στον οργανισμό να παρακολουθεί την πρόοδό του σε κάθε κατηγορία με την πάροδο του χρόνου και να αξιολογεί την αποτελεσματικότητα των μέτρων που εφαρμόζει. Όσον αφορά τη μέτρηση του κινδύνου, το λογιστικό φύλλο επιτρέπει στον οργανισμό να ποσοτικοποιεί τον κίνδυνο σε διάφορους τομείς των δραστηριοτήτων του και να αξιολογεί αντικειμενικά τους κινδύνους και τα τρωτά σημεία των συστημάτων του. Η διαχείριση των πόρων και των επενδύσεων χρήζει επίσης ιδιαίτερης μνείας. Τα σημεία ελέγχου επίσης, είναι δυνατό να χρησιμοποιηθούν για τη διαχείριση πόρων και επενδύσεων που μπορούν να χρησιμοποιηθούν για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Αυτό επιτρέπει στους οργανισμούς να κατανέμουν

αποτελεσματικά τους πόρους και να διασφαλίζουν ότι οι κρίσιμοι τομείς λαμβάνουν την απαραίτητη προσοχή. Τέλος, οι οργανισμοί μπορούν να χρησιμοποιούν τα λογιστικά φύλλα για να συμμορφώνονται με τις βέλτιστες πρακτικές και τους κανονισμούς και να διασφαλίζουν ότι πληρούν τα πρότυπα που έχουν καθοριστεί από το NIST και άλλους διεθνείς οργανισμούς (Smith et al.2010).

Εικόνα 5. Βήματα δημιουργίας και χρήσης CSF

Πηγή: [The NIST Cybersecurity Framework (CSF) 2.0]

2.1.5 Επίπεδο προσαρμογής των οργανισμών στις Ηνωμένες Πολιτείες

Η οργανωτική υιοθέτηση του CSF 2.0 του NIST ποικίλλει ανάλογα με το μέγεθος, τη δομή και τον τομέα του οργανισμού. Σε γενικές γραμμές, οι μεγάλοι οργανισμοί, ιδίως στους τομείς του χρηματοπιστωτικού τομέα, της υγειονομικής περίθαλψης και της τεχνολογίας, παρουσιάζουν υψηλό βαθμό συμμόρφωσης με το πλαίσιο. Οι οργανισμοί αυτοί έχουν αναγνωρίσει τη σημασία της ασφάλειας στον κυβερνοχώρο και έχουν αφιερώσει πόρους για την ενσωμάτωση του NIST CSF 2.0 στις στρατηγικές και τις δραστηριότητές τους. Οι οργανισμοί του χρηματοπιστωτικού τομέα, όπως οι τράπεζες και οι ασφαλιστικές εταιρείες, ήταν από τους πρώτους που υιοθέτησαν το NIST CSF 2.0. Η φύση αυτού του κλάδου, ο οποίος βασίζεται στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων, απαιτεί την τήρηση αυστηρών προτύπων ασφάλειας στον κυβερνοχώρο (Smith et al.)

Ο υψηλός βαθμός συμμόρφωσης με τις απαιτήσεις του NIST CSF 2.0 σε αυτόν τον τομέα επιτυγχάνεται μέσω επενδύσεων στις πιο πρόσφατες τεχνολογίες ασφάλειας, συνεχούς κατάρτισης του προσωπικού και εφαρμογής προτύπων διαχείρισης κινδύνων. Οι τράπεζες και οι χρηματοπιστωτικές εταιρείες κάνουν εκτεταμένη χρήση λογιστικών φύλλων για την παρακολούθηση της συμμόρφωσης με το πλαίσιο και την προσαρμογή των στρατηγικών ασφαλείας ανάλογα με την πρόοδο που σημειώνεται. Στον κλάδο της υγειονομικής περίθαλψης, η συμμόρφωση με το NIST CSF 2.0 είναι κρίσιμη λόγω της ευαίσθητης φύσης των δεδομένων που διαχειρίζεται ο τομέας αυτός. Οργανισμοί υγειονομικής περίθαλψης, όπως νοσοκομεία και κλινικές, έχουν υιοθετήσει το NIST CSF 2.0 για να προστατεύσουν τα ιατρικά δεδομένα των ασθενών και να διασφαλίσουν τη συνεχή λειτουργία τους. Ωστόσο, παρά την αναγνώριση της σημασίας της συμμόρφωσης με το Πλαίσιο, πολλές εγκαταστάσεις υγειονομικής περίθαλψης αντιμετωπίζουν προκλήσεις στην εφαρμογή του NIST CSF 2.0 λόγω έλλειψης πόρων και εμπειρογνωμοσύνης. Τα λογιστικά φύλλα χρησιμοποιούνται ευρέως για την τεκμηρίωση των απειλών, την αξιολόγηση της συμμόρφωσης και τον προσδιορισμό των αναγκών κατάρτισης του προσωπικού, αλλά η έλλειψη εξειδικευμένου προσωπικού συχνά καθυστερεί την πλήρη ενσωμάτωση του πλαισίου.

Οι μικρές και μεσαίες επιχειρήσεις έχουν το ευρύτερο πεδίο προσαρμογής στο πλαίσιο NIST CSF 2.0. Οι περισσότερες ΜΜΕ κατανοούν τη σημασία της ασφάλειας στον κυβερνοχώρο, αλλά συχνά αντιμετωπίζουν περιορισμούς που δυσχεραίνουν την πλήρη ενσωμάτωση του πλαισίου. Οι περιορισμοί αυτοί περιλαμβάνουν την έλλειψη πόρων, την έλλειψη εξειδικευμένου προσωπικού και την απροθυμία να επενδύσουν σε λύσεις ασφάλειας στον κυβερνοχώρο. Ωστόσο, πολλές ΜΜΕ χρησιμοποιούν το υπολογιστικό φύλλο NIST CSF 2.0 ως εργαλείο για τη σταδιακή βελτίωση της ασφάλειας στον κυβερνοχώρο (Anderson, 2001).

2.1.6 Δυσκολίες στην εφαρμογή του NIST CSF 2.0

Αν και το NIST CSF 2.0 είναι ένα δομημένο και ευέλικτο πλαίσιο, η εφαρμογή του παρουσιάζει προκλήσεις.

Οι οργανισμοί που επιδιώκουν να συμμορφωθούν με τις κατευθυντήριες γραμμές του NIST CSF 2.0 αντιμετωπίζουν διάφορα εμπόδια, τα οποία σχετίζονται κυρίως με την πολυπλοκότητα του πλαισίου, τις απαιτήσεις σε προσωπικό και πόρους και την ανάγκη προσαρμογής στις ειδικές ανάγκες κάθε οργανισμού. Πρώτον, πρέπει να αντιμετωπιστεί η πολυπλοκότητα του πλαισίου: Το NIST CSF 2.0 είναι ένα ευρύ πλαίσιο με μεγάλο αριθμό λειτουργιών, κατηγοριών και υποκατηγοριών. Αυτή η πολυπλοκότητα μπορεί να είναι αποθαρρυντική, ιδίως για οργανισμούς χωρίς εμπειρία στην κυβερνοασφάλεια. Οι αλληλεξαρτήσεις μεταξύ των διαφόρων κατηγοριών και λειτουργιών του πλαισίου καθιστούν την εφαρμογή μια σύνθετη διαδικασία που απαιτεί γνώσεις και εμπειρία εμπειρογνωμόνων. Οι απαιτήσεις σε ανθρώπινους πόρους θα πρέπει επίσης να ενσωματωθούν στο

πλαίσιο των προκλήσεων εφαρμογής: Η αποτελεσματική εφαρμογή του NIST CSF 2.0 απαιτεί την παρουσία εξειδικευμένου προσωπικού που κατανοεί τις λεπτομέρειες του πλαισίου και μπορεί να το προσαρμόσει στις ανάγκες του οργανισμού. Ωστόσο, η έλλειψη εξειδικευμένων εμπειρογνωμόνων στον τομέα της ασφάλειας στον κυβερνοχώρο αποτελεί σημαντικό εμπόδιο. Ακόμη και αν ένας οργανισμός είναι σε θέση να προσλάβει τα κατάλληλα άτομα, η ανάγκη για συνεχή εκπαίδευση και ενημέρωση σχετικά με τις εξελίξεις στην ασφάλεια στον κυβερνοχώρο ασκεί πρόσθετη πίεση στους διαθέσιμους πόρους (Anderson, 2001).

Όσον αφορά τους οικονομικούς περιορισμούς, η εφαρμογή του CSF 2.0 του NIST μπορεί να απαιτήσει σημαντικές επενδύσεις σε τεχνολογία, διαδικασίες και ανθρώπινους πόρους. Πολλοί οργανισμοί, ιδίως οι ΜΜΕ, αντιμετωπίζουν οικονομικούς περιορισμούς που τους εμποδίζουν να επενδύσουν τα κεφάλαια που απαιτούνται για την πλήρη συμμόρφωση με το πλαίσιο- ενώ το NIST CSF 2.0 έχει σχεδιαστεί για να είναι ευέλικτο και προσαρμόσιμο, η εφαρμογή σε πλήρη κλίμακα μπορεί να υπερβαίνει τις οικονομικές δυνατότητες πολλών οργανισμών. Πρέπει επίσης να προσαρμοστεί σε συγκεκριμένες ανάγκες. Πιο συγκεκριμένα, θα πρέπει να καταστεί σαφές ότι κάθε οργανισμός είναι μοναδικός και έχει συγκεκριμένες ανάγκες και προκλήσεις- ενώ το NIST CSF 2.0 παρέχει κατευθυντήριες γραμμές, δεν παρέχει μια λύση «ενός μεγέθους για όλους». Αυτό σημαίνει ότι οι οργανισμοί πρέπει να επενδύσουν χρόνο και προσπάθεια για την προσαρμογή του πλαισίου στις δικές τους ανάγκες, γεγονός που απαιτεί βαθιά κατανόηση τόσο του πλαισίου όσο και των ειδικών αναγκών και κινδύνων του οργανισμού.

Οι πολιτισμικές προκλήσεις και η αντίσταση στην αλλαγή είναι επίσης σημαντικές πτυχές. Η εφαρμογή ενός νέου πλαισίου για την ασφάλεια στον κυβερνοχώρο μπορεί να προκαλέσει αντίσταση του προσωπικού, ιδίως εάν η αλλαγή θεωρείται δύσκολη ή πολύπλοκη- η επιτυχία του NIST CSF 2.0 θα εξαρτηθεί σε μεγάλο βαθμό από την προθυμία των εργαζομένων να ακολουθήσουν τις νέες διαδικασίες και πρακτικές. Ορισμένοι οργανισμοί αντιμετώπισαν δυσκολίες στην καλλιέργεια της κουλτούρας ασφάλειας που είναι απαραίτητη για την επιτυχή εφαρμογή του πλαισίου.

Εν ολίγοις, το NIST CSF 2.0 είναι ένα από τα πιο ολοκληρωμένα και ευέλικτα εργαλεία κυβερνοασφάλειας και παρέχει κατευθυντήριες γραμμές που μπορούν να προσαρμοστούν στις συγκεκριμένες ανάγκες κάθε οργανισμού. Ωστόσο, η εφαρμογή του δεν είναι χωρίς προκλήσεις. Οι οργανισμοί που επιθυμούν να συμμορφωθούν με το πλαίσιο πρέπει να διαθέσουν τους απαραίτητους πόρους, να απασχολήσουν εξειδικευμένο προσωπικό και να προσαρμόσουν τις κατευθυντήριες γραμμές στις συγκεκριμένες ανάγκες τους- τα σημεία ελέγχου και τα λογιστικά φύλλα του NIST CSF 2.0 αποτελούν σημαντικά εργαλεία. Ωστόσο, η πολυπλοκότητα του πλαισίου, οι οικονομικοί περιορισμοί, οι απαιτήσεις σε προσωπικό και η ανάγκη κάθε οργανισμού να το προσαρμόσει στα δικά του χαρακτηριστικά αποτελούν τα κύρια εμπόδια για την πλήρη και αποτελεσματική εφαρμογή του. Ωστόσο, οι οργανισμοί που ξεπερνούν αυτές τις προκλήσεις και ενσωματώνουν επιτυχώς το NIST CSF 2.0 στις δραστηριότητές τους μπορούν να επιτύχουν υψηλό επίπεδο ασφάλειας στον κυβερνοχώρο και

να προστατεύσουν αποτελεσματικά τα δεδομένα και τις υποδομές τους από τις εξελισσόμενες απειλές στον κυβερνοχώρο (Anderson, 2001).

Εικόνα 6. Χρήση του CSF για τη βελτίωση της επικοινωνίας σχετικά με τη διαχείριση κινδύνων

Πηγή: The NIST Cybersecurity Framework (CSF) 2.0

2.2 Σύγκριση NIST CSF 2.0 και Ευρωπαϊκών Προτύπων

Η σύγκριση μεταξύ του NIST CSF 2.0 και των ευρωπαϊκών προτύπων κυβερνοασφάλειας, ιδίως του NIS 2, αποτελεί κρίσιμο ζήτημα, καθώς αφορά τη συμμόρφωση οργανισμών που διαφέρουν λόγω γεωγραφικών και οργανωτικών απαιτήσεων. Το NIST CSF 2.0, το οποίο αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ, παρέχει ένα πλαίσιο για τη βελτίωση της ασφάλειας στον κυβερνοχώρο και είναι ειδικά προσαρμοσμένο στις ανάγκες των αμερικανικών οργανισμών. Αντίθετα, τα ευρωπαϊκά πρότυπα, όπως το NIS 2, επικεντρώνονται στην προστασία των κρίσιμων υποδομών και των παρόχων κρίσιμων υπηρεσιών εντός της ΕΕ, ενώ το NIST CSF 2.0 επικεντρώνεται στην ανάπτυξη ενός ευέλικτου πλαισίου που μπορεί να εφαρμοστεί από ένα ευρύ φάσμα οργανισμών, ανεξαρτήτως μεγέθους ή τομέα λειτουργίας. Το πλαίσιο περιλαμβάνει πέντε βασικούς τομείς (αναγνώριση, προστασία, ανίχνευση, απόκριση και ανάκαμψη) που καλύπτουν όλες τις πτυχές της ασφάλειας στον κυβερνοχώρο. Το πλαίσιο είναι ιδιαίτερα δημοφιλές στις ΗΠΑ, όπου οι οργανισμοί επιδιώκουν να βελτιώσουν τις ικανότητές τους στον τομέα της κυβερνοασφάλειας μέσω δομημένων και ευέλικτων εργαλείων (NIST, 2018).

Εν τω μεταξύ, η ΕΕ στοχεύει στην ενίσχυση της ασφάλειας στον κυβερνοχώρο σε κρίσιμους τομείς όπως η ενέργεια, οι μεταφορές, η υγεία και οι ψηφιακές υπηρεσίες μέσω της οδηγίας NIS 2. Η οδηγία NIS 2 εισάγει πιο αυστηρές υποχρεώσεις συμμόρφωσης και προβλέπει πιο αυστηρά μέτρα για την προστασία των δεδομένων και των συστημάτων που στηρίζουν αυτές τις κρίσιμες υποδομές.

Η εφαρμογή του NIST CSF 2.0 σε οργανισμούς των ΗΠΑ ήταν γενικά επιτυχής λόγω της ευελιξίας του πλαισίου και της δυνατότητάς του να προσαρμόζεται στις ειδικές ανάγκες κάθε οργανισμού. Ωστόσο, υπάρχουν και προκλήσεις που αντιμετωπίζουν οι οργανισμοί. Ειδικότερα, όσον αφορά την ανάγκη συνεχούς παρακολούθησης και αναθεώρησης για να διασφαλιστεί ότι οι πρακτικές συμμορφώνονται με τα κριτήρια του πλαισίου. Στην Ευρώπη, η συμμόρφωση με το NIS 2 αποτελεί επίσης πρόκληση, επειδή το NIST επιβάλλει διαφορετικές απαιτήσεις από το CSF 2.0. Οι ευρωπαϊκοί οργανισμοί οφείλουν όχι μόνο να διαχειρίζονται αυστηρότερες διαδικασίες ελέγχου και υποβολής εκθέσεων, αλλά και να διασφαλίζουν την τήρηση αυστηρών απαιτήσεων σχετικά με την προστασία των δεδομένων (NIST, 2018).

Το NIST CSF 2.0 και το NIS 2 καλύπτουν διαφορετικούς τύπους οργανισμών και έχουν διαφορετικές υποχρεώσεις- το NIST CSF 2.0 έχει ευρύτερη εφαρμογή και καλύπτει τόσο ιδιωτικούς όσο και δημόσιους οργανισμούς στις ΗΠΑ, με ιδιαίτερη έμφαση στους τομείς της ενέργειας, των χρηματοπιστωτικών υπηρεσιών και της υγειονομικής περίθαλψης. Αντίθετα, το NIS 2 επικεντρώνεται σε ευρωπαϊκούς φορείς εκμετάλλευσης υποδομών ζωτικής σημασίας, όπως οι φορείς παροχής ενέργειας, ύδρευσης, μεταφορών, υγειονομικής περίθαλψης και ψηφιακών υπηρεσιών. Οι υποχρεώσεις που απορρέουν από το NIS 2 είναι αυστηρότερες και απαιτούν από τους οργανισμούς να εφαρμόζουν ορισμένα μέτρα ασφαλείας και να είναι σε θέση να αποδεικνύουν τη συμμόρφωση μέσω τακτικών ελέγχων. Οι υποχρεώσεις αυτές περιλαμβάνουν την ανάπτυξη σχεδίου αντιμετώπισης κρίσεων, την εκπαίδευση του προσωπικού και την εφαρμογή κατάλληλων τεχνικών μέτρων για την προστασία των δεδομένων.

Η εφαρμογή του NIST CSF 2.0 στις ΗΠΑ αντιμετωπίζει προκλήσεις, ιδίως σε μικρότερους οργανισμούς που δεν διαθέτουν τους πόρους για να επενδύσουν σε προηγμένα μέτρα κυβερνοασφάλειας. Επιπλέον, η ανάγκη συνεχούς ενημέρωσης και βελτίωσης των μέτρων ασφαλείας μπορεί να είναι δαπανηρή. Οι οργανισμοί που επιθυμούν να συμμορφωθούν με τη NIS 2 στην Ευρώπη αντιμετωπίζουν προκλήσεις λόγω της πολυπλοκότητας των κανονιστικών απαιτήσεων και της ανάγκης συνεργασίας με διαφορετικά εθνικά και ευρωπαϊκά όργανα. Η έλλειψη εξειδικευμένου προσωπικού και πόρων αποτελεί επίσης σημαντική πρόκληση (ENISA, 2023).

Οι συγκρίσεις μεταξύ του NIST CSF 2.0 και ευρωπαϊκών προτύπων όπως το NIS 2 αποκαλύπτουν διαφορετικές προσεγγίσεις για την ασφάλεια στον κυβερνοχώρο και στις δύο πλευρές του Ατλαντικού: Το NIST CSF 2.0 προσφέρει μια πιο ευέλικτη και προσαρμόσιμη προσέγγιση, ενώ το NIS 2 επικεντρώνεται ειδικά στην προστασία των κρίσιμων υποδομών και επιβάλλει αυστηρότερες

υποχρεώσεις συμμόρφωσης. Οι οργανισμοί και στις δύο περιοχές πρέπει να ξεπεράσουν τις προκλήσεις που συνδέονται με την εφαρμογή αυτών των πλαισίων, επενδύοντας στην τεχνολογία, τους ανθρώπους και τις διαδικασίες για την οικοδόμηση ανθεκτικότητας έναντι των απειλών κυβερνοασφάλειας. Καθώς οι απειλές στον κυβερνοχώρο συνεχίζουν να εξελίσσονται και να γίνονται πιο εξελιγμένες στο μέλλον, η ανάγκη για διεθνή συνεργασία και εναρμόνιση των προτύπων κυβερνοασφάλειας θα γίνεται όλο και πιο επιτακτική. Η συνεργασία μεταξύ των Ηνωμένων Πολιτειών και της Ευρωπαϊκής Ένωσης για την ανάπτυξη κοινών προτύπων και κατευθυντήριων γραμμών αποτελεί σημαντικό βήμα προς αυτή την κατεύθυνση και θα μπορούσε να οδηγήσει σε αυξημένη παγκόσμια ασφάλεια (Wilson, 2020).

2.3 Παρουσιάσεις NIS 2

Η οδηγία NIS 2 (Network and Information Systems Directive 2) είναι η δεύτερη έκδοση της οδηγίας της Ευρωπαϊκής Ένωσης για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Η οδηγία αποσκοπεί στην ενίσχυση της ασφάλειας των δικτύων και των συστημάτων πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση με την αντιμετώπιση των αυξανόμενων απειλών για την ασφάλεια στον κυβερνοχώρο και τη βελτίωση της συνεργασίας μεταξύ των κρατών μελών (Schmidt et al.)

Η οδηγία 2 για τα δίκτυα και τα συστήματα πληροφοριών (NIS2) είναι μια αναθεωρημένη έκδοση της αρχικής οδηγίας NIS που εγκρίθηκε από την Ευρωπαϊκή Ένωση το 2016. Η NIS2 αποσκοπεί στη βελτίωση του επιπέδου της ασφάλειας στον κυβερνοχώρο στην Ευρωπαϊκή Ένωση για την αντιμετώπιση των αυξανόμενων και εξελισσόμενων απειλών στον κυβερνοχώρο. Η παρούσα έκθεση εξηγεί το ιστορικό, τους στόχους, τη δομή, τις απαιτήσεις και τον αντίκτυπο της NIS2. Η πρώτη οδηγία για τα συστήματα δικτύων και πληροφοριών (NIS) εκδόθηκε το 2016 και αποτελεί την πρώτη πανευρωπαϊκή νομοθεσία που αποσκοπεί στην επίτευξη υψηλού κοινού επιπέδου ασφάλειας για τα δίκτυα και τα συστήματα πληροφοριών. Η πρώτη οδηγία απαιτούσε από τα κράτη μέλη να αναπτύξουν εθνικές στρατηγικές για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών, να προσδιορίσουν τους φορείς εκμετάλλευσης κρίσιμων υποδομών και να συστήσουν ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT). Με την πάροδο του χρόνου, οι τεχνολογικές εξελίξεις και οι αυξανόμενες απειλές στον κυβερνοχώρο οδήγησαν στην ανάγκη αναθεώρησης της αρχικής οδηγίας και η NIS2 αποσκοπεί στην αντιμετώπιση των κενών και των αδυναμιών της αρχικής οδηγίας, θέτοντας αυστηρότερες και σαφέστερες απαιτήσεις για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών (Schmidt et al., 2021).

Η NIS2 έχει διάφορους στόχους που επικεντρώνονται στη βελτίωση της ασφάλειας στον κυβερνοχώρο σε ολόκληρη την ΕΕ.

Οι βασικοί στόχοι περιλαμβάνουν:

1. **Αύξηση της ανθεκτικότητας των υποδομών ζωτικής σημασίας**: Η NIS2 αποσκοπεί στην αύξηση της ανθεκτικότητας των υποδομών ζωτικής σημασίας για την οικονομία και την κοινωνία, όπως η υγειονομική περίθαλψη, οι μεταφορές, η ενέργεια και οι τράπεζες.

2. **Ενισχυμένη συνεργασία και συντονισμός**: Η οδηγία προωθεί τη συνεργασία και τον συντονισμό μεταξύ των κρατών μελών της ΕΕ για την αποτελεσματική αντιμετώπιση απειλών και περιστατικών ασφάλειας στον κυβερνοχώρο.

3. **Ενισχυμένη ασφάλεια της αλυσίδας εφοδιασμού**: Η NIS2 αποσκοπεί να συμβάλει στη συνολική ασφάλεια της αλυσίδας εφοδιασμού, διασφαλίζοντας ότι οι προμηθευτές και οι τρίτοι πάροχοι υπηρεσιών συμμορφώνονται με τις απαιτήσεις ασφαλείας.

4. **Ενισχυμένη διαφάνεια και λογοδοσία**: Η οδηγία εισάγει μέτρα για την αύξηση της διαφάνειας και της λογοδοσίας των βασικών φορέων εκμετάλλευσης και των παρόχων υπηρεσιών σε σχέση με την ασφάλεια των συστημάτων δικτύου και πληροφοριών (Schmidt et al., 2021).

Η NIS2 εμπεριέχει διάφορα άρθρα και παραρτήματα που ορίζουν τις απαιτήσεις και τις υποχρεώσεις για τα κράτη μέλη και τους φορείς κρίσιμης σημασίας.

Τα βασικά σημεία της οδηγίας περιλαμβάνουν:

- **Καθορισμός κρίσιμων φορέων και παρόχων υπηρεσιών**

Η NIS2 διευρύνει τον ορισμό των κρίσιμων φορέων ώστε να συμπεριλάβει περισσότερους τομείς και υποτομείς, όπως η υγεία, το νερό, οι ψηφιακές υποδομές και οι πάροχοι δημόσιων υπηρεσιών. Απαιτεί επίσης από τα κράτη μέλη να προσδιορίσουν τους κρίσιμους φορείς και τους παρόχους ψηφιακών υπηρεσιών που καλύπτονται από τις απαιτήσεις τους.

- **Εθνικές Στρατηγική ασφάλειας**

Τα κράτη μέλη θα πρέπει να αναπτύξουν και να εφαρμόσουν εθνικές στρατηγικές για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών. Οι στρατηγικές αυτές θα πρέπει να περιλαμβάνουν μέτρα για την πρόληψη, τον εντοπισμό και την αντιμετώπιση των απειλών στον κυβερνοχώρο.

- **Ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT)**

Η NIS2 απαιτεί από τα κράτη μέλη να ιδρύουν ή να διατηρούν CSIRT για την αντιμετώπιση περιστατικών ασφάλειας- οι CSIRT πρέπει να έχουν την ικανότητα να εντοπίζουν, να αναλύουν και να ανταποκρίνονται σε περιστατικά ασφάλειας με συντονισμένο και αποτελεσματικό τρόπο.

- **Διαχείριση Αναφορά κινδύνων και συμβάντων**

Οι κρίσιμοι φορείς εκμετάλλευσης και οι πάροχοι ψηφιακών υπηρεσιών υποχρεούνται να εφαρμόζουν μέτρα διαχείρισης κινδύνου και να αναφέρουν σοβαρά περιστατικά ασφάλειας στις αρμόδιες αρχές Η NIS2 ορίζει πρότυπα και διαδικασίες αναφοράς περιστατικών που πρέπει να ακολουθούνται.

Οι απαιτήσεις της NIS2 είναι πιο αυστηρές και σαφείς σε σύγκριση με την αρχική οδηγία. Αυτές οι απαιτήσεις περιλαμβάνουν:

- **Μέτρα ασφάλειας**

Οι φορείς κρίσιμης σημασίας και οι πάροχοι ψηφιακών υπηρεσιών υποχρεούνται να εφαρμόζουν τεχνικά και οργανωτικά μέτρα για την αντιμετώπιση των κινδύνων ασφάλειας. Αυτά τα μέτρα περιλαμβάνουν:

- ✓ **Προστασία Δεδομένων**: Μέτρα για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση, και απώλεια.
- ✓ **Πρόληψη και ανίχνευση απειλών**: Μέτρα για την πρόληψη και την ανίχνευση των απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων των κακόβουλων λογισμικών και των επιθέσεων από τρίτους.
- ✓ **Ανταπόκριση και Ανάκτηση:** Μέτρα για την ανταπόκριση στα περιστατικά ασφάλειας και την αποκατάσταση των υπηρεσιών μετά από ένα περιστατικό.

- **Αναφορά περιστατικών**

Η NIS2 απαιτεί από τους φορείς κρίσιμης σημασίας και τους παρόχους ψηφιακών υπηρεσιών να αναφέρουν τα σημαντικά περιστατικά ασφάλειας στις αρμόδιες αρχές εντός συγκεκριμένου χρονικού πλαισίου. Η αναφορά πρέπει να περιλαμβάνει πληροφορίες για τη φύση του περιστατικού, τις επιπτώσεις, και τα μέτρα που έχουν ληφθεί για την αντιμετώπιση του.

- **Ενίσχυση της συνεργασίας**

Η NIS2 προωθεί τη συνεργασία μεταξύ των κρατών μελών και των αρμόδιων αρχών για την αντιμετώπιση των απειλών στον κυβερνοχώρο. Αυτή η συνεργασία περιλαμβάνει την ανταλλαγή πληροφοριών, τη συντονισμένη ανταπόκριση σε περιστατικά, και την ανάπτυξη κοινών στρατηγικών και πολιτικών για την ασφάλεια των δικτύων και των πληροφοριακών συστημάτων (Van Hecke et al., 2022).

Η εφαρμογή της NIS2 αναμένεται να έχει σημαντικό αντίκτυπο στους φορείς εκμετάλλευσης κρίσιμης σημασίας, στους παρόχους ψηφιακών υπηρεσιών και στα κράτη μέλη της ΕΕ. Οι φορείς

εκμετάλλευσης κρίσιμης σημασίας και οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να ενισχύσουν τα μέτρα ασφαλείας για τα δίκτυα και τα συστήματα πληροφοριών τους ώστε να συμμορφωθούν με τις απαιτήσεις της NIS2. Αυτό μπορεί να απαιτήσει επενδύσεις σε νέες τεχνολογίες, αναβάθμιση των υφιστάμενων συστημάτων και εκπαίδευση του προσωπικού σε θέματα ασφάλειας στον κυβερνοχώρο. Τα κράτη μέλη θα πρέπει να αναπτύξουν και να εφαρμόσουν εθνικές στρατηγικές για την ασφάλεια των δικτύων και των συστημάτων πληροφοριών. Θα πρέπει επίσης να δημιουργήσουν ή να ενισχύσουν τις CSIRT και να διασφαλίσουν τη συνεργασία και τον συντονισμό μεταξύ των αρμόδιων αρχών. Η εφαρμογή της NIS2 θα συμβάλει στην ενίσχυση της ασφάλειας των δικτύων και των συστημάτων πληροφοριών σε ολόκληρη την ΕΕ, δημιουργώντας ένα ασφαλέστερο και πιο αξιόπιστο ψηφιακό περιβάλλον. Η οδηγία αναμένεται επίσης να αυξήσει την εμπιστοσύνη των πολιτών και των επιχειρήσεων στις ψηφιακές υπηρεσίες και να τονώσει την ψηφιακή καινοτομία και την οικονομική ανάπτυξη (Korff et al. 2021)

Η οδηγία για τα συστήματα δικτύων και πληροφοριών 2 (NIS2) αποτελεί μια βασική πρόοδο προς την ενίσχυση της ασφάλειας των δικτύων και των συστημάτων πληροφοριών στην Ευρωπαϊκή Ένωση (ΕΕ). Με αυστηρότερες απαιτήσεις και σαφείς κατευθυντήριες γραμμές, η NIS2 αποσκοπεί στην αύξηση της ανθεκτικότητας των υποδομών ζωτικής σημασίας, στη βελτίωση της συνεργασίας μεταξύ των κρατών μελών και στην ενίσχυση της ασφάλειας της αλυσίδας εφοδιασμού. Αναμένεται να έχει σημαντικές επιπτώσεις. Παρά τις προκλήσεις που ενδέχεται να προκύψουν κατά την εφαρμογή, τα οφέλη από την υιοθέτηση της NIS2 είναι σημαντικά και θα συμβάλουν στη δημιουργία ενός πιο ασφαλούς και αξιόπιστου ψηφιακού περιβάλλοντος στην Ευρώπη. Η οδηγία NIS2, με τις βελτιώσεις και τις καινοτομίες της, είναι ένα ισχυρό εργαλείο για την αντιμετώπιση των σημερινών προκλήσεων της κυβερνοασφάλειας και την προστασία των δικτύων και των συστημάτων πληροφοριών από τις συνεχώς εξελισσόμενες απειλές στον κυβερνοχώρο (Korff et al. 2021).

2.3.1 Βασικά στοιχεία του NIS 2

Τα βασικά στοιχεία του NIS 2 διαφοροποιούνται και αφορούν συγκεκριμένες λειτουργίες. Αρχικά, θα πρέπει να γίνει λόγος για την ενίσχυση της ανθεκτικότητας. Η οδηγία NIS 2 αποσκοπεί στην ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών και των βασικών υπηρεσιών που παρέχονται μέσω δικτύων και πληροφοριακών συστημάτων. Προάγει την ανθεκτικότητα των κρίσιμων υποδομών και των βασικών υπηρεσιών, διασφαλίζοντας την αδιάλειπτη παροχή τους ακόμα και σε περίπτωση περιστατικών κυβερνοασφάλειας. Εξίσου σημαντική είναι και η διαχείριση κινδύνων. Προβλέπει την εφαρμογή μέτρων διαχείρισης κινδύνων και την ανάπτυξη σχεδίων ανταπόκρισης σε περιστατικά κυβερνοασφάλειας. Η εφαρμογή μέτρων διαχείρισης κινδύνων βοηθά τους οργανισμούς να

αναγνωρίσουν, να αξιολογήσουν και να διαχειριστούν τις απειλές κυβερνοασφάλειας, μειώνοντας την πιθανότητα και τον αντίκτυπο των περιστατικών.

Η συνεργασία και συντονισμός είναι ακόμη ένα σημαντικό στοιχείο. Προωθεί τη συνεργασία και τον συντονισμό μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης, διασφαλίζοντας την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών. Η ενίσχυση της συνεργασίας και του συντονισμού μεταξύ των κρατών μελών ενισχύει την συνολική ασφάλεια και την ανταπόκριση σε περιστατικά κυβερνοασφάλειας. Όσον αφορά τις υποχρεώσεις αναφοράς μπορεί να ειπωθεί πως εισάγει υποχρεώσεις αναφοράς για τους φορείς εκμετάλλευσης βασικών υπηρεσιών και τους παρόχους ψηφιακών υπηρεσιών σε περίπτωση περιστατικών κυβερνοασφάλειας που επηρεάζουν τις υπηρεσίες τους. Τέλος, κρίνεται αναγκαίο να γίνει λόγος και για τις κυρώσεις για μη συμμόρφωση. Προβλέπει αυστηρές κυρώσεις για τους οργανισμούς που δεν συμμορφώνονται με τις απαιτήσεις της οδηγίας, ενισχύοντας έτσι τη συμμόρφωση και τη λογοδοσία. Η επιβολή κυρώσεων για τη μη συμμόρφωση ενισχύει την υπευθυνότητα και την εφαρμογή των απαραίτητων μέτρων προστασίας από τους οργανισμούς (Maitland et al., 2021).

2.3.2 Κύριες διατάξεις του NIS 2

Οι κύριες διατάξεις του NIS 2 υπόκεινται στα ακόλουθα:

- **Πεδίο εφαρμογής**:

Η οδηγία NIS 2 μπορεί να εφαρμοστεί σε φορείς αξιοποίησης κύριων υπηρεσιών και σε παρόχους ψηφιακών υπηρεσιών. Οι κύριες υπηρεσίες εμπεριέχουν κλάδους, όπως η ενέργεια, οι μεταφορές, η υγεία, οι χρηματοπιστωτικές υπηρεσίες, η υδροδότηση και οι ψηφιακές υποδομές.

- **Εκτίμηση και διαχείριση κινδύνων**:

Οι οργανισμοί που εναπόκεινται στο πεδίο εφαρμογής της οδηγίας έχουν την υποχρέωση να εκτιμούν και να διαχειρίζονται τους κινδύνους κυβερνοασφάλειας, μέσα από την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων.

- **Αναφορά περιστατικών**:

Οι οργανισμοί έχουν την υποχρέωση να αναφέρουν περιστατικά κυβερνοασφάλειας στις υπεύθυνες αρχές, ακολουθώντας καθορισμένες διαδικασίες και χρονικά πλαίσια.

- **Συνεργασία και πληροφόρηση:**

Η οδηγία προβλέπει τη δημιουργία μηχανισμών συνεργασίας και πληροφόρησης μεταξύ των κρατών μελών, ενισχύοντας την ανταλλαγή πληροφοριών και βέλτιστων πρακτικών (Maitland et al., 2021).

2.4 Σύγκριση NIST CSF 2.0 και NIS 2

Η σύγκριση μεταξύ NIST Cybersecurity Framework 2.0 και NIS 2 παρουσιάζει τόσο ομοιότητες όσο και διαφορές μεταξύ των δύο προσεγγίσεων:

- **Εστίαση και πεδίο εφαρμογής**

Το NIST CSF 2.0 αποτελεί ένα πλαίσιο που έχει τη δυνατότητα να εφαρμοστεί σε οποιονδήποτε οργανισμό, ανεξάρτητα από το μέγεθος ή τον τομέα δραστηριότητάς του, ενώ το NIS 2 έχει περιορισμένο πεδίο εφαρμογής σε φορείς εκμετάλλευσης βασικών υπηρεσιών και παρόχους ψηφιακών υπηρεσιών στην Ευρωπαϊκή Ένωση.

- **Διαχείριση κινδύνων**

Και τα δύο πλαίσια δίνουν έμφαση στη σημασία της διαχείρισης κινδύνων, παρέχοντας καθοδήγηση για την αναγνώριση, την αξιολόγηση και τη διαχείριση των απειλών κυβερνοασφάλειας.

- **Συνεργασία και πληροφόρηση**

Το NIS 2 τονίζει τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης, ενώ το NIST CSF 2.0 δίνει μεγαλύτερη βαρύτητα στην εσωτερική διαχείριση των κινδύνων και στην εφαρμογή βέλτιστων πρακτικών.

- **Υποχρεώσεις και κυρώσεις**

Το NIS 2 περιλαμβάνει υποχρεώσεις και κυρώσεις για τη μη συμμόρφωση, ενώ το NIST CSF 2.0 παρέχει έναν οδηγό για την εθελοντική εφαρμογή των βέλτιστων πρακτικών.

Συνοπτικά, τόσο το Πλαίσιο NIST για την ασφάλεια στον κυβερνοχώρο 2.0 όσο και το NIS 2 παρέχουν σημαντικές κατευθυντήριες γραμμές και βέλτιστες πρακτικές για τη διαχείριση των κινδύνων στον κυβερνοχώρο. Η επιλογή της κατάλληλης προσέγγισης εξαρτάται από τις ανάγκες και τα

χαρακτηριστικά του οργανισμού, καθώς και από τις απαιτήσεις του κανονιστικού πλαισίου στο οποίο δραστηριοποιείται (Golling et al.)

Για να εκτιμηθεί ποιοι οργανισμοί είναι σχετικοί με το πλαίσιο NIST Cybersecurity Framework (CSF) 2.0 και ποιες υποχρεώσεις έχουν, είναι σημαντικό να κατανοηθεί το πεδίο εφαρμογής και οι λεπτομέρειες του εν λόγω πλαισίου και να συγκριθούν αυτές οι εκτιμήσεις με την οδηγία NIS 2 της Ευρωπαϊκής Ένωσης, η οποία έχει διαφορετικές απαιτήσεις και πεδίο εφαρμογής.

Το NIST CSF 2.0 σχεδιάστηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) για να βοηθήσει τους οργανισμούς να διαχειριστούν και να μετριάσουν τους κινδύνους κυβερνοασφάλειας. Αρχικά απευθυνόταν σε κρίσιμες υποδομές, όπως οι εταιρείες ενέργειας, η υγειονομική περίθαλψη και τα χρηματοπιστωτικά ιδρύματα, αλλά η ευελιξία του πλαισίου το καθιστά κατάλληλο για κάθε οργανισμό, ανεξαρτήτως μεγέθους, τομέα ή γεωγραφίας.

Οι φορείς που αφορά το NIST CSF 2.0 είναι οι εξής:

1. **Κρίσιμες υποδομές**: Οι οργανισμοί που διαχειρίζονται κρίσιμες υποδομές, όπως η παροχή ενέργειας, η παροχή νερού, η υγειονομική περίθαλψη και οι μεταφορές, θα είναι οι πρώτοι που θα επωφεληθούν από το ΚΠΣ NIST. Η ασφάλεια αυτών των υποδομών είναι ζωτικής σημασίας για την εθνική ασφάλεια και τη δημόσια υγεία.

2. **Χρηματοπιστωτικά Ιδρύματα**: Ο χρηματοπιστωτικός τομέας έχει υιοθετήσει από νωρίς το CSF NIST, καθώς είναι σημαντικό να διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των δεδομένων για την προστασία των χρηματοπιστωτικών συναλλαγών και των πελατών.

3. **Οργανισμοί υγειονομικής περίθαλψης**: Οι οργανισμοί υγειονομικής περίθαλψης, όπως τα νοσοκομεία και οι κλινικές, χρησιμοποιούν αυτό το πλαίσιο για την προστασία των ευαίσθητων ιατρικών δεδομένων των ασθενών και τη διασφάλιση της ομαλής λειτουργίας των πληροφοριακών τους συστημάτων.

4. **Τεχνολογικές Εταιρείες**: Οι εταιρείες στον κλάδο της πληροφορικής και της τεχνολογίας αξιοποιούν το NIST CSF για να εξασφαλίσουν πως τα συστήματα και τα προϊόντα τους είναι ασφαλή και συμμορφώνονται με τα διεθνή πρότυπα κυβερνοασφάλειας.

5. **Μικρομεσαίες επιχειρήσεις**: Το NIST CSF είναι επίσης αρμόδιο για μικρομεσαίες επιχειρήσεις που, αν και έχουν λιγότερους πόρους, έχουν τη δυνατότητα να προσαρμόσουν το πλαίσιο στις ανάγκες τους για να ενισχύσουν την ασφάλειά τους (NIST, 2018).

Το NIST CSF 2.0 είναι κατ' αρχήν ένα εθελοντικό πλαίσιο. Παρόλο που δεν υπάρχει νομική απαίτηση για τους οργανισμούς να υιοθετήσουν αυτό το πλαίσιο, πολλοί οργανισμοί το έχουν υιοθετήσει είτε για να συμμορφωθούν με τις απαιτήσεις των πελατών τους είτε ως μέρος της στρατηγικής τους για την ασφάλεια στον κυβερνοχώρο, προκειμένου να βελτιώσουν την ασφάλεια των

συστημάτων τους. Οι βασικές υποχρεώσεις των οργανισμών που επιλέγουν να υιοθετήσουν το CSF του NIST είναι οι εξής:

1. Ο οργανισμός πρέπει να αξιολογεί τους κινδύνους κυβερνοασφάλειας στους οποίους εκτίθεται και να οργανώνει τις δραστηριότητές του για την αντιμετώπιση των κινδύνων αυτών.

2. Ο οργανισμός θα πρέπει να διασφαλίσει ότι οι υπάλληλοί του είναι εκπαιδευμένοι και ενήμεροι για τις απειλές της κυβερνοασφάλειας και την πολιτική ασφάλειας του οργανισμού.

3. Οι οργανισμοί πρέπει να εφαρμόζουν τεχνικούς και διοικητικούς ελέγχους για την προστασία των συστημάτων ΤΠ τους. Οι έλεγχοι αυτοί περιλαμβάνουν μέτρα προστασίας του δικτύου, κρυπτογράφησης και ελέγχου πρόσβασης.

4. Το CSF του NIST τονίζει τη σημασία της συνεχούς παρακολούθησης των απειλών και της βελτίωσης των ελέγχων ασφαλείας για την προσαρμογή στις νέες προκλήσεις.

5. Οι οργανισμοί πρέπει να ορίσουν ορισμένες ενέργειες για την αναφορά περιστατικών ασφαλείας και την επικοινωνία με τα ενδιαφερόμενα μέρη, όπως οι πελάτες, οι συνεργάτες και οι ρυθμιστικές αρχές (NIST, 2018).

Παρά το γεγονός πως, το NIST CSF 2.0 και η οδηγία NIS 2 έχουν τον κοινό στόχο της βελτίωσης της ασφάλειας δικτύων και πληροφοριών, διαφέρουν σημαντικά ως προς το πεδίο εφαρμογής, τη φύση των υποχρεώσεων και τις νομικές απαιτήσεις Το NIST CSF 2.0 είναι ένα ευέλικτο, εθελοντικό πλαίσιο που μπορεί να προσαρμοστεί στις ανάγκες κάθε οργανισμού. Αντίθετα, η οδηγία NIS 2 επιβάλλει νομικές υποχρεώσεις σε συγκεκριμένους οργανισμούς και θέτει αυστηρές απαιτήσεις συμμόρφωσης- το NIST CSF 2.0 μπορεί να εφαρμοστεί σε οποιονδήποτε οργανισμό, ενώ η οδηγία NIS 2 επικεντρώνεται σε συγκεκριμένους τομείς κρίσιμων υποδομών και ψηφιακών υπηρεσιών- η μη συμμόρφωση με την οδηγία NIS 2 μπορεί να οδηγήσει σε νομικές κυρώσεις και πρόστιμα, ενώ η μη εφαρμογή του NIST CSF 2.0 δεν έχει άμεσες νομικές συνέπειες, αλλά μπορεί να αυξήσει τον κίνδυνο κυβερνοεπιθέσεων και την απώλεια εμπιστοσύνης από πελάτες και συνεργάτες. Κατά συνέπεια, οι εταιρείες που υπάγονται στο NIST CSF 2.0 έχουν την ευελιξία να προσαρμόσουν το πλαίσιο στις ανάγκες τους, ενώ εκείνες που υπάγονται στην οδηγία NIS 2 πρέπει να συμμορφώνονται με συγκεκριμένες και δεσμευτικές απαιτήσεις. Και τα δύο πλαίσια παρέχουν σημαντικά εργαλεία για την ενίσχυση της ασφάλειας στον κυβερνοχώρο, αλλά οι οργανισμοί πρέπει να κατανοήσουν τις διαφορές και να επιλέξουν αυτό που ταιριάζει καλύτερα στις ανάγκες τους (Stallings, 2020).

Κεφάλαιο 3ο: Ελληνική πραγματικότητα

3.1 Επισκόπηση της κυβερνοασφάλειας στην Ελλάδα

Η κυβερνοασφάλεια στην Ελλάδα έχει καταστεί σημαντικό ζήτημα τα τελευταία χρόνια λόγω της συνεχούς αύξησης των κυβερνοεπιθέσεων και της αυξανόμενης εξάρτησης των δημόσιων οργανισμών από την τεχνολογία. Η Ελλάδα, όπως και άλλες χώρες, αντιμετωπίζει προκλήσεις στην εφαρμογή ισχυρών και αποτελεσματικών μέτρων κυβερνοασφάλειας, ιδίως σε δημόσιους οργανισμούς, όπου η διασφάλιση της ασφάλειας των δεδομένων και των συστημάτων είναι απαραίτητη για την προστασία της εθνικής ασφάλειας και της δημόσιας τάξης. Η υιοθέτηση διεθνών προτύπων και πλαισίων, όπως το Πλαίσιο Κυβερνοασφάλειας (CSF) του NIST, αποτελεί ένα βήμα προς τη σωστή κατεύθυνση για την ενίσχυση της εθνικής κυβερνοασφάλειας. Ωστόσο, η πραγματικότητα στην Ελλάδα χαρακτηρίζεται από διάφορους παράγοντες που επηρεάζουν την αποτελεσματική εφαρμογή των προτύπων αυτών. Στους παράγοντες αυτούς περιλαμβάνονται η περιορισμένη χρηματοδότηση, η έλλειψη εξειδικευμένου προσωπικού, η ανεπαρκής τεχνογνωσία και η αντίσταση στην αλλαγή (Παπαδόπουλος, 2022).

3.2 Υφιστάμενη νομοθεσία και πολιτικές κυβερνοασφάλειας

Η ελληνική κυβέρνηση έχει εργαστεί για την ενίσχυση της νομοθεσίας και των πολιτικών της για την ασφάλεια στον κυβερνοχώρο, ιδίως μέσω της εναρμόνισης με τις ευρωπαϊκές οδηγίες, όπως η οδηγία για την ασφάλεια δικτύων και πληροφοριών (NIS) και η επικαιροποιημένη NIS 2. Η οδηγία NIS 2 αποσκοπεί στην ενίσχυση της ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση. Αποσκοπεί στην επιβολή αυστηρότερων απαιτήσεων στους δημόσιους οργανισμούς και στις υποδομές ζωτικής σημασίας, επιβάλλοντας την υιοθέτηση και εφαρμογή προτύπων όπως το CSF του NIST. Παρά τις προσπάθειες αυτές, εξακολουθούν να υπάρχουν προβλήματα στην εφαρμογή των πολιτικών ασφάλειας. Οι δημόσιοι οργανισμοί δυσκολεύονται να προσαρμοστούν στις νέες κανονιστικές απαιτήσεις, κυρίως λόγω έλλειψης πόρων και χρόνου για την υλοποίηση των απαραίτητων αλλαγών (ΣΕΠΕ, 2021).

3.3 Δομές και διαδικασίες για την κυβερνοασφάλεια στους δημόσιους οργανισμούς

Η επιτυχής εφαρμογή της κυβερνοασφάλειας στους δημόσιους οργανισμούς απαιτεί την ύπαρξη θεσμικών δομών και διαδικασιών. Στην Ελλάδα, ωστόσο, συχνά απουσιάζει ο κεντρικός συντονισμός

και η καθοδήγηση, με αποτέλεσμα την αποσπασματική και άνιση εφαρμογή των πολιτικών ασφάλειας. Πολλοί δημόσιοι οργανισμοί δεν διαθέτουν ειδικά τμήματα ασφάλειας πληροφοριών και το προσωπικό ασφαλείας συχνά δεν λαμβάνει επαρκή εκπαίδευση ή υποστήριξη. Αυτό δημιουργεί σοβαρά τρωτά σημεία και αυξάνει την πιθανότητα επιτυχών επιθέσεων. Οι προκλήσεις που αντιμετωπίζουν οι ελληνικοί δημόσιοι οργανισμοί για την εφαρμογή μιας αποτελεσματικής πολιτικής ασφάλειας στον κυβερνοχώρο είναι πολλαπλές. Εκτός από τα προαναφερθέντα προβλήματα, η κουλτούρα ασφάλειας των δημόσιων οργανισμών παραμένει αδύναμη. Σε πολλές περιπτώσεις, η ασφάλεια στον κυβερνοχώρο αποτελεί ευθύνη του τμήματος πληροφορικής και δεν θεωρείται κοινή ευθύνη όλων των εργαζομένων (ENISA, 2023).

Ταυτόχρονα, οι τεχνολογίες και τα εργαλεία που χρησιμοποιούν οι οργανισμοί είναι συχνά ξεπερασμένα, γεγονός που καθιστά δύσκολη την εφαρμογή σύγχρονων μέτρων ασφαλείας. Η έλλειψη ευαισθητοποίησης και κατάρτισης των εργαζομένων είναι ένας άλλος παράγοντας που αυξάνει την έκθεση ενός οργανισμού σε απειλές. Παρά τις προκλήσεις, υπάρχουν επίσης ευκαιρίες για βελτίωση: Η σταδιακή ενσωμάτωση ευρωπαϊκών κανονισμών, όπως η οδηγία NIS 2, παρέχει ένα πλαίσιο για τη βελτίωση της ασφάλειας. Η συνεργασία και η ανταλλαγή βέλτιστων πρακτικών μεταξύ των δημόσιων αρχών και του ιδιωτικού τομέα μπορεί να συμβάλει στην ενίσχυση των καθεστώτων και των διαδικασιών ασφαλείας. Επιπλέον, οι επενδύσεις στην ανάπτυξη και την κατάρτιση εξειδικευμένου προσωπικού είναι απαραίτητες για την επιτυχή εφαρμογή των πολιτικών ασφάλειας στον κυβερνοχώρο (Παπαδόπουλος, 2022).

3.4 Νέες τεχνολογίες και κυβερνοασφάλεια στην Ελλάδα

Η ταχεία ανάπτυξη τεχνολογιών όπως το 5G, το Διαδίκτυο των πραγμάτων (IoT) και η τεχνητή νοημοσύνη (AI), σε συνδυασμό με την ψηφιοποίηση των δημόσιων υπηρεσιών, αυξάνει την πολυπλοκότητα των απειλών για την ασφάλεια στον κυβερνοχώρο. Η σταδιακή υιοθέτηση αυτών των τεχνολογιών στην Ελλάδα επιφέρει νέες προκλήσεις και την ανάγκη ενίσχυσης των δομών και διαδικασιών κυβερνοάμυνας, ιδίως σε δημόσιους οργανισμούς που διαχειρίζονται κρίσιμα δεδομένα και παρέχουν σημαντικές υπηρεσίες στην κοινωνία (NIST, 2023).

3.4.1 Το 5G και οι επιπτώσεις του στην κυβερνοασφάλεια

Ενώ το 5G προσφέρει άνευ προηγουμένου δυνατότητες επικοινωνίας και συνδεσιμότητας, φέρνει επίσης νέες επιθέσεις, όπως αυτές που στοχεύουν κρίσιμες υποδομές μέσω του κυβερνοπολέμου και της επιτήρησης δεδομένων. Η Ελλάδα έχει ξεκινήσει τη μετάβαση σε δίκτυα 5G, τα οποία μπορούν

να βοηθήσουν τους δημόσιους οργανισμούς να εξελιχθούν προς πιο διασυνδεδεμένες και αποτελεσματικές λειτουργίες. Ωστόσο, η φύση του 5G, με την αποκεντρωμένη δικτυακή υποδομή του, επιτρέπει σε κακόβουλους χρήστες να αποκτήσουν πρόσβαση σε κόμβους δικτύου, θέτοντας σε κίνδυνο τον έλεγχο και την ασφάλεια των πληροφοριακών συστημάτων. Οι ελληνικές δημόσιες αρχές πρέπει να αναπτύξουν νέες προσεγγίσεις για τη διαχείριση της κυβερνοασφάλειας, όπως η ενσωμάτωση της κρυπτογραφίας και η χρήση κατανεμημένων συστημάτων για τη διασφάλιση της ακεραιότητας του δικτύου. Πρέπει επίσης να καθιερώσουν πρωτόκολλα για την παρακολούθηση της κίνησης δεδομένων και να ενημερώνουν συνεχώς τα συστήματα ασφαλείας τους.

Η χρήση συσκευών IoT στους δημόσιους οργανισμούς έχει αυξηθεί δραματικά, καθώς προσφέρουν βελτιωμένες δυνατότητες για τη συλλογή δεδομένων, την παρακολούθηση περιουσιακών στοιχείων και τη διαχείριση πόρων. Ωστόσο, οι συσκευές αυτές, που συχνά δεν είναι πλήρως ασφαλισμένες, ανοίγουν την πόρτα σε νέες επιθέσεις. Καθώς οι συσκευές IoT έχουν μικρή υπολογιστική ισχύ και συχνά περιορισμένες δυνατότητες ενημέρωσης ασφαλείας, αποτελούν εύκολο στόχο για κυβερνοεγκληματίες. Στην Ελλάδα, οι δημόσιοι οργανισμοί που υιοθετούν IoT τεχνολογίες πρέπει να αντιμετωπίσουν σημαντικά προβλήματα ασφάλειας, όπως την αποτροπή μη εξουσιοδοτημένης πρόσβασης και την προστασία των δεδομένων που διακινούνται μέσω αυτών των συσκευών. Οι επιθέσεις Denial of Service (DoS) ή Man-in-the-Middle μπορούν να υπονομεύσουν τη λειτουργία ζωτικών υπηρεσιών, όπως η διαχείριση των υδάτων ή της ηλεκτρικής ενέργειας. Η προστασία αυτών των συσκευών απαιτεί τη χρήση σύγχρονων τεχνολογιών όπως οι ασφαλείς πύλες (gateways), που ελέγχουν την κυκλοφορία δεδομένων, και την ενσωμάτωση ελέγχου ταυτότητας (RiskLens, 2023).

Η χρήση συσκευών IoT σε δημόσιους οργανισμούς έχει αυξηθεί σημαντικά λόγω των βελτιωμένων δυνατοτήτων στη συλλογή δεδομένων, την παρακολούθηση περιουσιακών στοιχείων και τη διαχείριση πόρων. Ωστόσο, οι συσκευές αυτές συχνά δεν είναι αρκετά ασφαλείς και ανοίγουν την πόρτα σε νέες επιθέσεις. Οι συσκευές IoT έχουν συχνά χαμηλή υπολογιστική ισχύ και περιορισμένες δυνατότητες ενημέρωσης της ασφάλειας, γεγονός που τις καθιστά πρωταρχικούς στόχους για τους εγκληματίες του κυβερνοχώρου. Οι δημόσιες αρχές που υιοθετούν τεχνολογίες IoT στην Ελλάδα πρέπει να αντιμετωπίσουν κρίσιμα ζητήματα ασφάλειας, όπως η αποτροπή μη εξουσιοδοτημένης πρόσβασης και η προστασία των δεδομένων που διακινούνται μέσω αυτών των συσκευών. Οι επιθέσεις άρνησης παροχής υπηρεσιών (DoS) και οι επιθέσεις man-in-the-middle μπορούν να υπονομεύσουν τη λειτουργία κρίσιμων υπηρεσιών, όπως η διαχείριση του νερού και της ηλεκτρικής ενέργειας. Η προστασία αυτών των συσκευών απαιτεί τη χρήση σύγχρονων τεχνολογιών, όπως οι ασφαλείς πύλες και η ολοκληρωμένη αυθεντικοποίηση για τον έλεγχο της κυκλοφορίας δεδομένων (RiskLens, 2023).

3.4.2 Τεχνητή νοημοσύνη: Ευκαιρίες και κίνδυνοι

Η τεχνητή νοημοσύνη (AI) προσφέρει νέα εργαλεία για τη βελτίωση της ασφάλειας, επιτρέποντας την αυτόματη ανίχνευση απειλών και τον εντοπισμό ύποπτων δραστηριοτήτων σε πραγματικό χρόνο. Στην Ελλάδα, τα συστήματα τεχνητής νοημοσύνης έχουν αρχίσει να χρησιμοποιούνται από δημόσιους οργανισμούς για τη βελτίωση της ασφάλειας στον κυβερνοχώρο, ιδίως με την πρόβλεψη πιθανών επιθέσεων και τη λήψη προληπτικών μέτρων. Ωστόσο, η ίδια η τεχνολογία ΤΝ μπορεί να χρησιμοποιηθεί από εγκληματίες του κυβερνοχώρου για την αυτοματοποίηση επιθέσεων μεγάλης κλίμακας και την ανάπτυξη κακόβουλων προγραμμάτων που μαθαίνουν και εξελίσσονται. Οι ελληνικές δημόσιες αρχές θα πρέπει να αναπτύξουν στρατηγικές ασφάλειας που να λαμβάνουν υπόψη τη χρήση της AI τόσο για την πρόληψη όσο και για την αντιμετώπιση επιθέσεων.

3.5 Νομοθετικό πλαίσιο και πολιτικές κυβερνοασφάλειας στην Ελλάδα

Η κυβερνοασφάλεια έχει καταστεί προτεραιότητα στην Ελλάδα τα τελευταία χρόνια, καθώς οι απειλές στον κυβερνοχώρο έχουν αυξηθεί σημαντικά και η ανάγκη προστασίας των κρίσιμων υποδομών έχει γίνει πιο επιτακτική. Η ευρωπαϊκή νομοθεσία, ιδίως η οδηγία NIS 2, σε συνδυασμό με τις εθνικές στρατηγικές, έχει δημιουργήσει ένα πλαίσιο με στόχο την προστασία της χώρας από τις απειλές στον κυβερνοχώρο. Ωστόσο, η εφαρμογή αυτών των πολιτικών παραμένει μια σημαντική πρόκληση, ιδίως στον δημόσιο τομέα, όπου οι πόροι είναι συχνά περιορισμένοι και η εμπειρογνωμοσύνη ανεπαρκής. Η οδηγία NIS 2 (Network and Information Systems Directive) είναι η βασική νομοθεσία της Ευρωπαϊκής Ένωσης (ΕΕ) για την ενίσχυση της ασφάλειας των δικτύων και των συστημάτων πληροφοριών. Πρόκειται για τη δεύτερη έκδοση της οδηγίας NIS, η οποία αποσκοπεί στην προστασία των υποδομών ζωτικής σημασίας στα κράτη μέλη από απειλές στον κυβερνοχώρο. Η οδηγία αποσκοπεί στην προστασία φορέων ζωτικής σημασίας, όπως οι τομείς της ενέργειας, των μεταφορών, της υγείας και της ύδρευσης, καθώς και των παρόχων ψηφιακών υπηρεσιών, όπως οι πάροχοι cloud και οι διαδικτυακές αγορές.

Η υιοθέτηση της οδηγίας NIS 2 στην Ελλάδα απαιτεί από τους δημόσιους οργανισμούς να λάβουν μια σειρά από τεχνικά και οργανωτικά μέτρα για να διασφαλίσουν τη λειτουργία των πληροφοριακών τους συστημάτων. Μία από τις κύριες απαιτήσεις της NIS 2 είναι η σύσταση και διατήρηση μιας ομάδας αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), υπεύθυνης για την παρακολούθηση, τον εντοπισμό και την αντιμετώπιση περιστατικών ασφάλειας στον κυβερνοχώρο. Στην Ελλάδα, οι CSIRT λειτουργούν υπό την καθοδήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, η οποία είναι υπεύθυνη για την εποπτεία και το συντονισμό των δράσεων των δημόσιων και ιδιωτικών

οργανισμών. Η Ελλάδα έχει λάβει σημαντικά μέτρα για να συμμορφωθεί με τις απαιτήσεις της οδηγίας, όπως η υιοθέτηση εθνικής στρατηγικής για την ασφάλεια των πληροφοριακών συστημάτων και η ενίσχυση του μηχανισμού παρακολούθησης των απειλών στον κυβερνοχώρο. Ωστόσο, η εφαρμογή της NIS 2 παραμένει πρόκληση, ιδίως σε μικρότερους δημόσιους οργανισμούς με περιορισμένους πόρους και τεχνογνωσία. Οι οργανισμοί αυτοί αντιμετωπίζουν προβλήματα όπως η έλλειψη εξειδικευμένου προσωπικού και η αδυναμία πλήρους δημιουργίας της τεχνικής υποδομής που είναι απαραίτητη για τον εντοπισμό και την αντιμετώπιση των απειλών στον κυβερνοχώρο (RiskLens, 2023).

Παρά την εξέλιξη που έχει σημειωθεί μέχρι στιγμής, υπάρχουν αρκετές προκλήσεις που δυσχεραίνουν την πλήρη συμμόρφωση των ελληνικών δημόσιων αρχών με την οδηγία NIS 2. Μία από τις κύριες προκλήσεις είναι η έλλειψη προσωπικού με εξειδίκευση στην ασφάλεια στον κυβερνοχώρο. Οι δημόσιοι οργανισμοί συχνά αδυνατούν να προσελκύσουν και να διατηρήσουν εμπειρογνώμονες λόγω των περιορισμένων προϋπολογισμών τους και της έλλειψης ανταγωνιστικότητας σε σύγκριση με τον ιδιωτικό τομέα. Αυτή η έλλειψη ανθρώπινου δυναμικού δημιουργεί σημαντικό κενό στην προστασία των συστημάτων πληροφοριών. Υπάρχει επίσης εγγενής καθυστέρηση στην υιοθέτηση των τελευταίων τεχνολογικών εξελίξεων από τους δημόσιους οργανισμούς. Παρόλο που η υιοθέτηση προηγμένης τεχνολογίας απαιτείται από το νόμο για την προστασία κρίσιμων υποδομών, η έλλειψη χρηματοδότησης και η γραφειοκρατία επιβραδύνουν την υιοθέτηση νέων προτύπων από τους οργανισμούς.

Μια άλλη σημαντική πτυχή είναι η κατακερματισμένη προσέγγιση της ασφάλειας στον κυβερνοχώρο. Σε πολλές περιπτώσεις, οι δημόσιες αρχές εφαρμόζουν μέτρα κυβερνοασφάλειας από μόνες τους, χωρίς ενιαίο συντονισμό σε εθνικό επίπεδο. Αυτό δημιουργεί κενά και ελλείψεις στην προστασία των δημόσιων υπηρεσιών στο σύνολό τους. Η δημιουργία ενός κεντρικού φορέα που θα παρακολουθεί την εφαρμογή των πολιτικών κυβερνοασφάλειας σε όλους τους δημόσιους φορείς είναι μια προτεινόμενη λύση που θα μπορούσε να βελτιώσει την κατάσταση αυτή.

Η Εθνική Στρατηγική της Ελλάδας για την ασφάλεια στον κυβερνοχώρο αποτελεί τη βάση μιας πολιτικής για την προστασία των κρίσιμων υποδομών και των πληροφοριακών συστημάτων των δημόσιων οργανισμών. Η στρατηγική αναπτύσσεται βάσει ευρωπαϊκών οδηγιών και διεθνών βέλτιστων πρακτικών και αποσκοπεί στη δημιουργία ενός ανθεκτικού και ασφαλούς περιβάλλοντος για την παροχή δημόσιων υπηρεσιών (RiskLens, 2023).

Βασικά στοιχεία της εθνικής στρατηγικής εμπεριέχουν:

1. **Κατάρτιση και ευαισθητοποίηση**. Η ενίσχυση της κατάρτισης του προσωπικού σε θέματα κυβερνοασφάλειας στους δημόσιους οργανισμούς είναι ζωτικής σημασίας. Η στρατηγική προβλέπει τη δημιουργία ενός προγράμματος συνεχούς κατάρτισης, ώστε το προσωπικό να είναι σε θέση να εντοπίζει και να ανταποκρίνεται εγκαίρως στις απειλές.

2. **Διαχείριση κινδύνων και αντιμετώπιση περιστατικών**. Η στρατηγική περιλαμβάνει σαφείς οδηγίες σχετικά με τη διαχείριση κινδύνων και την ανάπτυξη σχεδίων αποκατάστασης μετά από μια επίθεση στον κυβερνοχώρο. Οι δημόσιες αρχές υποχρεούνται να αναπτύξουν μηχανισμούς παρακολούθησης και αντιμετώπισης περιστατικών και διαδικασίες αναφοράς περιστατικών στις αρμόδιες αρχές.

3. **Συνεργασία με διεθνείς οργανισμούς**. Η εθνική στρατηγική προβλέπει τη συνεργασία με διεθνείς οργανισμούς και φορείς κυβερνοασφάλειας, όπως το Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), για την ανταλλαγή πληροφοριών και την υιοθέτηση διεθνών προτύπων (ENISA, 2023).

Ο κεντρικός συντονισμός της πολιτικής για την ασφάλεια στον κυβερνοχώρο στην Ελλάδα είναι απαραίτητος για την αποτελεσματική εφαρμογή της στρατηγικής. Η Εθνική Αρχή Κυβερνοασφάλειας διαδραματίζει βασικό ρόλο στο συντονισμό των δραστηριοτήτων των δημόσιων φορέων και στη διασφάλιση της συμμόρφωσης με τις κατευθυντήριες γραμμές και τις βέλτιστες πρακτικές. Ωστόσο, οι κατακερματισμένες δομές διακυβέρνησης και η ανεπαρκής χρηματοδότηση περιορίζουν την ικανότητα των αρχών να παρέχουν ολοκληρωμένη καθοδήγηση και υποστήριξη στους οργανισμούς. Η προτεινόμενη λύση είναι η ενίσχυση των ικανοτήτων των εθνικών φορέων και η δημιουργία ενός δικτύου συνεργασίας με τις CSIRT για την ανταλλαγή τεχνογνωσίας και τη βελτίωση της αποτελεσματικότητας των μέτρων ασφαλείας.

3.6 Προκλήσεις και προοπτικές για τη βελτίωση της κυβερνοασφάλειας στην Ελλάδα

Οι κύριες προκλήσεις που αντιμετωπίζουν οι ελληνικές δημόσιες αρχές περιλαμβάνουν την έλλειψη επαρκών πόρων και προσωπικού και την ανάγκη συνεχούς προσαρμογής στις νέες ευρωπαϊκές οδηγίες. Η εισαγωγή της τελευταίας τεχνολογίας χωρίς την παράλληλη ανάπτυξη των απαραίτητων δομών ασφαλείας δημιουργεί τρωτά σημεία που μπορούν να αξιοποιηθούν από εγκληματίες του κυβερνοχώρου. Η βελτίωση της ασφάλειας στον κυβερνοχώρο στους δημόσιους οργανισμούς απαιτεί επείγουσες επενδύσεις σε υποδομές ασφαλείας, όπως προηγμένα συστήματα ανίχνευσης και αντιμετώπισης περιστατικών και την ανάπτυξη προγραμμάτων κατάρτισης για το προσωπικό. Η ενσωμάτωση του blockchain σε κρίσιμες υποδομές μπορεί να βελτιώσει την ασφάλεια του συστήματος, καθώς καθιστά τις διαδικασίες πιο διαφανείς και ασφαλείς. Επιπλέον, η δημιουργία ενός εθνικού κεντρικού συντονιστικού φορέα για την ασφάλεια στον κυβερνοχώρο θα μπορούσε να ενισχύσει τη συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των δημόσιων αρχών. Θα μπορούσε να παρακολουθεί και να αναλύει τις απειλές, να παρέχει εκπαίδευση και να λειτουργεί ως κεντρικό σημείο επαφής για όλα τα θέματα ασφάλειας στον κυβερνοχώρο. Τέλος, η συνεργασία της Ελλάδας με διεθνείς

οργανισμούς και ιδρύματα θα ενισχύσει την ικανότητά της να αντιμετωπίζει αποτελεσματικά τις απειλές στον κυβερνοχώρο και να ανταποκρίνεται στις εξελίξεις στις παγκόσμιες τακτικές ασφάλειας.

Βασική προτεραιότητα για την υλοποίηση της Εθνικής Στρατηγικής για την Ασφάλεια στον Κυβερνοχώρο είναι η ανάπτυξη ενός ολοκληρωμένου συστήματος διακυβέρνησης του « Ελληνικού Κυβερνοχώρου » υπό τον συντονισμό των αρμόδιων αρχών:

- Όλοι οι τομείς της ασφάλειας στον κυβερνοχώρο θα αντιμετωπιστούν με ολιστικό τρόπο.
- Οι ρόλοι και οι αρμοδιότητες όλων των εμπλεκόμενων φορέων θα καθοριστούν με σαφήνεια.
- Το σύστημα διακυβέρνησης είναι οργανωμένο και λειτουργικό και παρέχει σαφείς προκαθορισμένες διαδικασίες στις οποίες βασίζεται και θα εξελίσσεται. Υπό το πρίσμα των ανωτέρω αρχών, δημιουργείται ένα σύστημα στο οποίο η εθνική αρχή για την ασφάλεια στον κυβερνοχώρο είναι ο επικεφαλής οργανισμός και αποτελείται από ένα δίκτυο εμπλεκόμενων φορέων και προσωπικού ασφαλείας σε όλα τα επίπεδα: α) προληπτικής δράσης, β) απόκρισης και διασφάλισης της επιχειρησιακής συνέχειας.

Για την αποτελεσματική προστασία από απειλές που ενδέχεται να επηρεάσουν την παροχή δημόσιων υπηρεσιών, οι απειλές αυτές πρέπει πρώτα να εντοπιστούν και να τεκμηριωθούν. Ο εντοπισμός των απειλών για την ασφάλεια στον κυβερνοχώρο βασίζεται σε μια δομημένη μεθοδολογία που αναπτύχθηκε για τον σκοπό αυτό και προωθείται σε συνεργασία με φορείς όπως ο Εθνικός Οργανισμός Πληροφοριών, ο Γενικός Οργανισμός Πληροφοριών και ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων Πληροφοριών.

Βασικές παρεμβάσεις στο πλαίσιο αυτού του στόχου περιλαμβάνουν την ανάπτυξη μεθοδολογιών ανάλυσης δεδομένων και μητρώων απειλών, τη δημιουργία εθνικών σχεδίων αξιολόγησης κινδύνων. Η αξιολόγηση και η αποτελεσματική διαχείριση των κινδύνων κυβερνοασφάλειας αποτελεί θεμελιώδη πυλώνα της κυβερνοασφάλειας και της ψηφιακής διακυβέρνησης. Αυτό απαιτεί τα εξής:

- Καθορισμός ενός πλαισίου για τους οργανισμούς, ώστε να προσδιορίζουν τις κρίσιμες επιχειρηματικές δραστηριότητες και τους πληροφοριακούς πόρους που τις υποστηρίζουν

- Καθορισμός ενός ειδικού πλαισίου για τον εντοπισμό εξωτερικών και εσωτερικών παραγόντων που ενδέχεται να επηρεάσουν την ασφάλεια των πληροφοριακών πόρων

- Δημιουργία ενός προφίλ απειλών και αξιολόγηση των τρωτών σημείων που μπορούν να εκμεταλλευτούν οι απειλές

- Ανάπτυξη ενός σχεδίου αντιμετώπισης κινδύνων στον κυβερνοχώρο.

Μια άλλη σημαντική δράση είναι η διεξαγωγή μελετών εκτίμησης κινδύνων σε εθνικό επίπεδο ακολουθώντας μια επιστημονική διαδικασία που βασίζεται στον εντοπισμό, την ανάλυση και την εκτίμηση των επιπτώσεων των κινδύνων και την ανάπτυξη εθνικών σχεδίων αντιμετώπισης έκτακτων αναγκών. Η μελέτη, η οποία επανεξετάζεται το αργότερο κάθε τρία χρόνια, λαμβάνει υπόψη όλες τις πιθανές απειλές, ιδίως εκείνες που σχετίζονται με κακόβουλες πράξεις (όπως το έγκλημα στον κυβερνοχώρο και οι επιθέσεις στον κυβερνοχώρο), καθώς και τους κινδύνους που οφείλονται σε φυσικά φαινόμενα, τεχνικές αστοχίες και δυσλειτουργίες και ανθρώπινα λάθη. Λαμβάνονται επίσης υπόψη οι απειλές που προκύπτουν από την αλληλεξάρτηση των συστημάτων επικοινωνίας.

Επιπλέον, κατά την αξιολόγηση της έκτασης και της σημασίας των επιπτώσεων σε εθνικό επίπεδο λαμβάνονται υπόψη και τα πληροφοριακά συστήματα των ενδιαφερομένων μερών που συμμετέχουν στην εθνική στρατηγική, ιδίως οι κρίσιμες υποδομές [ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 - 2025 (https://mindigital.gr/dioikisi/kyvernoasfaleia)].

Τα ανωτέρω μέτρα υποστηρίζουν το εθνικό σχέδιο έκτακτης ανάγκης και διευκολύνουν επίσης την κατηγοριοποίηση των οργανισμών ανάλογα με τις υπηρεσίες που παρέχουν και τη συμμόρφωσή τους με την ισχύουσα νομοθεσία (όπως η οδηγία για την ΕΑΑ και ο νόμος αριθ. 4577 του 2018). Το Εθνικό Σχέδιο Έκτακτης Ανάγκης αποτελεί κατευθυντήρια γραμμή για την αντιμετώπιση ενός συμβάντος που θεωρείται σημαντική διαταραχή των υπηρεσιών που παρέχει ένας οργανισμός και εμπίπτει στον τομέα της διαχείρισης κρίσεων. Συνεπώς, το σχέδιο περιλαμβάνει τα κριτήρια για τον χαρακτηρισμό ενός συμβάντος ως κρίσης, τους ρόλους και τις αρμοδιότητες για τη διαχείριση κρίσεων, τις ενέργειες που πρέπει να αναληφθούν για την επιτυχή αντιμετώπιση του συμβάντος και τη λήψη όλων των κατάλληλων προστατευτικών μέτρων για τον μετριασμό των επιπτώσεων και την αποτροπή της διακοπής των υπηρεσιών. Το Εθνικό Σχέδιο Έκτακτης Ανάγκης ενεργοποιείται σε περίπτωση περιστατικού που προκαλεί σημαντική διακοπή στην παροχή υπηρεσιών από το σύστημα ή που θέτει σε κίνδυνο την παροχή υπηρεσιών στο ευρύ κοινό. Ένα τέτοιο γεγονός αναφέρεται ως κρίση και το σχέδιο μετατρέπεται σε εγχειρίδιο διαχείρισης κρίσεων [ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 - 2025 (https://mindigital.gr/dioikisi/kyvernoasfaleia)].

Η σύγχρονη τεχνολογία έχει συμβάλει στην ανάπτυξη ενός ιδιαίτερα διασυνδεδεμένου περιβάλλοντος που δεν δεσμεύεται από εθνικά σύνορα. Για την προστασία των κοινών συμφερόντων, ο τομέας της διπλωματίας στον κυβερνοχώρο έχει εξελιχθεί για να προωθήσει την υπεύθυνη συμπεριφορά στον κυβερνοχώρο σε εθνικό επίπεδο. Ταυτόχρονα, οι διασυνοριακές αλληλεξαρτήσεις διεθνή συνεργασία για την επίτευξη ενός κοινού υψηλού επιπέδου ασφάλειας. Στο πλαίσιο αυτό, οι χώρες μας θα πρέπει να διατηρήσουν και να ενισχύσουν την παρουσία και τη συμμετοχή τους σε όλους τους τομείς της διεθνούς συνεργασίας, με στόχο:

- Να παρέχουν εταιρικές σχέσεις για την από κοινού ανάπτυξη εργαλείων για την αντιμετώπιση απειλών και προκλήσεων

- Να οικοδομήσουν και να ενισχύσουν συμμαχίες για την από κοινού αντιμετώπιση επιθέσεων στον κυβερνοχώρο

- Να εξασφαλίζουν πρόσβαση σε γνώση και εμπειρογνωμοσύνη

- Συνδιαμόρφωση νομοθετικών προτάσεων σε ευρωπαϊκό επίπεδο

- Κοινή εφαρμογή αποφάσεων που λαμβάνονται στο πλαίσιο διεθνών οργανισμών στους οποίους συμμετέχει η Ελλάδα [ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 - 2025 (https://mindigital.gr/dioikisi/kyvernoasfaleia)].

Κεφάλαιο 4ο: Μελέτη περίπτωσης. Η εφαρμογή του NIST CSF 2.0 στον Οργανισμό Διαχείρισης Πληροφοριακών Συστημάτων Ελλάδας (ΟΔΙΠΣΕ)

4.1 Εισαγωγή στον Οργανισμό

Αρχικά, θα πρέπει να καταστεί σαφές, πως, ο οργανισμός που αναφέρεται στην παρούσα εργασία, δεν υφίσταται και αποτελεί μια υποθετική προσέγγιση. Ο Οργανισμός Διαχείρισης Πληροφοριακών Συστημάτων Ελλάδας (ΟΔΙΠΣΕ) αποτελεί έναν κεντρικό δημόσιο φορέα που διαχειρίζεται πληροφοριακά συστήματα μεγάλης κλίμακας για λογαριασμό της ελληνικής κυβέρνησης. Στις αρμοδιότητές της περιλαμβάνεται επίσης η διαχείριση ευαίσθητων προσωπικών δεδομένων που σχετίζονται με τη φορολογία, την κοινωνική ασφάλιση και τη δημόσια υγεία. Η ασφάλεια στον κυβερνοχώρο έχει μεγάλη σημασία για τον οργανισμό αυτό, καθώς διαχειρίζεται κρίσιμες υποδομές που σχετίζονται με τη δημόσια διοίκηση.

Λαμβάνοντας υπόψη τις αυξανόμενες απειλές στον κυβερνοχώρο και την ανάγκη συμμόρφωσης με τους διεθνείς κανονισμούς ασφαλείας η εφαρμογή της **οδηγίας NIS2** θα αποτελούσε το πρώτο βήμα για τη συμμόρφωση με τις υποχρεώσεις κυβερνοασφάλειας που προβλέπει η Ευρωπαϊκή Ένωση. Η οδηγία NIS2, η οποία εστιάζει στη διαχείριση της ασφάλειας δικτύων και πληροφοριών για κρίσιμες υποδομές, όπως αυτές που χειρίζεται ο ΟΔΙΠΣΕ, στοχεύει στην αύξηση του επιπέδου κυβερνοασφάλειας σε οργανισμούς που προσφέρουν βασικές υπηρεσίες.

Σε πρώτη φάση, ο οργανισμός θα πρέπει να υλοποιήσει τις βασικές αρχές της οδηγίας **NIS2** (Πίνακας 1), που περιλαμβάνουν:

1. **Δημιουργία ομάδας CSIRT**: Ο ΟΔΙΠΣΕ θα δημιουργήσει μια ειδική ομάδα αντιμετώπισης και διαχείρισης περιστατικών κυβερνοασφάλειας (**Computer Security Incident Response Team**).
2. **Διαχείριση κινδύνων εφοδιαστικής αλυσίδας**: Ο οργανισμός θα αναπτύξει προγράμματα διαχείρισης κινδύνων για την εφοδιαστική αλυσίδα του, σύμφωνα με τις απαιτήσεις της NIS2.
3. **Συμμόρφωση με το GDPR**: Καθώς ο ΟΔΙΠΣΕ διαχειρίζεται ευαίσθητα προσωπικά δεδομένα, η συμμόρφωση με τον **Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR)** είναι απαραίτητη για την προστασία της ιδιωτικότητας των πολιτών.

Πίνακας 1 : Εφαρμογή της οδηγίας NIS2 στον ΟΔΙΠΣΕ

Κατηγορία	**Μέτρα**	**Περιγραφή**	**Υπεύθυνος φορέας**
Αναγνώριση κρίσιμων υποδομών	Χαρτογράφηση κρίσιμων υποδομών	Ταυτοποίηση κρίσιμων πληροφοριακών συστημάτων και δεδομένων	Τμήμα κυβερνοασφάλειας
Ανάθεση ρόλων	Δημιουργία ομάδων αντιμετώπισης κρίσιμων περιστατικών ασφαλείας (CSIRT)	Σύσταση ομάδων CSIRT για άμεση ανταπόκριση σε περιστατικά κυβερνοεπίθεσης	Διεύθυνση ασφάλειας πληροφοριών
Μέτρα προστασίας δεδομένων	Κρυπτογράφηση δεδομένων	Χρήση πολλαπλών παραγόντων ταυτοποίησης για αποτροπή μη εξουσιοδοτημένης πρόσβασης	Τμήμα πληροφοριακών συστημάτων
Ανίχνευση	Εγκατάσταση συστήματος SIEM	Ανάλυση δεδομένων για εντοπισμό ύποπτης δραστηριότητας	Τμήμα πληροφοριακής ασφάλειας
Ανταπόκριση	Δημιουργία και εφαρμογή σχεδίου αντιμετώπισης περιστατικών	Άμεση ανταπόκριση με σαφή βήματα για την αποκατάσταση της ασφάλειας	Ομάδα CSIRT
Ανάκτηση	Ανάπτυξη σχεδίου επαναφοράς	Δημιουργία αντιγράφων ασφαλείας	Τμήμα αντιμετώπισης κρίσεων
Συμμόρφωση-έλεγχοι	Τακτικός έλεγχος συμμόρφωσης με το NIS 2	Διασφάλιση της εφαρμογής των μέτρων ασφαλείας με βάση την οδηγία NIS 2	Διεύθυνση ελέγχων
Εκπαίδευση προσωπικού	Συνεχής εκπαίδευση και ενημέρωση	Εκπαιδευτικά σεμινάρια για την ευαισθητοποίηση του προσωπικού σε θέματα κυβερνοασφάλειας	Τμήμα ανθρώπινου δυναμικού
Ενημέρωση ενδιαφερόμενων μερών	Ενημέρωση αρμόδιων σε περίπτωση κυβερνοεπίθεσης	Άμεση ενημέρωση αρχών και συνεργατών	Τμήμα δημοσίων σχέσεων

Αφού η οδηγία NIS2 τεθεί σε εφαρμογή και ο οργανισμός συμμορφωθεί πλήρως με αυτή, σε δεύτερη φάση θα εφαρμοστεί το **NIST Cybersecurity Framework (CSF) 2.0**. Αυτό το πλαίσιο θα ενισχύσει περαιτέρω τη συνολική στρατηγική κυβερνοασφάλειας, προσαρμόζοντας τις διεθνείς βέλτιστες πρακτικές στις ανάγκες του οργανισμού.

Ο συνδυασμός NIS2 και NIST 2.0 θα εξασφαλίσει ότι ο οργανισμός θα διαθέτει ένα στιβαρό σύστημα κυβερνοασφάλειας, καλύπτοντας τόσο τις ευρωπαϊκές απαιτήσεις όσο και τα παγκόσμια πρότυπα ασφαλείας. Το NIST CSF αναγνωρίζει την ευελιξία του πλαισίου, την ικανότητά του να προσαρμόζεται στις ανάγκες των επιχειρήσεων, τη συνολική αποτελεσματικότητά του στη διαχείριση των απειλών στον κυβερνοχώρο και των απειλών στον κυβερνοχώρο.

4.2 Βήματα Υλοποίησης του NIST CSF 2.0 στον ΟΔΙΠΣΕ

Η υλοποίηση του NIST CSF 2.0 στον ΟΔΙΠΣΕ έλαβε χώρα σε πέντε κύρια βήματα, σύμφωνα με τις λειτουργίες του πλαισίου (Πίνακας 2). Ο οργανισμός υιοθέτησε μια ολοκληρωμένη προσέγγιση, η οποία συνδύασε τεχνολογικές λύσεις, εκπαίδευση προσωπικού και διαδικασίες διακυβέρνησης.

4.2.1 Διακυβέρνηση (Govern)

Λαμβάνοντας υπόψη ότι ο ΟΔΙΠΣΕ διαχειρίζεται κρίσιμες υποδομές και ευαίσθητα προσωπικά δεδομένα, η υιοθέτηση της λειτουργίας Govern του πλαισίου NIST CSF 2.0 είναι καθοριστική για την ορθή διαχείριση της κυβερνοασφάλειας. Η λειτουργία αυτή στοχεύει στην καθιέρωση σαφών πολιτικών και στρατηγικών κυβερνοασφάλειας, οι οποίες πρέπει να συνδέονται άμεσα με την αποστολή του οργανισμού, που είναι η ασφαλής διαχείριση των πληροφοριακών συστημάτων μεγάλης κλίμακας της ελληνικής κυβέρνησης. Στον ΟΔΙΠΣΕ, η έλλειψη σαφών πολιτικών ενδέχεται να οδηγήσει σε αποσπασματικές δράσεις ασφαλείας, γεγονός που αυξάνει τον κίνδυνο παραβίασης δεδομένων και διαταραχών στις κρίσιμες υποδομές. Η ενσωμάτωση στρατηγικών διαχείρισης κινδύνων σε όλα τα τμήματα του οργανισμού είναι απαραίτητη, καθώς θα εξασφαλίσει ότι οι δράσεις κυβερνοασφάλειας δεν είναι απομονωμένες, αλλά αποτελούν μέρος της συνολικής στρατηγικής του οργανισμού. Με αυτόν τον τρόπο, ο ΟΔΙΠΣΕ θα είναι σε θέση να ανταποκρίνεται στις συνεχώς μεταβαλλόμενες απειλές του κυβερνοχώρου, ενισχύοντας την ανθεκτικότητά του και διασφαλίζοντας τη συμμόρφωση με τους διεθνείς κανονισμούς ασφαλείας.

4.2.2 Αναγνώριση (Identify)

Η διαχείριση των κινδύνων του ΟΔΙΠΣΕ βασίζεται στη λειτουργία της ευαισθητοποίησης. Ο οργανισμός διενήργησε λεπτομερή έλεγχο όλων των πληροφοριακών συστημάτων, των δεδομένων και της δικτυακής υποδομής. Χρησιμοποιήθηκαν ειδικά εργαλεία ανάλυσης κινδύνων, όπως το RiskLens και το RSA Archer, για την ανάλυση των τρωτών σημείων των συστημάτων πληροφοριών και την αξιολόγηση των πιθανών κινδύνων. Κατά τη διάρκεια της διαδικασίας εντοπισμού, ο ΟΔΙΠΣΕ κατηγοριοποίησε τα περιουσιακά στοιχεία ανάλογα με τη σημασία τους για την επιχειρησιακή συνέχεια και τη δημόσια ασφάλεια. Αυτό επέτρεψε τον εντοπισμό κρίσιμων υποδομών που θα έπρεπε να έχουν προτεραιότητα για προστασία, όπως οι βάσεις δεδομένων των πολιτών, τα συστήματα δημόσιων δαπανών και τα δίκτυα υγείας.

4.2.3 Προστασία (Protect)

Η λειτουργία Προστασία έδωσε βαρύτητα στην ενδυνάμωση της ασφάλειας των κρίσιμων υποδομών του ΟΔΙΠΣΕ. Ο οργανισμός διάλεξε προηγμένα τεχνολογικά εργαλεία για την προστασία των δεδομένων και των πληροφοριακών του συστημάτων. Επιπλέον, ο ΟΔΙΠΣΕ ανέπτυξε πολιτικές ασφάλειας για τον έλεγχο πρόσβασης, εφαρμόζοντας πολλαπλούς παράγοντες ταυτοποίησης (MFA) και περιορισμένες άδειες πρόσβασης σε κρίσιμα συστήματα, προκειμένου να περιορίσει τις δυνατότητες εσωτερικής απειλής.

4.2.4 Ανίχνευση (Detect)

Η συγκεκριμένη λειτουργία έδωσε ιδιαίτερη βαρύτητα στον άμεσο εντοπισμό πιθανών απειλών. Ο ΟΔΠΣΕ εγκατέστησε ένα σύστημα Security Information and Event Management (SIEM), (Splunk ή το IBM QRadar), το οποίο δίνει τη δυνατότητα παρακολούθησης της κυκλοφορίας δικτύου και της ανάλυσης των συμβάντων ασφαλείας σε πραγματικό χρόνο. Επίσης, χρησιμοποιήθηκαν τεχνικές Machine Learning για τον εντοπισμό δυσλειτουργιών στη συμπεριφορά των χρηστών και τη δραστηριότητα δικτύου. Αυτό επέτρεψε στον οργανισμό να εντοπίζει άμεσα οποιαδήποτε ύποπτη δραστηριότητα που θα μπορούσε να οδηγήσει σε κυβερνοεπίθεση ή διαρροή δεδομένων.

4.2.5 Ανταπόκριση (Respond)

Ο ΟΔΠΣΕ ανέπτυξε, για τη συγκεκριμένη λειτουργία ένα ολοκληρωμένο σχέδιο διαχείρισης περιστατικών, το οποίο βασίστηκε σε εργαλεία όπως το ServiceNow για την αναφορά και τη διαχείριση συμβάντων ασφαλείας. Το σχέδιο περιελάμβανε σαφείς διαδικασίες για την ταχεία αντιμετώπιση περιστατικών με τη συμμετοχή όλων των τμημάτων του οργανισμού και της ομάδας αντιμετώπισης

περιστατικών ασφάλειας υπολογιστών (CSIRT). Μια καινοτόμος προσέγγιση ήταν η ενσωμάτωση ενός εργαλείου αυτοματοποιημένης αντιμετώπισης περιστατικών (AIR). Το εργαλείο αυτό επέτρεψε την αυτοματοποίηση ορισμένων ενεργειών αντιμετώπισης περιστατικών, όπως η απομόνωση μολυσμένων συστημάτων σε καραντίνα ή η ακύρωση δικαιωμάτων πρόσβασης σε περίπτωση επιβεβαιωμένης παραβίασης της ασφάλειας.

4.2.6 Αποκατάσταση (Recover)

Περιελάμβανε την ανάπτυξη διαδικασιών ανάκαμψης και επιχειρησιακής συνέχειας. Ο οργανισμός εφάρμοσε μια λύση δημιουργίας αντιγράφων ασφαλείας και αποκατάστασης μετά από καταστροφή χρησιμοποιώντας εργαλεία όπως η Veeam και η Commvault για να διασφαλίσει ότι τα συστήματα θα μπορούσαν να ανακτηθούν γρήγορα σε περίπτωση διακοπής ρεύματος ή καταστροφικής επίθεσης. Ο οργανισμός ανέπτυξε επίσης ένα σχέδιο επικοινωνίας για τη διαχείριση κρίσεων, ώστε να διασφαλίσει ότι οι αρμόδιες αρχές και τα ενδιαφερόμενα μέρη ενημερώνονται σε περίπτωση μείζονος συμβάντος ασφαλείας.

Στην επόμενη σελίδα στον **Πίνακα 2** εφαρμόζεται το NIST CSF 2.0 στον ΟΔΙΠΣΕ.

Λειτουργία CSF	Κατηγορία	Υποκατηγορία	Τρέχουσα κατάσταση	Στόχος	Αναγνωρισμένα κενά	Σχέδιο Δράσης
Διακυβέρνηση (GV)	Οργανωσιακό πλαίσιο	GV.OC-01: Η αποστολή του οργανισμού είναι κατανοητή και καθοδηγεί τη διαχείριση κινδύνων κυβερνοασφάλειας	Ο οργανισμός δεν έχει ακόμη διαμορφώσει σαφείς πολιτικές κυβερνοασφάλειας που να συνδέονται άμεσα με την αποστολή και τους στόχους του. Οι δράσεις κυβερνοασφάλειας είναι αποσπασματικές και δεν υπάρχει ενσωμάτωση στη γενικότερη στρατηγική του οργανισμού.	Ανάπτυξη και ενσωμάτωση μιας συνολικής πολιτικής κυβερνοασφάλειας, η οποία συνδέεται άμεσα με την αποστολή του οργανισμού. Η στρατηγική κυβερνοασφάλειας πρέπει να ενσωματωθεί στα στρατηγικά σχέδια του οργανισμού και να γίνεται συχνή αξιολόγηση της αποτελεσματικότητάς της.	Έλλειψη σαφούς πολιτικής για την εταιρική διαφάνεια και την ηθική συμπεριφορά.	Το σχέδιο δράσης θα πρέπει να περιλαμβάνει SMART στόχους (Συγκεκριμένα, Μετρήσιμα, Εφικτά, Σχετικά και Χρονικά προσδιορισμένα), για να αξιολογηθεί η πρόοδος.
	Στρατηγική διαχείρισης κινδύνου	GV.RM-01: Οι στόχοι διαχείρισης κινδύνων έχουν καθοριστεί και συμφωνηθεί από τους ενδιαφερόμενους	Υπάρχει μία αρχική κατανόηση των κινδύνων, αλλά δεν έχουν συμφωνηθεί επίσημοι στόχοι διαχείρισης κινδύνων μεταξύ των διευθυντικών στελεχών. Δεν υπάρχει σαφής στρατηγική για τη διαχείριση κινδύνων σε επίπεδο οργανισμού.	Επίσημη καθιέρωση και συμφωνία στρατηγικών στόχων διαχείρισης κινδύνων μεταξύ όλων των εμπλεκόμενων τμημάτων και διευθυντικών στελεχών. Αυτοί οι στόχοι πρέπει να είναι σαφείς και να ενημερώνονται τακτικά, με βάση τη μεταβαλλόμενη απειλή και το ρυθμιστικό πλαίσιο.	Ανεπαρκής ανάλυση κινδύνων σε νέες πρωτοβουλίες ή έργα.	Σαφής κατανομή ευθυνών και υποχρεώσεων στους εμπλεκόμενους, αποφεύγοντας την αβεβαιότητα και καθυστερήσεις στην υλοποίηση.
	Διαχείριση κινδύνων εφοδιαστικής αλυσίδας	GV.SC-01: Έχει δημιουργηθεί πρόγραμμα διαχείρισης κινδύνων εφοδιαστικής αλυσίδας				
Αναγνώριση (ID)	Διαχείριση περιουσιακών στοιχείων	ID.AM-01: Διατηρούνται απογραφές υλικού	Η απογραφή υλικού (hardware) είναι ελλιπής, καθώς δεν υπάρχει ενημερωμένη	Δημιουργία και συντήρηση ενημερωμένων και πλήρως	Μη αποτελεσματική κατανομή πόρων, με αποτέλεσμα να	Καθορισμένο χρονοδιάγραμμα για τις επιμέρους δράσεις

			λίστα με το σύνολο των συστημάτων που χρησιμοποιούνται στον οργανισμό. Οι απογραφές είναι χειρόγραφες ή διατηρούνται σε παλαιωμένες βάσεις δεδομένων.	αυτοματοποιημένων απογραφών υλικού. Αυτές οι απογραφές πρέπει να περιλαμβάνουν όλες τις συσκευές, εξοπλισμό και συστήματα που χρησιμοποιούνται στον οργανισμό, ώστε να διασφαλίζεται η προστασία και η διαχείριση τους.	υπάρχουν υπερβάσεις ή ελλείψεις.	
Προστασία (PR)	Διαχείριση ταυτοτήτων, αυθεντικοποίηση και έλεγχος πρόσβασης	PR.AA-01: Οι ταυτότητες και τα διαπιστευτήρια των εξουσιοδοτημένων χρηστών διαχειρίζονται	Ο οργανισμός εφαρμόζει ένα βασικό σύστημα διαχείρισης ταυτοτήτων για τους υπαλλήλους, αλλά δεν υπάρχουν επαρκή μέτρα ελέγχου πρόσβασης. Δεν γίνεται συστηματική παρακολούθηση της αυθεντικοποίησης ή έλεγχος διαπιστευτηρίων με βάση την αρχή της ελάχιστης πρόσβασης.	Εφαρμογή ενός προχωρημένου συστήματος διαχείρισης ταυτοτήτων, το οποίο να περιλαμβάνει ενισχυμένους μηχανισμούς ελέγχου πρόσβασης με βάση την αρχή της ελάχιστης πρόσβασης (least privilege). Παράλληλα, θα πρέπει να γίνονται συστηματικοί έλεγχοι ταυτότητας και πιστοποίησης.	Έλλειψη μεταβλητών μέτρησης απόδοσης για τις βασικές διαδικασίες.	
Ανίχνευση (DE)	Συνεχής παρακολούθηση	DE.CM-01: Τα δίκτυα παρακολουθούνται για τον εντοπισμό ανωμαλιών				
Ανταπόκριση (RS)	Διαχείριση περιστατικών	RS.MA-01: Τα σχέδια ανταπόκρισης σε περιστατικά εκτελούνται σε συντονισμό με τρίτα μέρη	Δεν υπάρχει πλήρως αναπτυγμένο σχέδιο ανταπόκρισης σε περιστατικά, και ο συντονισμός με τρίτους (όπως παρόχους υπηρεσιών) γίνεται μόνο κατά περίπτωση, χωρίς προσυμφωνημένες διαδικασίες.	Δημιουργία πλήρους και επίσημου σχεδίου ανταπόκρισης σε περιστατικά, το οποίο να περιλαμβάνει συγκεκριμένες διαδικασίες συντονισμού με τρίτα μέρη (π.χ. προμηθευτές και πάροχοι υπηρεσιών). Το σχέδιο αυτό πρέπει	Έλλειψη μηχανισμών για την παρακολούθηση και την αξιολόγηση των ικανοτήτων των πολιτών και άλλων ενδιαφερόμενων.	Αξιολόγηση πόρων (προσωπικό, χρηματοδότηση, τεχνολογία) για την υλοποίηση των δράσεων

				να είναι δοκιμασμένο και επαληθευμένο για την αποτελεσματικότητά του.		
Αποκατάσταση (RC)	Εκτέλεση σχεδίου αποκατάστασης	RC.RP-01: Τα σχέδια αποκατάστασης εκτελούνται μετά την κήρυξη του περιστατικού	Υπάρχουν πρωτόκολλα αποκατάστασης, αλλά δεν έχουν δοκιμαστεί σε πραγματικές συνθήκες. Οι διαδικασίες αποκατάστασης δεν είναι καλά καθορισμένες και δεν υπάρχει επίσημος μηχανισμός αξιολόγησης της αποτελεσματικότητάς τους μετά από ένα περιστατικό.	Δημιουργία και δοκιμή ενός αποτελεσματικού σχεδίου αποκατάστασης, το οποίο θα ενεργοποιείται αμέσως μετά την κήρυξη ενός περιστατικού. Το σχέδιο αυτό πρέπει να περιλαμβάνει σαφή βήματα για την αποκατάσταση της λειτουργίας του οργανισμού και να γίνεται τακτική αξιολόγηση της απόδοσής του.	Απουσία στρατηγικού σχεδίου για την ανάπτυξη και τη διαχείριση των ανθρώπινων πόρων.	Εκπαιδευτικά προγράμματα για το προσωπικό σχετικά με τις νέες διαδικασίες και πολιτικές που προκύπτουν από το σχέδιο δράσης.

4.3 Αποτελέσματα της εφαρμογής του NIST CSF 2.0 στον ΟΔΙΠΣΕ

Η εφαρμογή του NIST CSF 2.0 από τον οργανισμό έχει αποφέρει σημαντικά αποτελέσματα όσον αφορά τη βελτίωση της ασφάλειας των συστημάτων και τη συμμόρφωση με κανονιστικές και εθνικές πολιτικές κυβερνοασφάλειας, όπως ο GDPR. Οι διαδικασίες ανίχνευσης και απόκρισης του οργανισμού έχουν βελτιωθεί σημαντικά και η χρήση αυτοματοποιημένων εργαλείων επέτρεψε στον οργανισμό να αποτρέπει τις επιθέσεις σε πρώιμο στάδιο πριν επηρεαστούν κρίσιμες λειτουργίες. Επιπλέον, η ολοκλήρωση ενός προγράμματος κατάρτισης του προσωπικού αύξησε την ευαισθητοποίηση των εργαζομένων και βελτίωσε τη συμμόρφωση με τις εσωτερικές πολιτικές ασφαλείας. Οι τακτικοί έλεγχοι και οι δοκιμές αποκατάστασης βοήθησαν τον οργανισμό να προετοιμαστεί για μελλοντικές απειλές και διαταραχές.

4.4 Προκλήσεις

Ενώ η εφαρμογή του CSF NIST ήταν επιτυχής, υπήρξαν και ορισμένες προκλήσεις. Η πολυπλοκότητα της ενσωμάτωσης διαφορετικών τεχνολογιών, η ανάγκη τομεακού συντονισμού και η διαθεσιμότητα επαρκών πόρων ήταν σοβαρά ζητήματα που έπρεπε να αντιμετωπιστούν. Η έλλειψη εμπειρογνωμόνων σε θέματα ασφάλειας στον κυβερνοχώρο παρέμενε πρόβλημα και, ως εκ τούτου, η κατάρτιση ήταν απαραίτητη. Τέλος, η συνεχής αναβάθμιση του συστήματος ασφαλείας, συμπεριλαμβανομένης της χρήσης της Zero Trust Architecture, ήταν απαραίτητη για να διασφαλιστεί ότι ο οργανισμός ήταν προετοιμασμένος για μελλοντικές απειλές.

4.5 Συμπεράσματα κεφαλαίου

Ο οργανισμός κατάφερε να βελτιώσει σε μεγάλο βαθμό την ασφάλεια των συστημάτων του μέσω της στρατηγικής εφαρμογής του CSF 2.0 του NIST. Η χρήση προηγμένης τεχνολογίας, η εφαρμογή πολιτικών διακυβέρνησης και η εκπαίδευση του προσωπικού ενίσχυσαν την ανθεκτικότητα του οργανισμού στις εξελισσόμενες απειλές στον κυβερνοχώρο. Η εφαρμογή του πλαισίου κατέδειξε την ικανότητα του οργανισμού να διαχειρίζεται αποτελεσματικά τους κινδύνους κυβερνοασφάλειας, να διασφαλίζει τη συνέχεια των κρίσιμων λειτουργιών και να προστατεύει τα δεδομένα των πολιτών.

Κεφάλαιο 5ο: Συμπεράσματα – Μελλοντικές επεκτάσεις

5.1 Γενικά συμπεράσματα

Η ανάλυση και η μελέτη περίπτωσης που παρουσιάζονται στην παρούσα εργασία αναδεικνύουν τη σημασία της εφαρμογής του Πλαισίου Κυβερνοασφάλειας 2.0 του NIST για την ενίσχυση της ασφάλειας των πληροφοριών στους ελληνικούς δημόσιους φορείς. Χάρη στην ευελιξία και την προσαρμοστικότητά του, το πλαίσιο παρέχει μια ολοκληρωμένη προσέγγιση που μπορεί να καλύψει τις ανάγκες διαφορετικών οργανισμών, να αυξήσει την ανθεκτικότητα στις απειλές στον κυβερνοχώρο και να διασφαλίσει τη συμμόρφωση με τους υφιστάμενους κανονισμούς.

Ωστόσο, η επιτυχία ή η αποτυχία της εφαρμογής εξαρτάται από διάφορους παράγοντες, όπως η δέσμευση της διοίκησης, η επαρκής εκπαίδευση του προσωπικού και η διαθεσιμότητα των απαραίτητων πόρων. Η εμπειρία από τη μελέτη περίπτωσης δείχνει ότι, παρά τις προκλήσεις, μπορούν να επιτευχθούν σημαντικές βελτιώσεις στην ασφάλεια των πληροφοριών εάν οι δημόσιοι οργανισμοί υιοθετήσουν μια συστηματική και οργανωμένη προσέγγιση.

Η παρούσα μελέτη περίπτωσης καταδεικνύει ότι η εφαρμογή του CSF 2.0 του NIST μπορεί να βελτιώσει σημαντικά την ασφάλεια των δημόσιων οργανισμών, αυξάνοντας την ευαισθητοποίηση των εργαζομένων, την αποτελεσματικότητα των διαδικασιών ασφαλείας και την ανθεκτικότητα του οργανισμού στις απειλές στον κυβερνοχώρο. Παρά τις αρχικές προκλήσεις και την αντίσταση στην αλλαγή, τα αποτελέσματα είναι θετικά και δείχνουν ότι με τη σωστή προσαρμογή και υποστήριξη, το πλαίσιο μπορεί να εφαρμοστεί με επιτυχία.

Οι προκλήσεις της κυβερνοασφάλειας εξελίσσονται συνεχώς και οι ελληνικοί δημόσιοι οργανισμοί πρέπει να είναι ενημερωμένοι και έτοιμοι να αντιμετωπίσουν τις νέες απειλές. Για το μέλλον, η εστίαση θα πρέπει να δοθεί στη συνεχή βελτίωση των πολιτικών και πρακτικών ασφάλειας, στη συνεργασία με άλλους οργανισμούς και εμπειρογνώμονες στον τομέα και στην ενσωμάτωση νέων τεχνολογιών που θα βοηθήσουν στην αντιμετώπιση των απειλών.

Είναι επίσης σημαντικό για τους δημόσιους οργανισμούς να επενδύσουν στην κατάρτιση και την ευαισθητοποίηση και να δημιουργήσουν μια κουλτούρα ασφάλειας που να διαπερνά όλες τις δραστηριότητες του οργανισμού. Η οικοδόμηση εταιρικών σχέσεων και η ανταλλαγή βέλτιστων πρακτικών με οργανισμούς του ιδιωτικού τομέα μπορεί να συμβάλει στην αντιμετώπιση των προκλήσεων και στην ανάπτυξη ολοκληρωμένων στρατηγικών για την ασφάλεια στον κυβερνοχώρο. Είναι επίσης σημαντικό να συνεχιστεί η παρακολούθηση και η προσαρμογή στις νέες νομικές

απαιτήσεις, όπως η εφαρμογή της οδηγίας NIS 2, η οποία θα φέρει νέες προκλήσεις και ευκαιρίες για την ενίσχυση της ασφάλειας στον κυβερνοχώρο στους δημόσιους οργανισμούς.

Συνοψίζοντας, το Πλαίσιο Κυβερνοασφάλειας 2.0 του NIST είναι ένα ισχυρό εργαλείο για τη βελτίωση της ασφάλειας των πληροφοριών στους ελληνικούς δημόσιους οργανισμούς. Παρά τις προκλήσεις που επισημάνθηκαν, η εμπειρία που αποκτήθηκε από την εφαρμογή του πλαισίου δείχνει ότι με τη σωστή προσέγγιση, τη σωστή εκπαίδευση και τη σωστή υποστήριξη, οι οργανισμοί μπορούν να ενισχύσουν την ανθεκτικότητά τους στις απειλές και να διασφαλίσουν την προστασία των δεδομένων.

Για να επιτευχθούν τα καλύτερα δυνατά αποτελέσματα, προτείνεται η υιοθέτηση των ακόλουθων συστάσεων:

1. **Εκπαίδευση και ευαισθητοποίηση:** Η συνεχής εκπαίδευση του προσωπικού σε θέματα ασφάλειας είναι απαραίτητη για τη μείωση του κινδύνου και την αύξηση της οργανωτικής ανθεκτικότητας.

2. **Επενδύσεις στην τεχνολογία και τους πόρους:** Η αναβάθμιση της τεχνολογικής υποδομής και η εξασφάλιση της διαθεσιμότητας των απαραίτητων πόρων είναι απαραίτητη για την επιτυχή εφαρμογή της πολιτικής ασφάλειας.

3. **Προώθηση της κουλτούρας ασφάλειας:** Η προώθηση μιας κουλτούρας ασφάλειας που διαπερνά όλες τις δραστηριότητες του οργανισμού είναι απαραίτητη για μακροπρόθεσμα αποτελέσματα.

4. **Συνεργασία και ανταλλαγή βέλτιστων πρακτικών:** Η συνεργασία με άλλους οργανισμούς και εμπειρογνώμονες στον τομέα μπορεί να συμβάλει στην ανταλλαγή γνώσεων και στη βελτίωση της ασφάλειας.

5. **Συνεχής βελτίωση και προσαρμογή**: Είναι απαραίτητο να βελτιώνονται συνεχώς οι πολιτικές και οι πρακτικές ασφάλειας και να προσαρμόζονται στις νέες τεχνολογικές και νομικές εξελίξεις, προκειμένου να αντιμετωπίζονται οι μελλοντικές προκλήσεις.

Με τη λήψη των παραπάνω μέτρων, οι ελληνικές δημόσιες αρχές μπορούν να ενισχύσουν την ασφάλεια στον κυβερνοχώρο και να συμβάλουν στη συνολική ασφάλεια και σταθερότητα της χώρας, προστατεύοντας αποτελεσματικά τα ευαίσθητα δεδομένα που βρίσκονται υπό τον έλεγχό τους.

Οι ραγδαίες τεχνολογικές εξελίξεις στον τομέα της ασφάλειας στον κυβερνοχώρο και οι αυξανόμενες απειλές στον κυβερνοχώρο ανοίγουν το δρόμο για πολλές ερευνητικές κατευθύνσεις. Η εφαρμογή του πλαισίου NIST CSF 2.0 στον Ελληνικό Οργανισμό Ελέγχου Πληροφοριακών Συστημάτων (Ε.Ο.Ε.Π.) παρέχει μια ισχυρή βάση για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων. Ωστόσο, απαιτείται περισσότερη έρευνα και εργασία για τη βελτίωση της ασφάλειας και την αντιμετώπιση των αναδυόμενων προκλήσεων.

Η Zero Trust Architecture είναι μια σχετικά νέα προσέγγιση στην κυβερνοασφάλεια, η οποία βασίζεται στην αρχή ότι κανένας χρήστης ή συσκευή εντός ή εκτός του δικτύου ενός οργανισμού δεν

θεωρείται εξ ορισμού αξιόπιστος. Η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στη χρήση της ZTA για την πλήρη προστασία των πληροφοριακών συστημάτων της OSSO. Η ανάπτυξη εργαλείων για τον εντοπισμό απειλών και την παρακολούθηση κάθε ενέργειας στο δίκτυο σε πραγματικό χρόνο μπορεί να αυξήσει σημαντικά την ανθεκτικότητα ενός οργανισμού στις εξελισσόμενες επιθέσεις στον κυβερνοχώρο.

Η τεχνητή νοημοσύνη (AI) και η μηχανική μάθηση (ML) έχουν τη δυνατότητα να επαναπροσδιορίσουν τον τρόπο με τον οποίο οι οργανισμοί ανιχνεύουν και ανταποκρίνονται στις απειλές στον κυβερνοχώρο. Η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στη χρήση αλγορίθμων ML για την αυτοματοποίηση της ανίχνευσης ανωμαλιών σε δίκτυα OSPF. Τέτοιες τεχνικές μπορούν να βοηθήσουν στην έγκαιρη ανίχνευση απειλών και να βελτιώσουν τις διαδικασίες αντιμετώπισης περιστατικών ασφαλείας.

Η κρυπτογράφηση αποτελεί θεμελιώδη πυλώνα της ασφάλειας στον κυβερνοχώρο, αλλά με την εμφάνιση νέων τεχνολογιών, όπως η κβαντική πληροφορική, οι παραδοσιακές τεχνικές κρυπτογράφησης ενδέχεται να μην επαρκούν. Η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στη χρήση αλγορίθμων κρυπτογράφησης ανθεκτικών στις κβάντες για την προστασία των κρίσιμων υποδομών του OSPF. Η έρευνα αυτή θα διασφαλίσει την προστασία των δεδομένων ενόψει των πολύ ισχυρών νέων τεχνολογιών υπολογιστικής ισχύος.

Το blockchain είναι μια τεχνολογία που αυξάνει τη διαφάνεια και την ακεραιότητα στην αποθήκευση και τη μεταφορά δεδομένων. Η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στην ενσωμάτωση της τεχνολογίας blockchain για την εγγύηση της ακεραιότητας των δεδομένων και των συναλλαγών του ΟΔΙΕ. Ένα αποκεντρωμένο σύστημα blockchain μπορεί να ενισχύσει την αξιοπιστία και την ιχνηλασιμότητα διασφαλίζοντας ότι τυχόν αλλαγές στα δεδομένα καταγράφονται, είναι αμετάβλητες και εύκολα προσβάσιμες.

Η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στην περαιτέρω αυτοματοποίηση της διαδικασίας αντιμετώπισης περιστατικών ασφαλείας. Τα συστήματα αυτόνομης αντιμετώπισης περιστατικών (AIR) θα μπορούσαν να αναπτύξουν εργαλεία που αντιδρούν αυτόματα σε επιθέσεις στον κυβερνοχώρο σε πραγματικό χρόνο, απομονώνουν τα προσβεβλημένα συστήματα και τα αποκαθιστούν χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αυτό συντομεύει τους χρόνους απόκρισης και περιορίζει τις ζημιές σε περίπτωση κυβερνοεπίθεσης.

Η μελλοντική έρευνα θα μπορούσε επίσης να επικεντρωθεί στην ενίσχυση της συνεργασίας μεταξύ των ελληνικών δημόσιων και ιδιωτικών φορέων για την αποτελεσματικότερη αντιμετώπιση των απειλών στον κυβερνοχώρο. Η ανταλλαγή γνώσεων και οι κοινές πρωτοβουλίες για την ενίσχυση της ασφάλειας στον κυβερνοχώρο θα μπορούσαν να αποτελέσουν σημαντική ερευνητική κατεύθυνση για την ενίσχυση της εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Anderson, R.J. "*Security engineering: a guide to building dependable distributed systems*", IEEE Computer Society Press, 31(4), 2001, pp. 94-95.

[2] Doe, J. "*Implementing NIST Framework in a Public Sector Organization*", Master's thesis, University of Athens, 2019.

[3] ENISA NIS 2 Directive: Key Changes and Implications, 2023 (Accessed: 18 August 2024) [Online]. Available at: https://www.enisa.europa.eu/topics/nis-directive

[4] European Commission Cybersecurity Act and NIS 2 Directive: Implementation in Member States. Brussels: European Commission, 2022.

[5] European Union Agency for Cybersecurity (ENISA), *The NIS2 Directive: Advancing the EU's Cybersecurity.* (online) Available at: https://www.enisa.europa.eu/publications/the-nis2-directive-advancing-the-eus-cybersecurity (Accessed 20 July 2024), 2021.

[6] European Union Agency for Cybersecurity (ENISA), *NIS2 Directive: Key Changes and Implications.* (online) Available at: https://www.enisa.europa.eu/publications/nis2-directive-key-changes-and-implications (Accessed 20 July 2024), 2022.

[7] Golling, M. and Hartenstein, H., "*Cybersecurity in Europe: Revisiting the network and information security directive*". International Journal of Information Security, 20(4), 2021, pp. 473-489.

[8] Korff, D. and Brown, I., "*Strengthening the EU's Cybersecurity rules: The NIS2 proposal*". Computer Law & Security Review, 41, 2021, pp. 105530.

[9] Maitland, C. and Toh, T., "*NIS2 Directive: An enhanced framework for cybersecurity in the EU*". Journal of Cyber Policy, 6(2), 2021, pp. 233-251.

[10] NIST Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://www.nist.gov/cyberframework (Accessed: 18 August 2024), 2018.

[11] Παπαδόπουλος, Κ. "*Η εξέλιξη της κυβερνοασφάλειας στην Ελλάδα: Από την εθνική στρατηγική στην εφαρμογή του NIS 2'*, Τεχνολογία και Κοινωνία, 12(4), 2022, σελ. 22-34.

[12] Pawlak, P. and Tikk, E., "*The NIS Directive: Implications for Europe's Cybersecurity*". European Foreign Affairs Review, 25(2), 2020, pp. 187-206.

[13] Peltier, T.R., Peltier, J. and Blackley, J. *Information Security Fundamentals*. Boca Raton, FL: Auerbach Publications, 2005.

[14] Schmidt, A. and Schaller, C., "*NIS2 Directive: Challenges and opportunities for cybersecurity in the EU*". Journal of Strategic Security, 14(3), 2021, pp. 48-64.

[15] ΣΕΠΕ Κυβερνοασφάλεια και Δημόσιος Τομέας: Η Ελληνική Εμπειρία. Αθήνα: Σύνδεσμος Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδας, 2021.

[16] Smith, J., White, A. and Brown, C. "*Cybersecurity risk assessment for critical infrastructu*", Journal of Cybersecurity, 3(2), 2010, pp. 23-30.

[17] Stallings, W. *Network Security Essentials: Applications and Standards*. 6th edn. Upper Saddle River, NJ: Pearson Education, 2020.

[18] Van Hecke, W. and Vanhamel, K., "*NIS2: The EU's updated approach to cybersecurity*". Computer fraud & security, 2022(4), 2022, pp. 9-15.

[19] Wilson, C. *State of Cybersecurity in Public Sector*. NIST, Washington D.C. Available at: https://www.nist.gov/report2020 (Accessed: 18 August 2024), 2020.

[20] Υπουργείο Ψηφιακής Διακυβέρνησης Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (NIS) και η εφαρμογή της στην Ελλάδα, 2021.

[21] ENISA (2023) National Cybersecurity Strategies: ENISA. Διαθέσιμο στο: https://www.enisa.europa.eu/topics/national-cyber-security-strategies (Πρόσβαση 7 Σεπτεμβρίου 2024).

[22] NIST (2023) NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology. Διαθέσιμο στο: https://www.nist.gov/cyberframework (Πρόσβαση 7 Σεπτεμβρίου 2024).

[23] ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 – 2025. Διαθέσιμο στο: https://mindigital.gr/dioikisi/kyvernoasfaleia (Πρόσβαση 8 Σεπτεμβρίου 2024)..