Το Πλαίσιο Κυβερνοασφάλειας NIST (CSF) 2.0

Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας
Η παρούσα αγγλική έκδοση διατίθεται δωρεάν από: https://doi.org/10.6028/NIST.CSWP.29.gre
26 Φεβρουαρίου 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Μεταφράστηκε από τα μέλη του Ελληνικού Παραρτήματος του Διεθνούς Ινστιτούτου για την Ασφάλεια Πληροφοριακών Συστημάτων (ISC)2: Μαρία ΜΠΡΕΜΠΟΥ, Ιωάννα ΔΗΜΑ, Δημήτρης ΓΕΩΡΓΙΟΥ, Γιάννης ΠΑΥΛΟΣΟΓΛΟΥ, Σπύρος ΠΙΤΙΚΑΡΗΣ, Παναγιώτης ΣΟΥΛΟΣ.
Η μετάφραση έγινε με την ευγενή άδεια του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST). Η επιμέλεια της μετάφρασης έγινε για λογαριασμό του NIST από την TaikaTranslations LLC βάσει σύμβασης {133ND23PNB770271}. Επίσημη μετάφραση για την Κυβέρνηση των Η.Π.Α. Με την επιφύλαξη παντός νόμιμου δικαιώματος, Υπουργός Εμπορίου ΗΠΑ.

Translated by members of the (ISC)2 Hellenic Chapter: Maria BREMPOU, Ioanna DIMA, Dimitris GEORGIOU, Yiannis PAVLOSOGLOU, Spiros PITIKARIS, Panagiotis SOULOS.
Translated with permission courtesy of the National Institute of Standards and Technology (NIST). Translation reviewed on behalf of NIST by TaikaTranslations LLC under contract {133ND23PNB770271}. Official U.S. Government Translation. All rights reserved, US Secretary of Commerce.

Σύνοψη

Η έκδοση 2.0 του Πλαισίου Κυβερνοασφάλειας (CSF – Cybersecurity Framework, εφεξής Πλαίσιο) του Εθνικού Ινστιτούτου Επιστήμης και Τεχνολογίας των Η.Π.Α. (NIST – National Institute of Standards and Technology) παρέχει στη βιομηχανία, σε κυβερνητικές υπηρεσίες και άλλους οργανισμούς καθοδήγηση για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Προσφέρει μια ταξινόμηση επιθυμητών αποτελεσμάτων κυβερνοασφάλειας υψηλού επιπέδου, η οποία μπορεί να χρησιμοποιηθεί από κάθε οργανισμό – ανεξαρτήτως μεγέθους, κλάδου ή ωριμότητας – προκειμένου να κατανοήσει καλύτερα, να αξιολογήσει, να ιεραρχήσει και να επικοινωνήσει τις προσπάθειές του στον τομέα της κυβερνοασφάλειας. Το Πλαίσιο δεν υπαγορεύει τον τρόπο με τον οποίο πρέπει να επιτυγχάνονται τα επιθυμητά αποτελέσματα. Αντ' αυτού, παραπέμπει σε διαδικτυακούς πόρους, οι οποίοι παρέχουν πρόσθετη καθοδήγηση σχετικά με πρακτικές και σημεία ελέγχου ασφάλειας που θα μπορούσαν να χρησιμοποιηθούν για την επίτευξη των εν λόγω αποτελεσμάτων. Αυτό το έγγραφο περιγράφει τη δεύτερη έκδοση (2.0) του Πλαισίου, τα στοιχεία του και μερικούς από τους πολλούς τρόπους που μπορεί να χρησιμοποιηθεί.

Λέξεις Κλειδιά

κυβερνοασφάλεια, Πλαίσιο Κυβερνοασφάλειας (Πλαίσιο), διακυβέρνηση κινδύνων κυβερνοασφάλειας, διαχείριση κινδύνων κυβερνοασφάλειας, διαχείριση επιχειρηματικών κινδύνων, Προφίλ, Βαθμίδες.

Αποδέκτες

Οι κύριοι αποδέκτες του Πλαισίου είναι τα άτομα που είναι υπεύθυνα για την ανάπτυξη και την ηγεσία προγραμμάτων κυβερνοασφάλειας. Το Πλαίσιο μπορεί, επίσης, να χρησιμοποιηθεί και από άλλους που εμπλέκονται στη διαχείριση κινδύνων – συμπεριλαμβανομένων των στελεχών, των συμβουλίων διοίκησης, των επαγγελματιών που ασχολούνται με εξαγορές, των τεχνολόγων, των διαχειριστών κινδύνων, των δικηγόρων, των ειδικών ανθρωπίνου δυναμικού και των ελεγκτών κυβερνοασφάλειας και διαχείρισης κινδύνων – για να καθοδηγήσει τις σχετικές με την κυβερνοασφάλεια αποφάσεις τους. Επιπλέον, το Πλαίσιο μπορεί να είναι χρήσιμο σε όσους διαμορφώνουν και επηρεάζουν πολιτικές (π.χ. σωματεία, επαγγελματικές οργανώσεις, ρυθμιστικές αρχές), οι οποίοι θέτουν και επικοινωνούν προτεραιότητες για τη διαχείριση κινδύνων κυβερνοασφάλειας.

Συμπληρωματικό Περιεχόμενο

Το NIST θα συνεχίσει να αναπτύσσει και να φιλοξενεί επιπλέον υλικό για να βοηθήσει τους ενδιαφερόμενους οργανισμούς να εφαρμόσουν το Πλαίσιο, όπως Οδηγούς Γρήγορης Εκκίνησης (QSG – Quick Start Guides) και Κοινοτικά Προφίλ. Όλο το υλικό θα είναι δημοσίως διαθέσιμο στην ιστοσελίδα του Πλαισίου. Προτάσεις για επιπλέον υλικό για συμπερίληψη

στην ιστοσελίδα του Πλαισίου μπορούν να αποστέλλονται στο NIST στη διεύθυνση ηλεκτρονικού ταχυδρομείου cyberframework@nist.gov.

Σημείωση για τους Αναγνώστες

Σημειώνεται ότι, εκτός αν αναφέρεται κάτι διαφορετικό, τα έγγραφα που μνημονεύονται ή παρατίθενται δεν ενσωματώνονται πλήρως σε αυτή τη δημοσίευση.

Πριν από την έκδοση 2.0, το Πλαίσιο Κυβερνοασφάλειας ονομαζόταν «Πλαίσιο για τη Βελτίωση της Κυβερνοασφάλειας των Κρίσιμων Υποδομών». Αυτός ο τίτλος δεν χρησιμοποιείται για την έκδοση 2.0.

Ευχαριστίες

Το Πλαίσιο είναι αποτέλεσμα πολυετούς συνεργασίας βιομηχανίας, πανεπιστημίων και κυβερνητικών οργανισμών τόσο στις Ηνωμένες Πολιτείες, όσο και στον υπόλοιπο κόσμο. Το NIST αναγνωρίζει και ευχαριστεί όλους, όσοι έχουν συμβάλει σε αυτή την αναθεωρημένη έκδοση του Πλαισίου. Πληροφορίες για τη διαδικασία ανάπτυξης του Πλαισίου υπάρχουν στην ιστοσελίδα του Πλαισίου. Διδάγματα από την αξιοποίηση του Πλαισίου μπορούν να αποστέλλονται στο NIST στην ηλεκτρονική διεύθυνση cyberframework@nist.gov.

Πίνακας Περιεχομένων

Κατάλογος Σχημάτων

Πρόλογος

Το Πλαίσιο Κυβερνοασφάλειας 2.0 (το Πλαίσιο) έχει σχεδιαστεί για να βοηθήσει οργανισμούς κάθε μεγέθους και κλάδου – συμπεριλαμβανομένων βιομηχανικών, κυβερνητικών, ακαδημαϊκών και μη κερδοσκοπικών οργανισμών – να διαχειριστούν και να μειώσουν τους κινδύνους κυβερνοασφάλειας που αντιμετωπίζουν. Έχει χρησιμότητα ανεξάρτητα από το επίπεδο ωριμότητας και την τεχνική εξειδίκευση των προγραμμάτων κυβερνοασφάλειας κάθε οργανισμού. Παρ' όλα αυτά, το Πλαίσιο δεν ακολουθεί μια ενιαία προσέγγιση για κάθε τύπο ανάγκης. Κάθε οργανισμός αντιμετωπίζει κινδύνους που είναι κοινοί με άλλους οργανισμούς, αλλά και κινδύνους που τον απειλούν ατομικά, και εμφανίζει διαφορετική διάθεση ανάληψης ρίσκου και διαφορετική ανοχή στους κινδύνους, ξεχωριστή αποστολή, και στόχους για την επίτευξη αυτής της αποστολής. Ο τρόπος με τον οποίο διαφορετικοί οργανισμοί εφαρμόζουν το Πλαίσιο αναγκαστικά διαφέρει.

Ιδανικά, το Πλαίσιο θα χρησιμοποιηθεί για να αντιμετωπίσει κινδύνους κυβερνοασφάλειας παράλληλα με άλλους επιχειρηματικούς κινδύνους, όπως οικονομικοί κίνδυνοι, κίνδυνοι ιδιωτικότητας, κίνδυνοι αλυσίδας εφοδιασμού, φήμης, τεχνολογικοί ή φυσικοί κίνδυνοι.

Το Πλαίσιο *περιγράφει* επιθυμητά αποτελέσματα, σκοπός των οποίων είναι να γίνουν αντιληπτά σ΄ ένα ευρύ κοινό, αποτελούμενο από στελέχη, διευθυντές και επαγγελματίες, ανεξάρτητα από την ειδίκευσή τους στην κυβερνοασφάλεια. Επειδή αυτά τα αποτελέσματα είναι ανεξάρτητα από κλάδο, χώρα και τεχνολογία, παρέχουν σε έναν οργανισμό την ευελιξία που χρειάζεται για να αντιμετωπίσει τους ιδιαίτερους κινδύνους του, τις τεχνολογικές ανάγκες και τις ιδιαιτερότητες της αποστολής του. Τα αποτελέσματα ομαδοποιούνται απευθείας σε μια λίστα πιθανών σημείων ελέγχου ασφάλειας για άμεση εξέταση, προκειμένου να μετριαστούν οι κίνδυνοι κυβερνοασφάλειας.

Αν και δεν το προδιαγράφει επακριβώς, το Πλαίσιο βοηθά τους χρήστες του να μαθαίνουν και να επιλέγουν συγκεκριμένα αποτελέσματα. Προτάσεις για το πώς μπορούν να επιτευχθούν συγκεκριμένα αποτελέσματα περιέχονται σε μια διευρυνόμενη ομάδα διαδικτυακών πηγών που συμπληρώνουν το Πλαίσιο, στις οποίες συμπεριλαμβάνεται μια σειρά από Οδηγούς Γρήγορης Εκκίνησης (QSG ή Οδηγοί). Επίσης, σε οργανισμούς που επιλέγουν να αυτοματοποιήσουν ορισμένες από τις διαδικασίες τους προσφέρονται προς λήψη διάφορα εργαλεία. Οι Οδηγοί προτείνουν ορισμένους αρχικούς τρόπους χρήσης του Πλαισίου και προσκαλούν τον αναγνώστη να εξερευνήσει το Πλαίσιο και το συμπληρωματικό υλικό σε μεγαλύτερο βάθος. Το Πλαίσιο και το συμπληρωματικό υλικό που διατίθεται από το NIST και άλλους στην ιστοσελίδα του Πλαισίου, θα πρέπει να θεωρούνται ως η «Εργαλειοθήκη του Πλαισίου» που βοηθά στη διαχείριση και μείωση των κινδύνων. Ανεξάρτητα από το πώς εφαρμόζεται, το Πλαίσιο προτρέπει τους χρήστες του να λαμβάνουν υπόψη τους τη στάση τους ως προς την κυβερνοασφάλεια και στη συνέχεια να προσαρμόζουν το Πλαίσιο στις ιδιαίτερες ανάγκες τους.

Βασιζόμενη στις προηγούμενες εκδόσεις, η έκδοση 2.0 του Πλαισίου περιέχει και νέα χαρακτηριστικά που υπογραμμίζουν τη σημασία *της διακυβέρνησης και της αλυσίδας εφοδιασμού*. Ιδιαίτερη προσοχή δίνεται στους Οδηγούς (QSG), ώστε να διασφαλιστεί ότι το

Πλαίσιο είναι εξίσου χρήσιμο και εύκολα προσβάσιμο σε μικρούς και μεγάλους οργανισμούς. Το NIST πλέον παρέχει *Παραδείγματα Υλοποίησης* και *Πληροφοριακές Αναφορές*, τα οποία είναι διαθέσιμα διαδικτυακά και ενημερώνονται τακτικά. Η δημιουργία Οργανωτικών Προφίλ της τρέχουσας κατάστασης και της κατάστασης-στόχου βοηθά τους οργανισμούς να συγκρίνουν πού βρίσκονται σε σχέση με πού θέλουν ή πρέπει να βρεθούν, και τους επιτρέπει να εφαρμόζουν και να αξιολογούν ταχύτερα τα σημεία ελέγχου ασφάλειας.

Οι κίνδυνοι κυβερνοασφάλειας διευρύνονται συνεχώς και η διαχείρισή τους πρέπει να είναι μια συνεχής διαδικασία. Αυτό ισχύει ανεξάρτητα από αν ένας οργανισμός βρίσκεται στο αρχικό στάδιο αντιμετώπισης των προκλήσεών του σχετικά με την κυβερνοασφάλεια ή αν δραστηριοποιείται στο πεδίο αυτό αρκετά χρόνια με μια εξελιγμένη, καλά στελεχωμένη ομάδα κυβερνοασφάλειας. Το Πλαίσιο έχει σχεδιαστεί, ώστε να είναι πολύτιμο για οποιοδήποτε είδος οργανισμού και αναμένεται να παρέχει κατάλληλη καθοδήγηση για μεγάλο χρονικό διάστημα.

1. Επισκόπηση του Πλαισίου Κυβερνοασφάλειας

Αυτό το έγγραφο είναι η έκδοση 2.0 του Πλαισίου Κυβερνοασφάλειας του NIST (CSF), το οποίο απαρτίζουν τα ακόλουθα στοιχεία:

- ***Πυρήνας του Πλαισίου***, το επίκεντρο του Πλαισίου, το οποίο είναι μια ταξινόμηση υψηλού επιπέδου επιθυμητών αποτελεσμάτων κυβερνοασφάλειας, τα οποία μπορούν να βοηθήσουν οποιονδήποτε οργανισμό να διαχειριστεί τους δικούς του κινδύνους κυβερνοασφάλειας. Τα στοιχεία του Πυρήνα του Πλαισίου είναι μία ιεραρχία από Λειτουργίες, Κατηγορίες και Υποκατηγορίες που περιγράφουν λεπτομερώς το κάθε αποτέλεσμα. Αυτά τα αποτελέσματα μπορούν να γίνουν κατανοητά από ένα ευρύ κοινό, συμπεριλαμβανομένων στελεχών, διευθυντών και επαγγελματιών, ανεξάρτητα από την εξειδίκευσή τους στον τομέα της κυβερνοασφάλειας. Επειδή τα αποτελέσματα είναι ουδέτερα ως προς τον κλάδο, τη χώρα και την τεχνολογία, παρέχουν σε έναν οργανισμό την ευελιξία που απαιτείται για να διαχειριστεί τους εξατομικευμένους κινδύνους του, τις τεχνολογίες και τις ιδιαιτερότητες της αποστολής του.
- ***Οργανωτικά Προφίλ του Πλαισίου***, αποτελούν ένα μηχανισμό για την περιγραφή της τρέχουσας ή/και επιθυμητής στάσης κυβερνοασφάλειας ενός οργανισμού απέναντι στα αποτελέσματα του Πυρήνα του Πλαισίου.
- ***Βαθμίδες του Πλαισίου***, οι οποίες μπορούν να εφαρμοστούν στα Οργανωτικά Προφίλ του Πλαισίου για να χαρακτηρίσουν την αυστηρότητα των πρακτικών διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας ενός οργανισμού. Οι Βαθμίδες μπορούν, επίσης, να αποτελέσουν το περίγραμμα στο οποίο ένας οργανισμός αντιλαμβάνεται τους κινδύνους κυβερνοασφάλειας και τις διαδικασίες που υπάρχουν για τη διαχείριση των κινδύνων αυτών.

Αυτό το έγγραφο περιγράφει *ποια* επιθυμητά αποτελέσματα μπορεί να φιλοδοξεί να πετύχει ένας οργανισμός. Δεν *ορίζει* αποτελέσματα, ούτε *πώς* αυτά μπορούν να επιτευχθούν. Περιγραφές για το *πώς* ένας οργανισμός μπορεί να επιτύχει αυτά τα αποτελέσματα παρέχονται στο πλήθος του διαδικτυακού υλικού που συμπληρώνει το Πλαίσιο και είναι διαθέσιμο μέσω της ιστοσελίδας του Πλαισίου. Αυτό το υλικό παρέχει πρόσθετη καθοδήγηση σχετικά με πρακτικές και σημεία ελέγχου ασφάλειας που θα μπορούσαν να χρησιμοποιηθούν για την επίτευξη αποτελεσμάτων, και η πρόθεσή τους είναι να βοηθήσουν έναν οργανισμό να κατανοήσει, να υιοθετήσει και να χρησιμοποιήσει το Πλαίσιο. Στο υλικό αυτό περιλαμβάνονται:

- *Πληροφοριακές Αναφορές* που οδηγούν σε πηγές καθοδήγησης για κάθε αποτέλεσμα από υπάρχοντα παγκόσμια πρότυπα, κατευθυντήριες γραμμές, πλαίσια, κανονισμούς, πολιτικές, κ.λπ.
- *Παραδείγματα Εφαρμογής* που απεικονίζουν πιθανούς τρόπους επίτευξης κάθε αποτελέσματος

- *Οδηγοί Γρήγορης Εκκίνησης* που παρέχουν πρακτικές οδηγίες σχετικά με τη χρήση του Πλαισίου και του διαδικτυακού υλικού του, συμπεριλαμβανομένου του τρόπου μετάβασης από προηγούμενες εκδόσεις του Πλαισίου στην έκδοση 2.0.
- *Κοινοτικά Προφίλ και Πρότυπα Οργανωτικά Προφίλ* που βοηθούν τους οργανισμούς να εφαρμόσουν το Πλαίσιο στην πράξη και να θέσουν προτεραιότητες για τη διαχείριση των κινδύνων κυβερνοασφάλειας.

Οι οργανισμοί μπορούν να χρησιμοποιήσουν τον Πυρήνα, τα Προφίλ και τις Βαθμίδες του Πλαισίου μαζί με το συμπληρωματικό υλικό για να κατανοήσουν, να αξιολογήσουν, να ιεραρχήσουν και να επικοινωνήσουν σχετικά με τους κινδύνους κυβερνοασφάλειας.

- **Κατανόηση και Αξιολόγηση:** Περιγραφή της τρέχουσας ή της επιθυμητής στάσης ενός τμήματος ή και ολόκληρου του οργανισμού έναντι της κυβερνοασφάλειας, προσδιορισμός ελλείψεων και αξιολόγηση της προόδου ως προς την αντιμετώπιση αυτών των ελλείψεων.
- **Ιεράρχηση:** Προσδιορισμός, οργάνωση και ιεράρχηση ενεργειών για τη διαχείριση κινδύνων κυβερνοασφάλειας που ευθυγραμμίζονται με την αποστολή του οργανισμού, τις νομικές και κανονιστικές απαιτήσεις και τις προσδοκίες διαχείρισης κινδύνων και διακυβέρνησης.
- **Επικοινωνία:** Χρήση κοινής γλώσσας για την επικοινωνία εντός και εκτός του οργανισμού σχετικά με τους κινδύνους κυβερνοασφάλειας, τις δυνατότητες, τις ανάγκες και τις προσδοκίες.

Το Πλαίσιο σχεδιάστηκε για να χρησιμοποιηθεί από οργανισμούς όλων των μεγεθών και κλάδων, συμπεριλαμβανομένων βιομηχανικών, κυβερνητικών, ακαδημαϊκών και μη κερδοσκοπικών οργανισμών, ανεξάρτητα από το επίπεδο ωριμότητας των προγραμμάτων κυβερνοασφάλειάς τους. Το Πλαίσιο είναι ένας θεμελιώδης πόρος που μπορεί να υιοθετηθεί είτε εθελοντικά, είτε μέσω κυβερνητικών πολιτικών και υποχρεωτικών κανονισμών. Η ταξινόμηση του Πλαισίου και τα αναφερόμενα πρότυπα, οι κατευθυντήριες γραμμές και οι πρακτικές δεν αφορούν συγκεκριμένες χώρες. Μάλιστα προηγούμενες εκδόσεις του Πλαισίου έχουν αξιοποιηθεί με επιτυχία από πολλές κυβερνήσεις και άλλους οργανισμούς τόσο εντός όσο και εκτός των Ηνωμένων Πολιτειών.

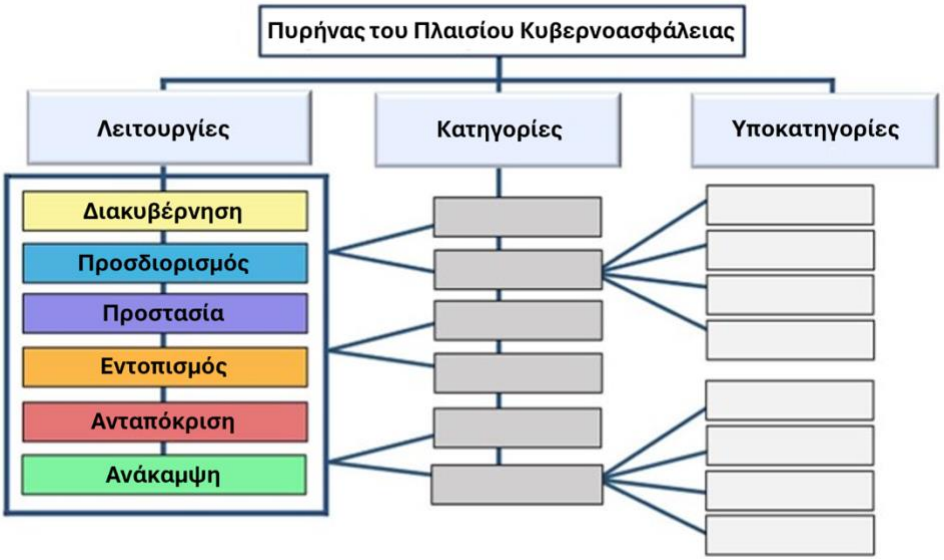
Το Πλαίσιο θα πρέπει να χρησιμοποιείται σε συνδυασμό με άλλους πόρους (π.χ. πλαίσια, πρότυπα, κατευθυντήριες γραμμές, βέλτιστες πρακτικές) για την καλύτερη διαχείριση των κινδύνων κυβερνοασφάλειας και την επικαιροποίηση της συνολικής διαδικασίας διαχείρισης κινδύνων των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ) (ICT – Information and Communication Technology) σε επίπεδο επιχείρησης. Το Πλαίσιο είναι ευέλικτο και μπορεί να χρησιμοποιηθεί από όλους τους οργανισμούς ανεξαρτήτως μεγέθους. Κάθε οργανισμός θα συνεχίσει να έχει ξεχωριστούς κινδύνους – συμπεριλαμβανομένων διαφορετικών απειλών και ευπαθειών – και ανοχή στους κινδύνους αυτούς, καθώς και μοναδικούς στόχους ως προς την αποστολή και τις απαιτήσεις του. Επομένως, οι προσεγγίσεις των οργανισμών για τη διαχείριση των κινδύνων τους και οι υλοποιήσεις του Πλαισίου θα ποικίλλουν.

Το υπόλοιπο αυτού του εγγράφου είναι δομημένο ως εξής:

- Η Ενότητα 2 εξηγεί τα βασικά στοιχεία του Πυρήνα του Πλαισίου: Λειτουργίες, Κατηγορίες και Υποκατηγορίες.
- Η Ενότητα 3 ορίζει τις έννοιες των Προφίλ και Βαθμίδων του Πλαισίου.
- Η Ενότητα 4 αποτελεί μια επισκόπηση επιλεγμένων στοιχείων από το διαδικτυακό υλικό του Πλαισίου, όπως Πληροφοριακών Αναφορών, Παραδειγμάτων Εφαρμογής και Οδηγών Γρήγορης Εκκίνησης.
- Η Ενότητα 5 πραγματεύεται πώς ένας οργανισμός μπορεί να ενοποιήσει το Πλαίσιο με άλλα προγράμματα διαχείρισης κινδύνων.
- Το Παράρτημα Α είναι ο Πυρήνας του Πλαισίου.
- Το Παράρτημα Β περιέχει μια απεικόνιση των Βαθμίδων του Πλαισίου.
- Το Παράρτημα Γ περιέχει έναν πίνακα όρων του Πλαισίου.

2. Εισαγωγή στον Πυρήνα του Πλαισίου

Το Παράρτημα Α είναι ο Πυρήνας του Πλαισίου – μια σειρά από αποτελέσματα κυβερνοασφάλειας που έχουν διευθετηθεί ανά Λειτουργία, Κατηγορία και εν τέλει Υποκατηγορία, όπως απεικονίζεται στο Σχήμα 1. Τα αποτελέσματα αυτά δεν αποτελούν μια λίστα από ενέργειες που πρέπει να εκτελεστούν. Οι συγκεκριμένες ενέργειες που πρέπει να αναληφθούν για να επιτευχθεί ένα αποτέλεσμα θα ποικίλουν ανάλογα με τον οργανισμό και το εκάστοτε σενάριο εφαρμογής, όπως και ανάλογα με το άτομο που είναι υπεύθυνο για αυτές τις ενέργειες. Επιπρόσθετα, η σειρά και το μέγεθος των Λειτουργιών, Κατηγοριών και Υποκατηγοριών στον Πυρήνα δεν προσδιορίζει την ακολουθία και τη σημασία επίτευξής τους. Η δομή του Πυρήνα έχει σχεδιαστεί με στόχο να ανταποκρίνεται κυρίως στις ανάγκες εκείνων που έχουν αναλάβει την ενσωμάτωση της διαχείρισης κινδύνου στις λειτουργικές διαδικασίες ενός οργανισμού.



Σχήμα 1. Δομή του Πυρήνα του Πλαισίου

Οι Λειτουργίες του Πυρήνα του Πλαισίου – ΔΙΑΚΥΒΕΡΝΗΣΗ, ΠΡΟΣΔΙΟΡΙΣΜΟΣ, ΠΡΟΣΤΑΣΙΑ, ΕΝΤΟΠΙΣΜΟΣ, ΑΝΤΑΠΟΚΡΙΣΗ, και ΑΝΑΚΑΜΨΗ – οργανώνουν τα αποτελέσματα κυβερνοασφάλειας στο υψηλότερο επίπεδό τους.

- **ΔΙΑΚΥΒΕΡΝΗΣΗ (GV)** – *Καθορίζεται, κοινοποιείται και εποπτεύεται η στρατηγική διαχείρισης κινδύνων κυβερνοασφάλειας, οι προσδοκίες και η πολιτική του οργανισμού.* Η Λειτουργία ΔΙΑΚΥΒΕΡΝΗΣΗ παρέχει αποτελέσματα που αποτυπώνουν τι μπορεί να κάνει ένας οργανισμός για την επίτευξη και την ιεράρχηση των αποτελεσμάτων των άλλων πέντε Λειτουργιών, στο πλαίσιο της αποστολής του και των προσδοκιών των ενδιαφερόμενων μερών. Οι δραστηριότητες διακυβέρνησης είναι κρίσιμες για την ενσωμάτωση της κυβερνοασφάλειας στην ευρύτερη στρατηγική της Διαχείρισης Επιχειρηματικών Κινδύνων (ERM – Enterprise Risk Management) ενός οργανισμού. Η ΔΙΑΚΥΒΕΡΝΗΣΗ αναφέρεται στην κατανόηση του οργανωτικού πλαισίου, στην καθιέρωση στρατηγικής κυβερνοασφάλειας και διαχείρισης κινδύνων

κυβερνοασφάλειας που πηγάζει από την εφοδιαστική αλυσίδα, σε ρόλους, ευθύνες και αρμοδιότητες, στη πολιτική και στην εποπτεία της στρατηγικής κυβερνοασφάλειας.

- **ΠΡΟΣΔΙΟΡΙΣΜΟΣ (ID)** – *Κατανοούνται οι τρέχοντες κίνδυνοι κυβερνοασφάλειας ενός οργανισμού.* Η κατανόηση των πληροφοριακών αγαθών του οργανισμού (π.χ. δεδομένων, υλικού, λογισμικού, συστημάτων, εγκαταστάσεων, υπηρεσιών, ανθρώπων), των προμηθευτών και των σχετικών κινδύνων κυβερνοασφάλειας επιτρέπει σε έναν οργανισμό να ιεραρχήσει τις προσπάθειές του σύμφωνα με τη στρατηγική διαχείρισης των κινδύνων του και τις ανάγκες της αποστολής του, όπως έχουν προσδιοριστεί στη ΔΙΑΚΥΒΕΡΝΗΣΗ. Αυτή η Λειτουργία, επίσης, περιλαμβάνει τον εντοπισμό ευκαιριών βελτίωσης για τις πολιτικές, τα σχέδια, τις διαδικασίες, τις διεργασίες και τις πρακτικές του οργανισμού που υποστηρίζουν τη διαχείριση κινδύνων κυβερνοασφάλειας, προκειμένου να εμπλουτιστούν οι προσπάθειες και στις έξι Λειτουργίες.
- **ΠΡΟΣΤΑΣΙΑ (PR)** – *Αξιοποιούνται μέτρα προστασίας για τη διαχείριση των κινδύνων κυβερνοασφάλειας του οργανισμού.* Όταν τα πληροφοριακά αγαθά και οι κίνδυνοι έχουν προσδιοριστεί και ιεραρχηθεί, η ΠΡΟΣΤΑΣΙΑ υποστηρίζει τη δυνατότητα διασφάλισης αυτών των πληροφοριακών αγαθών, προκειμένου να αποφευχθεί ή να ελαττωθεί η πιθανότητα και οι επιπτώσεις δυσμενών συμβάντων κυβερνοασφάλειας, αλλά και να αυξηθεί η πιθανότητα και η επίδραση από την αξιοποίηση ευκαιριών. Τα αποτελέσματα που καλύπτονται από αυτή τη Λειτουργία περιλαμβάνουν τη διαχείριση ταυτότητας, την αυθεντικοποίηση και τον έλεγχο πρόσβασης, την ευαισθητοποίηση και την εκπαίδευση, την ασφάλεια δεδομένων, την ασφάλεια πλατφόρμας (δηλ. την ασφάλιση του υλικού, του λογισμικού και των υπηρεσιών των φυσικών και εικονικών πλατφορμών) και την ανθεκτικότητα των τεχνολογικών υποδομών.
- **ΕΝΤΟΠΙΣΜΟΣ (DE)** – *Εντοπίζονται και αναλύονται πιθανές επιθέσεις και παραβιάσεις κυβερνοασφάλειας.* Ο ΕΝΤΟΠΙΣΜΟΣ καθιστά ικανή την έγκαιρη ανακάλυψη και ανάλυση ανωμαλιών, δεικτών παραβίασης και άλλων πιθανών δυσμενών συμβάντων που ενδέχεται να υποδεικνύουν ότι συμβαίνουν κυβερνοεπιθέσεις και περιστατικά κυβερνοασφάλειας. Αυτή η Λειτουργία υποστηρίζει την επιτυχή ανταπόκριση σε περιστατικά ασφάλειας και τις δραστηριότητες ανάκαμψης από αυτά.
- **ΑΝΤΑΠΟΚΡΙΣΗ (RS)** – *Αναλαμβάνονται δράσεις για την αντιμετώπιση ενός εντοπισμένου περιστατικού κυβερνοασφάλειας.* Η ΑΝΤΑΠΟΚΡΙΣΗ υποστηρίζει τη δυνατότητα περιορισμού των επιπτώσεων των περιστατικών κυβερνοασφάλειας. Τα αποτελέσματα που περιλαμβάνονται σε αυτή τη Λειτουργία καλύπτουν τη διαχείριση, την ανάλυση, τη μετρίαση, την αναφορά και την επικοινωνία περιστατικών.
- **ΑΝΑΚΑΜΨΗ (RC)** – *Αποκαθίστανται τα πληροφοριακά αγαθά και οι λειτουργίες που επηρεάζονται από ένα περιστατικό κυβερνοασφάλειας.* Η ΑΝΑΚΑΜΨΗ υποστηρίζει την έγκαιρη αποκατάσταση των κανονικών λειτουργιών για να μειώσει τις επιδράσεις των περιστατικών κυβερνοασφάλειας και για να καταστήσει δυνατή την κατάλληλη επικοινωνία κατά τη διάρκεια των προσπαθειών ανάκαμψης.

Ενώ πολλές δραστηριότητες διαχείρισης κινδύνων κυβερνοασφάλειας επικεντρώνονται στην πρόληψη αρνητικών γεγονότων, οι ίδιες δραστηριότητες μπορούν επίσης να υποστηρίξουν την αξιοποίηση ευκαιριών. Οι ενέργειες για τη μείωση κινδύνων κυβερνοασφάλειας θα μπορούσαν να ωφελήσουν έναν οργανισμό με άλλους τρόπους, όπως με αύξηση εσόδων (π.χ. αρχικά με τη διάθεση πλεονάζοντος χώρου εγκαταστάσεων σε έναν εμπορικό πάροχο φιλοξενίας για τη φιλοξενία των δικών του κέντρων δεδομένων και των κέντρων δεδομένων άλλων οργανισμών και στη συνέχεια με τη μετακίνηση ενός σημαντικού πληροφοριακού συστήματος οικονομικής διαχείρισης του οργανισμού από το εσωτερικό κέντρο δεδομένων του στον πάροχο φιλοξενίας με σκοπό τη μείωση των κινδύνων κυβερνοασφάλειας).

Το Σχήμα 2 παρουσιάζει τις Λειτουργίες του Πλαισίου με ένα κυκλικό σχήμα επειδή όλες οι Λειτουργίες σχετίζονται μεταξύ τους. Για παράδειγμα, ένας οργανισμός θα κατατάξει τα πληροφοριακά αγαθά εντός του ΠΡΟΣΔΙΟΡΙΣΜΟΥ και θα λάβει μέτρα για την ασφάλεια αυτών των αγαθών εντός της ΠΡΟΣΤΑΣΙΑΣ. Οι επενδύσεις σε σχεδιασμό και δοκιμές στις Λειτουργίες ΔΙΑΚΥΒΕΡΝΗΣΗΣ και ΠΡΟΣΔΙΟΡΙΣΜΟΥ θα υποστηρίξουν την έγκαιρη ανίχνευση απροσδόκητων συμβάντων στη Λειτουργία ΕΝΤΟΠΙΣΜΟΥ και θα επιτρέψουν δράσεις ανταπόκρισης και ανάκαμψης από περιστατικά κυβερνοασφάλειας στις Λειτουργίες ΑΝΤΑΠΟΚΡΙΣΗΣ και ΑΝΑΚΑΜΨΗΣ. Η ΔΙΑΚΥΒΕΡΝΗΣΗ βρίσκεται στο κέντρο του κύκλου επειδή παρέχει πληροφορίες για το πώς ένας οργανισμός θα υλοποιήσει τις άλλες πέντε Λειτουργίες.

Σχήμα 2. Οι Λειτουργίες του Πλαισίου

Οι Λειτουργίες θα πρέπει να λαμβάνουν την απαιτούμενη προσοχή ταυτόχρονα. Δράσεις που υποστηρίζουν τη ΔΙΑΚΥΒΕΡΝΗΣΗ, τον ΠΡΟΣΔΙΟΡΙΣΜΟ, την ΠΡΟΣΤΑΣΙΑ και τον ΕΝΤΟΠΙΣΜΟ θα πρέπει να

εκτελούνται διαρκώς, ενώ δράσεις που υποστηρίζουν την ΑΝΤΑΠΟΚΡΙΣΗ και την ΑΝΑΚΑΜΨΗ θα πρέπει να είναι πάντα έτοιμες και να λάβουν χώρα όταν έχουμε περιστατικά κυβερνοασφάλειας. Όλες οι Λειτουργίες διαδραματίζουν ζωτικό ρόλο σε σχέση με τα περιστατικά κυβερνοασφάλειας. Τα αποτελέσματα της ΔΙΑΚΥΒΕΡΝΗΣΗΣ, του ΠΡΟΣΔΙΟΡΙΣΜΟΥ και της ΠΡΟΣΤΑΣΙΑΣ βοηθούν στην πρόληψη και την προετοιμασία έναντι περιστατικών, ενώ τα αποτελέσματα της ΔΙΑΚΥΒΕΡΝΗΣΗΣ, του ΕΝΤΟΠΙΣΜΟΥ, της ΑΝΤΑΠΟΚΡΙΣΗΣ και της ΑΝΑΚΑΜΨΗΣ βοηθούν στην ανακάλυψη και τη διαχείριση περιστατικών.

Κάθε Λειτουργία έχει πάρει το όνομά της από έναν όρο που περιληπτικά περιγράφει το περιεχόμενό της. Κάθε Λειτουργία χωρίζεται σε *Κατηγορίες*, οι οποίες αφορούν συναφή αποτελέσματα κυβερνοασφάλειας που συλλογικά αποτελούν τη Λειτουργία. Οι *Υποκατηγορίες* διαιρούν περαιτέρω κάθε Κατηγορία σε πιο συγκεκριμένα αποτελέσματα τεχνικών και διαχειριστικών δραστηριοτήτων. Οι Υποκατηγορίες δεν είναι υπεραναλυτικές, αλλά περιγράφουν λεπτομερή αποτελέσματα που υποστηρίζουν κάθε Κατηγορία.

Οι Λειτουργίες, οι Κατηγορίες και οι Υποκατηγορίες εφαρμόζονται στο σύνολο των ΤΠΕ που χρησιμοποιεί ένας οργανισμός συμπεριλαμβανομένων των Τεχνολογιών Πληροφορικής (IT – Information Technology), των συσκευών του Διαδικτύου των Πραγμάτων (IoT – Internet of Things) και της Επιχειρησιακής Τεχνολογίας (OT – Operational Technology). Επίσης, εφαρμόζονται σε όλα τα είδη τεχνολογικών περιβαλλόντων, συμπεριλαμβανομένων νεφοϋπολογιστικών συστημάτων, κινητών συσκευών και συστημάτων τεχνητής νοημοσύνης. Ο Πυρήνας του Πλαισίου είναι προσανατολισμένος στο μέλλον και προορίζεται να είναι εφαρμόσιμος σε μελλοντικές αλλαγές σε τεχνολογίες και περιβάλλοντα.

3. Εισαγωγή στα Προφίλ και τις Βαθμίδες του Πλαισίου

Αυτή η ενότητα ορίζει τις έννοιες των Προφίλ και Βαθμίδων του Πλαισίου.

3.1. Προφίλ του Πλαισίου

Ένα *Οργανωτικό Προφίλ του Πλαισίου* περιγράφει την τρέχουσα ή/και την επιδιωκόμενη στάση ενός οργανισμού έναντι της κυβερνοασφάλειας, σε όρους αποτελεσμάτων του Πυρήνα. Τα Οργανωτικά Προφίλ χρησιμοποιούνται για την κατανόηση, προσαρμογή, αξιολόγηση, ιεράρχηση και επικοινωνία των αποτελεσμάτων του Πυρήνα, λαμβάνοντας υπόψιν τους επιχειρησιακούς στόχους, τις προσδοκίες των ενδιαφερόμενων μερών, το τοπίο των απειλών και τις απαιτήσεις του οργανισμού. Στη συνέχεια, ο οργανισμός μπορεί να ιεραρχήσει τις ενέργειές του, για να επιτύχει συγκεκριμένα αποτελέσματα και να επικοινωνήσει τις σχετικές πληροφορίες στα ενδιαφερόμενα μέρη.

Κάθε Οργανωτικό Προφίλ περιλαμβάνει τουλάχιστον ένα από τα παρακάτω:

1. Ένα *Τρέχον Προφίλ* που προσδιορίζει τα αποτελέσματα του Πυρήνα που ένας οργανισμός επιτυγχάνει επί του παρόντος (ή προσπαθεί να επιτύχει) και χαρακτηρίζει τον τρόπο ή τον βαθμό επίτευξης κάθε αποτελέσματος.
2. Ένα *Προφίλ-Στόχος* που προσδιορίζει τα επιθυμητά αποτελέσματα που έχει επιλέξει και ιεραρχήσει ένας οργανισμός για την επίτευξη των στόχων του ως προς τη διαχείριση κινδύνων κυβερνοασφάλειας. Ένα Προφίλ-Στόχος λαμβάνει υπόψη αναμενόμενες αλλαγές στη στάση του οργανισμού έναντι της κυβερνοασφάλειας, όπως οι προκλήσεις που θέτουν οι νέες απαιτήσεις, η υιοθέτηση νέων τεχνολογιών και οι τάσεις που αποκαλύπτουν οι πληροφορίες για απειλές.

> Ένα *Κοινοτικό Προφίλ* είναι μια βασική αναφορά αποτελεσμάτων του Πλαισίου που δημιουργείται και δημοσιεύεται για να ανταποκριθεί σε ενδιαφέροντα και στόχους που είναι κοινά μεταξύ πολλών οργανισμών. Ένα Κοινοτικό Προφίλ αναπτύσσεται συνήθως για έναν συγκεκριμένο τομέα, υποτομέα, τεχνολογία, τύπο απειλής ή άλλη περίπτωση χρήσης. Ένας οργανισμός μπορεί να χρησιμοποιήσει ένα Κοινοτικό Προφίλ ως βάση για το δικό του Προφίλ-Στόχο. Παραδείγματα Κοινοτικών Προφίλ παρατίθενται στην ιστοσελίδα του Πλαισίου.

Τα βήματα που παρουσιάζονται στο Σχήμα 3 και συνοψίζονται παρακάτω απεικονίζουν έναν από τους τρόπους με τους οποίους ένας οργανισμός θα μπορούσε να χρησιμοποιήσει ένα Οργανωτικό Προφίλ για τη συνεχή βελτίωση της κυβερνοασφάλειάς του.

Σχήμα 3. Βήματα για τη δημιουργία και τη χρήση ενός Οργανωτικού Προφίλ του Πλαισίου

1. **Ορίστε το πεδίο εφαρμογής του Οργανωτικού Προφίλ.** Τεκμηριώστε τα κύρια γεγονότα και τις υποθέσεις στις οποίες θα βασιστεί το Προφίλ, για να καθορίσετε το πεδίο εφαρμογής του. Ένας οργανισμός μπορεί να έχει όσα Οργανωτικά Προφίλ επιθυμεί, το καθένα με διαφορετικό πεδίο εφαρμογής. Για παράδειγμα, ένα Προφίλ θα μπορούσε να απευθύνεται σε έναν ολόκληρο οργανισμό ή να αναφέρεται συγκεκριμένα στα συστήματα οικονομικής διαχείρισής του ή στην αντιμετώπιση απειλών λυτρισμικού και στο χειρισμό περιστατικών λυτρισμικού που αφορούν αυτά τα οικονομικά συστήματα.
2. **Συγκεντρώστε τις πληροφορίες που απαιτούνται για την προετοιμασία του Οργανωτικού Προφίλ.** Παραδείγματα πληροφοριών μπορεί να περιλαμβάνουν οργανωτικές πολιτικές, προτεραιότητες διαχείρισης κινδύνων και πόρους, προφίλ επιχειρηματικών κινδύνων, μητρώα ανάλυσης επιχειρηματικών αντικτύπων (Business Impact Analysis – BIA), απαιτήσεις και πρότυπα κυβερνοασφάλειας που ακολουθούνται από τον οργανισμό, πρακτικές και εργαλεία (π.χ. διαδικασίες και μέτρα προστασίας) και ρόλους εργασίας.
3. **Δημιουργήστε το Οργανωτικό Προφίλ.** Καθορίστε τι είδους πληροφορίες θα πρέπει να περιλαμβάνει το Προφίλ για τα επιλεγμένα αποτελέσματα του Πλαισίου και τεκμηριώστε τις απαραίτητες πληροφορίες. Εξετάστε τις επιπτώσεις κινδύνων του Τρέχοντος Προφίλ για να ενημερώσετε τον σχεδιασμό και την ιεράρχηση του Προφίλ-Στόχου. Επίσης, εξετάστε το ενδεχόμενο να χρησιμοποιήσετε ένα Κοινοτικό Προφίλ ως βάση για το Προφίλ-Στόχο.
4. **Αναλύστε τα κενά μεταξύ του Τρέχοντος Προφίλ και του Προφίλ-Στόχου και δημιουργήστε ένα σχέδιο δράσης.** Διεξάγετε μια ανάλυση κενών (gap analysis) για τον εντοπισμό και την ανάλυση των διαφορών μεταξύ του Τρέχοντος Προφίλ και του Προφίλ Στόχου, και αναπτύξτε ένα ιεραρχημένο σχέδιο δράσης (π.χ. μητρώο κινδύνων, έκθεση λεπτομερειών κινδύνων, Σχέδιο Ενεργειών και Στόχων (Plan of Action and Milestones – POA&M) για την αντιμετώπιση αυτών των κενών.

5. **Υλοποιήστε το σχέδιο δράσης και ενημερώστε το Οργανωτικό Προφίλ.** Ακολουθήστε το σχέδιο δράσης για να αντιμετωπίσετε τα κενά και να μετακινήσετε τον οργανισμό προς το Προφίλ-Στόχο. Ένα σχέδιο δράσης μπορεί να έχει μια τελική ημερομηνία ολοκλήρωσης ή να είναι διαρκές.

Δεδομένης της σημασίας της συνεχούς βελτίωσης, ένας οργανισμός μπορεί να επαναλαμβάνει αυτά τα βήματα όσο συχνά χρειάζεται.

Υπάρχουν πρόσθετες χρήσεις για τα Οργανωτικά Προφίλ. Για παράδειγμα, ένα Τρέχον Προφίλ μπορεί να χρησιμοποιηθεί για την τεκμηρίωση και την επικοινωνία των δυνατοτήτων κυβερνοασφάλειας του οργανισμού και τη γνωστοποίηση ευκαιριών βελτίωσης σε εξωτερικούς ενδιαφερόμενους, όπως επιχειρηματικούς εταίρους ή υποψήφιους πελάτες. Επίσης, ένα Προφίλ-Στόχος μπορεί να βοηθήσει έναν οργανισμό να εκφράσει τις απαιτήσεις και τις προσδοκίες του αναφορικά με τη διαχείριση κινδύνων κυβερνοασφάλειας προς τους προμηθευτές, συνεργάτες και άλλα τρίτα μέρη, ως στόχο που πρέπει να επιτύχουν και αυτά τα μέρη.

3.2. Βαθμίδες του Πλαισίου

Ένας οργανισμός μπορεί να επιλέξει να χρησιμοποιήσει τις Βαθμίδες για να ενημερώσει το Τρέχον Προφίλ και το Προφίλ-Στόχου του. Οι *Βαθμίδες* χαρακτηρίζουν την αυστηρότητα των πρακτικών διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας ενός οργανισμού, και παρέχουν το πλαίσιο για το πώς ένας οργανισμός βλέπει τους κινδύνους κυβερνοασφάλειας και τις διαδικασίες που εφαρμόζονται για τη διαχείριση αυτών των κινδύνων. Οι Βαθμίδες, όπως φαίνονται στο Σχήμα 4 και απεικονίζονται εννοιολογικά στο Παράρτημα Β, αντικατοπτρίζουν τις πρακτικές ενός οργανισμού για τη διαχείριση κινδύνων κυβερνοασφάλειας και εκφράζονται με τους όρους «Μερικής Υλοποίησης» (Βαθμίδα 1), «Επίγνωσης Κινδύνου» (Βαθμίδα 2), «Επαναλαμβανόμενων Πρακτικών» (Βαθμίδα 3) και «Προσαρμοζόμενων Πρακτικών» (Βαθμίδα 4). Οι Βαθμίδες περιγράφουν μια εξέλιξη από τις πρόχειρες, άτυπες αποκρίσεις στις ευέλικτες προσεγγίσεις που αναγνωρίζουν τους κινδύνους και βελτιώνονται συνεχώς. Η επιλογή των Βαθμίδων δίνει τον γενικό τόνο για τον τρόπο με τον οποίο ένας οργανισμός θα διαχειριστεί τους κινδύνους κυβερνοασφάλειας.

Σχήμα 4. Βαθμίδες του Πλαισίου για τη διακυβέρνηση και τη διαχείριση κινδύνων κυβερνοασφάλειας

Οι Βαθμίδες πρέπει να συμπληρώνουν τη μεθοδολογία διαχείρισης κινδύνων κυβερνοασφάλειας ενός οργανισμού και όχι να την αντικαθιστούν. Για παράδειγμα, ένας οργανισμός μπορεί να χρησιμοποιήσει τις Βαθμίδες ως σημείο αναφοράς για να επικοινωνήσει εσωτερικά μια προσέγγιση για τη διαχείριση των κινδύνων κυβερνοασφάλειας σε όλο τον οργανισμό[1]. Η μετάβαση σε υψηλότερες Βαθμίδες ενθαρρύνεται όταν οι κίνδυνοι ή οι εντολές είναι μεγαλύτεροι/-ες, ή όταν η ανάλυση κόστους-οφέλους υποδεικνύει μια εφικτή και οικονομικά αποδοτική μείωση αρνητικών κινδύνων κυβερνοασφάλειας.

Η ιστοσελίδα του Πλαισίου παρέχει πρόσθετες πληροφορίες σχετικά με τη χρήση των Προφίλ και των Βαθμίδων. Περιλαμβάνει δείκτες σε πρότυπα Οργανωτικών Προφίλ που φιλοξενούνται από το NIST και ένα αποθετήριο Κοινοτικών Προφίλ σε διάφορες μορφές είτε αναγνώσιμες από μηχανές είτε χρήσιμες σε ανθρώπους.

[1] Για τους σκοπούς αυτού του εγγράφου, οι όροι: «όλος ο οργανισμός», «επιχείρηση» ή «επιχειρηματικός» αποδίδουν την ίδια σημασία.

4. Εισαγωγή στο Διαδικτυακό Υλικό Που Συμπληρώνει το Πλαίσιο

Το NIST και άλλοι οργανισμοί έχουν δημιουργήσει ένα αποθετήριο διαδικτυακού υλικού που βοηθά τους οργανισμούς να κατανοήσουν, να υιοθετήσουν και να χρησιμοποιήσουν το Πλαίσιο. Δεδομένου ότι φιλοξενείται στο διαδίκτυο, αυτό το πρόσθετο υλικό μπορεί να ενημερώνεται πιο συχνά από αυτό το έγγραφο, το οποίο ενημερώνεται λιγότερο συχνά για να παρέχεται σταθερότητα στους χρήστες του, και να είναι διαθέσιμο σε μορφές αναγνώσιμες από μηχανές. Αυτή η ενότητα παρέχει μία επισκόπηση τριών τύπων διαδικτυακού υλικού: Πληροφοριακών Αναφορών, Παραδειγμάτων Εφαρμογής και Οδηγών Γρήγορης Εκκίνησης.

Οι *Πληροφοριακές Αναφορές* είναι αντιστοιχίσεις που υποδεικνύουν σχέσεις μεταξύ του Πυρήνα και διαφόρων προτύπων, κατευθυντήριων γραμμών, κανονισμών και εγγράφων άλλου περιεχομένου. Οι Πληροφοριακές Αναφορές βοηθούν στην ενημέρωση ενός οργανισμού σχετικά με το πώς μπορεί να επιτύχει τα επιθυμητά αποτελέσματα του Πυρήνα. Οι Πληροφοριακές Αναφορές μπορεί να αφορούν συγκεκριμένους κλάδους ή τεχνολογίες. Αυτές μπορεί να παράγονται από το NIST ή από άλλο οργανισμό. Κάποιες Πληροφοριακές Αναφορές έχουν πιο περιορισμένο εύρος από το εύρος μίας Υποκατηγορίας. Για παράδειγμα, ένα συγκεκριμένο σημείο ελέγχου από την Ειδική Έκδοση (Special Publication, SP) 800-53, *Σημεία Ελέγχου Ασφάλειας και Ιδιωτικότητας για Πληροφοριακά Συστήματα και Οργανισμούς*, μπορεί να είναι μια από τις πολλές αναφορές που χρειάζονται για να επιτευχθεί το αποτέλεσμα που περιγράφεται σε μία Υποκατηγορία. Άλλες Πληροφοριακές Αναφορές μπορεί να είναι υψηλότερου επίπεδου, όπως μια απαίτηση από μια πολιτική που καλύπτει εν μέρει πολλές Υποκατηγορίες. Κάθε οργανισμός που χρησιμοποιεί το Πλαίσιο, μπορεί να αναγνωρίσει τις καταλληλότερες προς αυτόν Πληροφοριακές Αναφορές.

Τα *Παραδείγματα Εφαρμογής* παρέχουν παραδείγματα συνοπτικών, πρακτικών βημάτων που βοηθούν στην επίτευξη των επιθυμητών αποτελεσμάτων των Υποκατηγοριών. Τα ρήματα που χρησιμοποιούνται για να εκφράσουν τέτοια Παραδείγματα περιλαμβάνουν τα: μοιράζομαι, τεκμηριώνω, αναπτύσσω, εκτελώ, παρακολουθώ, αναλύω, αξιολογώ και εξασκώ. Τα Παραδείγματα δεν αποτελούν έναν εξαντλητικό κατάλογο όλων των ενεργειών που θα μπορούσαν να αναληφθούν από έναν οργανισμό για την επίτευξη ενός αποτελέσματος, ούτε αντιπροσωπεύουν το ελάχιστο σύνολο απαιτούμενων ενεργειών για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας.

Οι *Οδηγοί Γρήγορης Εκκίνησης (Οδηγοί - Quick Start Guides [QSGs])* είναι σύντομα έγγραφα για συγκεκριμένα θέματα που σχετίζονται με το Πλαίσιο και είναι συχνά προσαρμοσμένα σε συγκεκριμένα ακροατήρια. Οι Οδηγοί μπορούν να βοηθήσουν έναν οργανισμό να εφαρμόσει το Πλαίσιο, επειδή αποσαφηνίζουν συγκεκριμένους τομείς του Πλαισίου προσφέροντας τα πρακτικά «πρώτα βήματα» που ένας οργανισμός μπορεί να λάβει υπόψη του στην πορεία βελτίωσης της στάσης του έναντι της κυβερνοασφάλειας και στη διαχείριση των σχετικών κινδύνων. Οι οδηγοί αναθεωρούνται σε δικά τους χρονικά πλαίσια και νέοι οδηγοί προστίθενται ανάλογα με τις ανάγκες.

Προτάσεις για νέες Πληροφοριακές Αναφορές για την έκδοση 2.0 του Πλαισίου μπορούν πάντα να κοινοποιούνται στο NIST στην ηλεκτρονική διεύθυνση olir@nist.gov. Προτάσεις για άλλο υλικό προς δημοσίευση στην ιστοσελίδα του Πλαισίου, συμπεριλαμβανομένων επιπλέον

θεμάτων για τους Οδηγούς Γρήγορης Εκκίνησης, θα πρέπει να απευθύνονται στη διεύθυνση cyberframework@nist.gov.

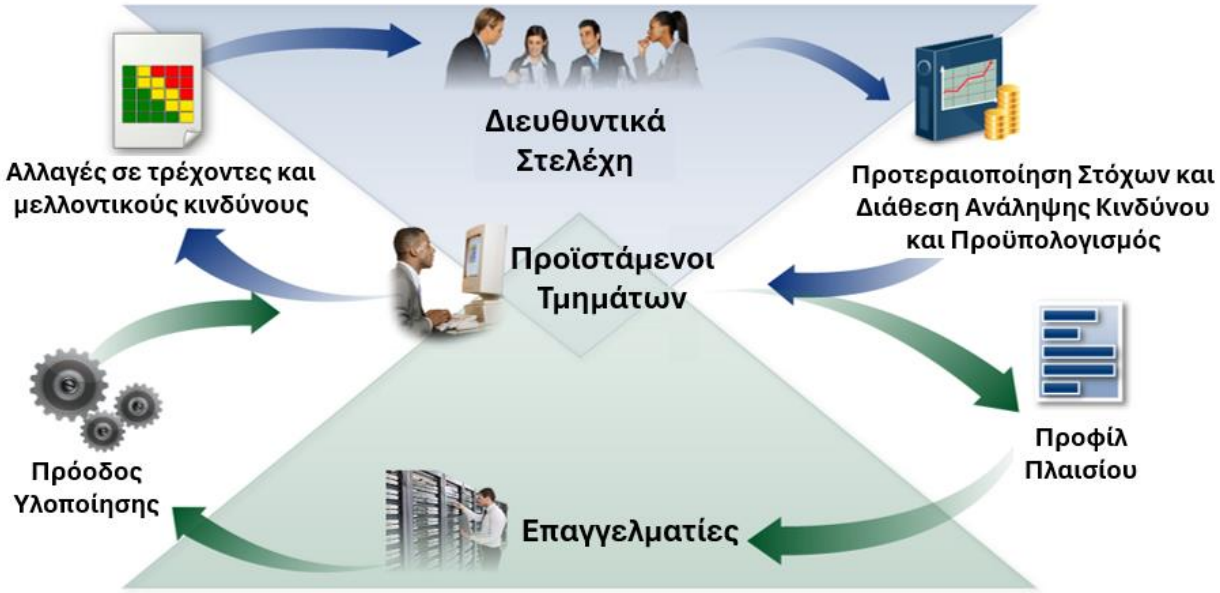
5. Βελτίωση της Επικοινωνίας και Ενσωμάτωσης των Κινδύνων Κυβερνοασφάλειας

Η χρήση του Πλαισίου θα ποικίλει ανάλογα με την ξεχωριστή αποστολή και τους κινδύνους που αντιμετωπίζει κάθε οργανισμός. Με την κατανόηση των προσδοκιών των εμπλεκόμενων, της διάθεσης για ανάληψη κινδύνων και του ορίου ανοχής κινδύνων (όπως εκφράζονται στη ΔΙΑΚΥΒΕΡΝΗΣΗ), ένας οργανισμός μπορεί να ιεραρχήσει τις δραστηριότητες κυβερνοασφάλειας, ώστε να λαμβάνει τεκμηριωμένες αποφάσεις σχετικά με τις δαπάνες και τις δράσεις κυβερνοασφάλειας. Ένας οργανισμός μπορεί να επιλέξει να χειριστεί τον κίνδυνο με έναν ή περισσότερους τρόπους — συμπεριλαμβανομένου του μετριασμού, της μεταφοράς, της αποφυγής ή της αποδοχής αρνητικών κινδύνων και της συνειδητοποίησης, της κοινής αξιοποίησης, της ενίσχυσης των αποτελεσμάτων ή της αποδοχής των θετικών κινδύνων — ανάλογα με τις πιθανές επιπτώσεις και πιθανότητες. Είναι σημαντικό ότι ένας οργανισμός μπορεί να χρησιμοποιήσει το Πλαίσιο τόσο εσωτερικά για τη διαχείριση των δυνατοτήτων του στον τομέα της κυβερνοασφάλειας, όσο και εξωτερικά για την εποπτεία ή την επικοινωνία με τρίτα μέρη.

Ανεξαρτήτως της χρήσης του Πλαισίου, ένας οργανισμός μπορεί να επωφεληθεί, χρησιμοποιώντας το Πλαίσιο ως οδηγό για να κατανοήσει τους κινδύνους κυβερνοασφάλειας, να τους αξιολογήσει, να τους ιεραρχήσει, και να τους επικοινωνήσει παράλληλα με τις ενέργειες που θα επιτρέψουν τη διαχείριση αυτών των κινδύνων. Τα επιλεγμένα αποτελέσματα μπορούν να χρησιμοποιηθούν για να εστιάσει και να υλοποιήσει στρατηγικές αποφάσεις με σκοπό τη βελτίωση της στάσης του έναντι της κυβερνοασφάλειας, και τη διατήρηση της συνέχειας των βασικών λειτουργιών της εκάστοτε αποστολής του, λαμβάνοντας υπόψη τις προτεραιότητες και τους διαθέσιμους πόρους του.

5.1. Βελτίωση της Επικοινωνίας για τη Διαχείριση Κινδύνων

Το Πλαίσιο αποτελεί μια βάση για τη βελτίωση της επικοινωνίας όσον αφορά στις προσδοκίες, στον σχεδιασμό και στους πόρους κυβερνοασφάλειας. Το Πλαίσιο προάγει την αμφίδρομη ροή πληροφοριών (όπως φαίνεται στο πάνω μισό του Σχήματος 5) μεταξύ των διευθυντικών στελεχών που εστιάζουν στις προτεραιότητες και τη στρατηγική κατεύθυνση του οργανισμού και των προϊσταμένων τμημάτων που διαχειρίζονται συγκεκριμένους κινδύνους κυβερνοασφάλειας που θα μπορούσαν να επηρεάσουν την επίτευξη αυτών των προτεραιοτήτων. Το Πλαίσιο υποστηρίζει επίσης μια παρόμοια ροή (όπως φαίνεται στο κάτω μισό του Σχήματος 5) μεταξύ των προϊσταμένων τμημάτων και των επαγγελματιών που υλοποιούν και διαχειρίζονται τις τεχνολογίες. Η αριστερή πλευρά του σχήματος δείχνει τη σημασία που έχει οι επαγγελματίες να ενημερώνουν τους προϊσταμένους τους και τα διευθυντικά στελέχη για τις εξελίξεις που τους αφορούν και για τις ιδέες και τις ανησυχίες που έχουν.



Σχήμα 5. Χρήση του Πλαισίου για τη βελτίωση της επικοινωνίας στη διαχείριση κινδύνων

Η προετοιμασία για τη δημιουργία και χρήση Οργανωτικών Προφίλ περιλαμβάνει τη συλλογή πληροφοριών σχετικά με τις προτεραιότητες του οργανισμού, τους διαθέσιμους πόρους και την κατεύθυνση των κινδύνων από τα διευθυντικά στελέχη. Οι προϊστάμενοι τμημάτων συνεργάζονται στη συνέχεια με τους επαγγελματίες για να επικοινωνήσουν τις επιχειρησιακές ανάγκες και να δημιουργήσουν Οργανωτικά Προφίλ βασισμένα στους κινδύνους. Οι δράσεις για την κάλυψη κενών που εντοπίζονται μεταξύ του Τρέχοντος Προφίλ και του Προφίλ-Στόχου θα υλοποιηθούν από τους προϊσταμένους και τους επαγγελματίες, και θα παράσχουν σημαντικές εισροές στα σχέδια συστημικού επιπέδου. Καθώς επιτυγχάνεται η προσδοκώμενη κατάσταση σε όλο τον οργανισμό — μεταξύ άλλων και μέσω σημείων ελέγχου και παρακολούθησης που εφαρμόζονται σε συστημικό επίπεδο — τα ενημερωμένα αποτελέσματα μπορούν να κοινοποιηθούν μέσω μητρώων κινδύνων και εκθέσεων προόδου. Στο πλαίσιο της διαρκούς αξιολόγησης, οι προϊστάμενοι αποκτούν γνώσεις για να κάνουν προσαρμογές που μειώνουν περαιτέρω τους πιθανούς κινδύνους και αυξάνουν τα πιθανά οφέλη.

Η Λειτουργία ΔΙΑΚΥΒΕΡΝΗΣΗ υποστηρίζει την επικοινωνία με **διευθυντικά στελέχη** για οργανωτικούς κινδύνους. Οι συζητήσεις των διευθυντικών στελεχών επικεντρώνονται στη στρατηγική, ιδίως στο πώς οι αβεβαιότητες που σχετίζονται με την κυβερνοασφάλεια μπορεί να επηρεάσουν την επίτευξη των οργανωτικών στόχων. Αυτές οι συζητήσεις διακυβέρνησης υποστηρίζουν τον διάλογο και τη συναίνεση σχετικά με τις στρατηγικές διαχείρισης κινδύνων (συμπεριλαμβανομένων των κινδύνων κυβερνοασφάλειας εφοδιαστικής αλυσίδας), τους ρόλους, τις ευθύνες και τις αρμοδιότητες, τις πολιτικές και την εποπτεία. Καθώς τα διευθυντικά στελέχη θέτουν τις προτεραιότητες και τους στόχους για την κυβερνοασφάλεια με βάση αυτές τις ανάγκες, επικοινωνούν τις προσδοκίες σχετικά με τη διάθεση ανάληψης

κινδύνου, τη λογοδοσία και τους πόρους. Τα διευθυντικά στελέχη είναι επίσης υπεύθυνα για την ενσωμάτωση της διαχείρισης κινδύνων κυβερνοασφάλειας με τα προγράμματα διαχείρισης επιχειρηματικών κινδύνων (ERM) και τα προγράμματα διαχείρισης κινδύνων χαμηλότερου επιπέδου (βλ. Ενότητα 5.2). Οι επικοινωνίες που αποτυπώνονται στο πάνω μισό του Σχήματος 5 μπορούν να περιλαμβάνουν εκτιμήσεις για τη διαχείριση επιχειρηματικών κινδύνων και για τα προγράμματα χαμηλότερου επιπέδου και επομένως παρέχουν πληροφόρηση στους προϊσταμένους τμημάτων και στους επαγγελματίες.

Οι συνολικοί στόχοι κυβερνοασφάλειας που καθορίζονται από τα διευθυντικά στελέχη διαμορφώνονται με τη συμβολή των **προϊσταμένων τμημάτων** και μεταφέρονται σε αυτούς. Σε μια εμπορική επιχείρηση, αυτοί οι στόχοι μπορεί να εφαρμόζονται σε έναν επιχειρηματικό τομέα ή ένα τμήμα. Για τους κυβερνητικούς οργανισμούς, μπορεί να αφορά σε αρμοδιότητες επιπέδου τμήματος ή παραρτήματος. Κατά την υλοποίηση του Πλαισίου, οι προϊστάμενοι τμημάτων εστιάζουν στο πώς θα επιτύχουν τους στόχους που απορρέουν από τους κινδύνους μέσω κοινών υπηρεσιών, σημείων ελέγχου και συνεργασίας, όπως εκφράζονται στο Προφίλ-Στόχου και βελτιώνονται μέσω των ενεργειών που παρακολουθούνται στο σχέδιο δράσης (π.χ. μέσω του μητρώου κινδύνων, της λεπτομερούς αναφοράς κινδύνων, του πλάνου ενεργειών και στόχων [Plan of Action and Milestones – POA&M]).

Οι **επαγγελματίες** επικεντρώνονται στην επίτευξη της κατάστασης-στόχου και στη μέτρηση των αλλαγών στον επιχειρησιακό κίνδυνο, για να βοηθήσουν στον σχεδιασμό, την εκτέλεση και την παρακολούθηση συγκεκριμένων δραστηριοτήτων κυβερνοασφάλειας. Καθώς υλοποιούνται σημεία ελέγχου ασφάλειας για τη διαχείριση των κινδύνων σε αποδεκτό επίπεδο, οι επαγγελματίες παρέχουν στους προϊσταμένους και τα διευθυντικά στελέχη τις πληροφορίες (π.χ. βασικούς δείκτες απόδοσης, βασικούς δείκτες κινδύνου) που χρειάζονται για να κατανοήσουν τη στάση του οργανισμού έναντι της κυβερνοασφάλειας, να λάβουν εγνωσμένες αποφάσεις και να διατηρήσουν ή να προσαρμόσουν τη στρατηγική κινδύνου αναλόγως. Τα διευθυντικά στελέχη μπορούν επίσης να συνδυάσουν αυτά τα δεδομένα κινδύνων κυβερνοασφάλειας με πληροφορίες για άλλους τύπους κινδύνων από όλο τον οργανισμό. Καθώς ο κύκλος επαναλαμβάνεται, οι αλλαγές στις προσδοκίες και τις προτεραιότητες ενσωματώνονται στα ενημερωμένα Οργανωτικά Προφίλ.

5.2. Βελτίωση της Ενσωμάτωσης με Άλλα Προγράμματα Διαχείρισης Κινδύνων

Κάθε οργανισμός αντιμετωπίζει πολλά είδη κινδύνων ΤΠΕ (π.χ. ιδιωτικότητα, εφοδιαστική αλυσίδα, τεχνητή νοημοσύνη) και ενδέχεται να χρησιμοποιεί εξειδικευμένα πλαίσια και εργαλεία διαχείρισης για κάθε κίνδυνο. Όσον αφορά στην προσπάθεια διαχείρισης κινδύνων ΤΠΕ και άλλων παρόμοιων προσπαθειών διαχείρισης κινδύνων, κάποιοι οργανισμοί εστιάζουν σε υψηλό επίπεδο, χρησιμοποιώντας τη Διαχείριση Επιχειρηματικού Κινδύνου (Enterprise Risk Management – ERM), ενώ άλλοι οργανισμοί διαχωρίζουν τις προσπάθειες διαχείρισης κινδύνων για να εξασφαλίσουν επαρκή προσοχή σε καθεμία από αυτές. Μικροί οργανισμοί από τη φύση τους ενδέχεται να παρακολουθούν τους κινδύνους συνολικά σε επίπεδο επιχείρησης, ενώ μεγαλύτερες εταιρείες ενδέχεται να διαχωρίζουν τις προσπάθειες διαχείρισης κινδύνων ενσωματώνοντάς τις στη Διαχείριση Επιχειρηματικών Κινδύνων.

Οι οργανισμοί μπορούν να αξιοποιούν μια προσέγγιση Διαχείρισης Επιχειρηματικών Κινδύνων για να αντισταθμίσουν ένα *χαρτοφυλάκιο* κινδύνων που συμπεριλαμβάνει την κυβερνοασφάλεια και να λαμβάνουν τεκμηριωμένες αποφάσεις. Τα διευθυντικά στελέχη λαμβάνουν σημαντικές πληροφορίες σχετικά με τρέχουσες και προγραμματισμένες δραστηριότητες αντιμετώπισης κινδύνων, ενώ ενσωματώνουν τις στρατηγικές διακυβέρνησης και διαχείρισης κινδύνων με αποτελέσματα από προηγούμενες χρήσεις του Πλαισίου. Το Πλαίσιο βοηθά τους οργανισμούς να μεταφράσουν την ορολογία τους για την κυβερνοασφάλεια και για τη διαχείριση κινδύνων κυβερνοασφάλειας σε γενική γλώσσα διαχείρισης κινδύνων, την οποία κατανοούν τα διευθυντικά στελέχη.

Οι παρακάτω δημοσιεύσεις του NIST περιγράφουν την αμοιβαία σχέση μεταξύ της διαχείρισης κινδύνων κυβερνοασφάλειας και της Διαχείρισης Επιχειρηματικών Κινδύνων:

- Έκδοση 2.0 του Πλαισίου Κυβερνοασφάλειας NIST - *Οδηγός Γρήγορης Εκκίνησης για τη Διαχείριση Επιχειρηματικών Κινδύνων*
- Διϋπηρεσιακή Έκθεση (NIST Interagency Report, IR) 8286, *Ενσωμάτωση της Κυβερνοασφάλειας με τη Διαχείρηση Επιχειρηματικών Κινδύνων*
- Διϋπηρεσιακή Έκθεση 8286A, *Προσδιορισμός και Εκτίμηση Κινδύνων Κυβερνοασφάλειας για τη Διαχείριση Επιχειρηματικών Κινδύνων*
- Διϋπηρεσιακή Έκθεση 8286B, *Δίνοντας Προτεραιότητα στους Κινδύνους Κυβερνοασφάλειας για τη Διαχείριση Επιχειρηματικών Κινδύνων*
- Διϋπηρεσιακή Έκθεση 8286C, *Σταδιοποίηση των Κινδύνων Κυβερνοασφάλειας για τη Διαχείριση Επιχειρηματικών Κινδύνων και την Εποπτεία της Διακυβέρνησης*
- Διϋπηρεσιακή Έκθεση 8286D, *Χρήση της Ανάλυσης Επιχειρηματικού Αντικτύπου στη Λήψη Αποφάσεων Προτεραιοποίησης και Απόκρισης σε Κινδύνους*
- Ειδική Έκδοση (Special Publication, SP) 800-221, *Επιχειρηματικός Αντίκτυπος των Κινδύνων Τεχνολογιών Πληροφορικής και Επικοινωνιών: Διακυβέρνηση και Διαχείριση Προγραμμάτων Αντιμετώπισης Κινδύνων ΤΠΕ σε ένα Χαρτοφυλάκιο Επιχειρηματικών Κινδύνων*
- Ειδική Έκδοση 800-221A, *Αποτελέσματα Κινδύνων Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ): Ενσωμάτωση Προγραμμάτων Διαχείρισης Κινδύνων ΤΠΕ με το Χαρτοφυλάκιο Επιχειρηματικών Κινδύνων*

Ένας οργανισμός μπορεί επίσης να βρει το Πλαίσιο επωφελές για την ενσωμάτωση της διαχείρισης κινδύνων κυβερνοασφάλειας σε εξειδικευμένα προγράμματα διαχείρισης κινδύνων ΤΠΕ, όπως:

- **Διαχείριση και αξιολόγηση κινδύνων κυβερνοασφάλειας:** Το Πλαίσιο μπορεί να ενσωματωθεί σε υπάρχοντα προγράμματα διαχείρισης και αξιολόγησης κινδύνων κυβερνοασφάλειας, όπως η Ειδική Έκδοση 800-37, *Πλαίσιο Διαχείρισης Κινδύνων για Πληροφοριακά Συστήματα και Οργανισμούς* και η Ειδική Έκδοση 800-30, *Οδηγός Διεξαγωγής Αξιολόγησης Κινδύνων* από το Πλαίσιο Διαχείρισης Κινδύνων (RMF – Risk Management Framework) του NIST. Για έναν οργανισμό που χρησιμοποιεί *το Πλαίσιο*

Διαχείρισης Κινδύνων του NIST και τις σχετικές δημοσιεύσεις του, το Πλαίσιο μπορεί να χρησιμοποιηθεί για να συμπληρώσει την προσέγγιση του Πλαισίου Διαχείρισης Κινδύνων ως προς την επιλογή και την ιεράρχηση των ελέγχων από την Ειδική Έκδοση 800-53, *Σημεία Ελέγχου Ασφάλειας και Ιδιωτικότητας για Πληροφοριακά Συστήματα και Οργανισμούς*.

- **Κίνδυνοι ιδιωτικότητας:** Ενώ η κυβερνοασφάλεια και η ιδιωτικότητα είναι ανεξάρτητοι κλάδοι, οι στόχοι τους επικαλύπτονται σε ορισμένες περιπτώσεις, όπως φαίνεται στο Σχήμα 6.

Σχήμα 6. Σχέση μεταξύ κινδύνων κυβερνοασφάλειας και ιδιωτικότητας

Η διαχείριση των κινδύνων κυβερνοασφάλειας είναι απαραίτητη για την αντιμετώπιση των κινδύνων ιδιωτικότητας που σχετίζονται με την απώλεια της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων των ατόμων. Για παράδειγμα, παραβιάσεις δεδομένων θα μπορούσαν να οδηγήσουν σε κλοπή ταυτότητας. Ωστόσο, κίνδυνοι ιδιωτικότητας μπορεί επίσης να προκύψουν και από ζητήματα, τα οποία δεν σχετίζονται με περιστατικά κυβερνοασφάλειας.

Ένας οργανισμός επεξεργάζεται δεδομένα για να επιτύχει επιχειρηματικούς σκοπούς ή στόχους που σχετίζονται με την αποστολή του, γεγονός που μερικές φορές μπορεί να προκαλέσει *συμβάντα ιδιωτικότητας,* κατά τα οποία τα άτομα μπορεί να αντιμετωπίσουν προβλήματα ως αποτέλεσμα της επεξεργασίας δεδομένων. Αυτά τα προβλήματα μπορούν να εκφραστούν με διάφορους τρόπους, αλλά το NIST τα περιγράφει ως επιδράσεις που κυμαίνονται από ζητήματα αξιοπρέπειας (π.χ. αίσθημα ταπείνωσης ή κοινωνικό στιγματισμό) έως πιο απτές βλάβες (π.χ. κοινωνικές διακρίσεις, οικονομική ή σωματική βλάβη). Το Πλαίσιο Ιδιωτικότητας του NIST και το Πλαίσιο Κυβερνοασφάλειας μπορούν να χρησιμοποιηθούν μαζί για να αντιμετωπίσουν τις διάφορες πτυχές της κυβερνοασφάλειας και των κινδύνων ιδιωτικότητας. Επιπλέον, η Μεθοδολογία Αξιολόγησης Κινδύνων Ιδιωτικότητας του NIST (Privacy Risk Assessment Methodology, PRAM) συμπεριλαμβάνει έναν κατάλογο με παραδείγματα προβλημάτων για χρήση σε αξιολογήσεις κινδύνων ιδιωτικότητας.

- **Κίνδυνοι εφοδιαστικής αλυσίδας:** Ένας οργανισμός μπορεί να χρησιμοποιήσει το Πλαίσιο για να ενισχύσει την εποπτεία και την επικοινωνία σχετικά με τους κινδύνους κυβερνοασφάλειας με τους ενδιαφερόμενους σε όλη την αλυσίδα εφοδιασμού. Όλα τα είδη τεχνολογίας βασίζονται σε ένα σύνθετο, παγκόσμια κατανεμημένο, εκτενές και διασυνδεδεμένο οικοσύστημα εφοδιαστικής αλυσίδας με γεωγραφικά διαφορετικές διαδρομές και πολλαπλά επίπεδα εξωτερικής ανάθεσης. Αυτό το οικοσύστημα αποτελείται από οντότητες του δημόσιου και του ιδιωτικού τομέα (π.χ. αγοραστές, προμηθευτές, προγραμματιστές, υλοποιητές συστημάτων, εξωτερικούς παρόχους υπηρεσιών συστημάτων και άλλους παρόχους υπηρεσιών που σχετίζονται με την τεχνολογία) που αλληλεπιδρούν για την έρευνα, την ανάπτυξη, τον σχεδιασμό, την κατασκευή, την απόκτηση, την παράδοση, την ενοποίηση, τη λειτουργία, τη συντήρηση, την απόρριψη και τη χρήση ή διαχείριση με άλλους τρόπους προϊόντων και υπηρεσιών τεχνολογίας. Αυτές οι αλληλεπιδράσεις διαμορφώνονται και επηρεάζονται από τεχνολογίες, νόμους, πολιτικές, διαδικασίες και πρακτικές.

  Δεδομένων των πολύπλοκων και διασυνδεδεμένων σχέσεων σε αυτό το οικοσύστημα, η διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας (SCRM – Supply Chain Risk Management) είναι ζωτικής σημασίας για τους οργανισμούς. Η διαχείριση κινδύνων κυβερνοασφάλειας εφοδιαστικής αλυσίδας (C-SCRM – Cybersecurity Supply Chain Risk Management) είναι μία συστηματική διεργασία που αφορά στη διαχείριση της έκθεσης σε κινδύνους κυβερνοασφάλειας σε όλη την εφοδιαστική αλυσίδα και στην ανάπτυξη κατάλληλων στρατηγικών ανταπόκρισης, πολιτικών, διεργασιών και διαδικασιών. Οι Υποκατηγορίες εντός της Κατηγορίας C-SCRM [GV.SC] του Πλαισίου παρέχουν μια σύνδεση μεταξύ των επιθυμητών αποτελεσμάτων που εστιάζουν αποκλειστικά στην κυβερνοασφάλεια και εκείνων που εστιάζουν στη διαχείριση των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας (C-SCRM). Η Ειδική Έκδοση (Special Publication, SP) 800-161r1 (Έκδοση 1), Πρακτικές Διαχείρισης Κινδύνων Κυβερνοασφάλειας Εφοδιαστικής Αλυσίδας για Συστήματα και Οργανισμούς, παρέχει αναλυτικές πληροφορίες για το C-SCRM.

- **Κίνδυνοι από τις αναδυόμενες τεχνολογίες:** Καθώς νέες τεχνολογίες και νέες τεχνολογικές εφαρμογές γίνονται διαθέσιμες, εμφανίζονται νέοι κίνδυνοι με πιο ξεκάθαρο τρόπο. Ένα σύγχρονο παράδειγμα είναι η Τεχνητή Νοημοσύνη (ΤΝ) (AI – Artificial Intelligence), η οποία έχει κινδύνους κυβερνοασφάλειας και ιδιωτικότητας, καθώς και πολλούς άλλους τύπους κινδύνων. Το Πλαίσιο Διαχείρισης Κινδύνων Τεχνητής Νοημοσύνης του NIST (AI RMF – Artificial Intelligence Risk Management Framework) αναπτύχθηκε για να βοηθήσει στην αντιμετώπιση αυτών των κινδύνων. Η αντιμετώπιση των κινδύνων τεχνητής νοημοσύνης παράλληλα με άλλους επιχειρηματικούς κινδύνους (π.χ. οικονομικούς, κυβερνοασφάλειας, φήμης και ιδιωτικότητας) θα προσφέρει ένα πιο ολοκληρωμένο αποτέλεσμα και θα βελτιώσει την αποδοτικότητα του οργανισμού. Οι εκτιμήσεις και οι προσεγγίσεις για τη διαχείριση κινδύνων κυβερνοασφάλειας και ιδιωτικότητας ισχύουν και για τον σχεδιασμό, την

ανάπτυξη, την εφαρμογή, την αξιολόγηση και τη χρήση συστημάτων ΤΝ. Ο Πυρήνας του Πλαισίου Διαχείρισης Κινδύνων Τεχνητής Νοημοσύνης (AI RMF) χρησιμοποιεί Λειτουργίες, Κατηγορίες και Υποκατηγορίες για να περιγράψει τα αποτελέσματα της τεχνητής νοημοσύνης και να βοηθήσει στη διαχείριση κινδύνων που σχετίζονται με την τεχνητή νοημοσύνη.

Παράρτημα Α. Πυρήνας του Πλαισίου

Το παρόν παράρτημα περιγράφει τις Λειτουργίες, τις Κατηγορίες και τις Υποκατηγορίες του Πυρήνα του Πλαισίου. Ο Πίνακας 1 παραθέτει τα ονόματα και τα μοναδικά αλφαβητικά αναγνωριστικά των Λειτουργιών και Κατηγοριών του Πυρήνα του Πλαισίου 2.0. Κάθε όνομα Λειτουργίας στον πίνακα συνδέεται με το αντίστοιχο τμήμα του παραρτήματος. Η σειρά των Λειτουργιών, των Κατηγοριών και των Υποκατηγοριών του Πυρήνα δεν είναι αλφαβητική - ο στόχος είναι να έχει μεγαλύτερη απήχηση σε όσους είναι επιφορτισμένοι με τη λειτουργική εφαρμογή της διαχείρισης κινδύνων σε έναν οργανισμό. Η αρίθμηση των Υποκατηγοριών σκόπιμα δεν είναι διαδοχική - τα κενά στην αρίθμηση υποδηλώνουν Υποκατηγορίες του Πλαισίου 1.1 που μεταφέρθηκαν στο Πλαίσιο 2.0.

Πίνακας 1. Ονόματα και αναγνωριστικά των Λειτουργιών και Κατηγοριών του Πυρήνα του Πλαισίου 2.0

Λειτουργία	Κατηγορία	Αναγνωριστικό Κατηγορίας
Διακυβέρνηση (GV)	Οργανωτικό Πλαίσιο (Organizational Context)	GV.OC
	Στρατηγική Διαχείρισης Κινδύνων (Risk Management Strategy)	GV.RM
	Ρόλοι, Ευθύνες και Αρμοδιότητες (Roles, Responsibilities, and Authorities)	GV.RR
	Πολιτική (Policy)	GV.PO
	Εποπτεία (Oversight)	GV.OV
	Διαχείριση Κινδύνων Κυβερνοασφάλειας στην Εφοδιαστική Αλυσίδα (Cybersecurity Supply Chain Risk Management)	GV.SC
Προσδιορισμός (ID)	Διαχείριση Αγαθών (Asset Management)	ID.AM
	Εκτίμηση Κινδύνων (Risk Assessment)	ID.RA
	Βελτίωση (Improvement)	ID.IM
Προστασία (PR)	Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης (Identity Management, Authentication, and Access Control)	PR.AA
	Ευαισθητοποίηση και Εκπαίδευση (Awareness and Training)	PR.AT
	Ασφάλεια Δεδομένων (Data Security)	PR.DS
	Ασφάλεια Πλατφόρμας (Platform Security)	PR.PS
	Ανθεκτικότητα Τεχνολογικής Υποδομής (Technology Infrastructure Resilience)	PR.IR
Εντοπισμός (DE)	Συνεχής Παρακολούθηση (Continuous Monitoring)	DE.CM
	Ανάλυση Ανεπιθύμητων Συμβάντων (Adverse Event Analysis)	DE.AE
Ανταπόκριση (RS)	Διαχείριση Περιστατικών (Incident Management)	RS.MA
	Ανάλυση Περιστατικών (Incident Analysis)	RS.AN
	Αναφορά και Επικοινωνία Ανταπόκρισης σε Περιστατικά (Incident Response Reporting and Communication)	RS.CO
	Μετριασμός Περιστατικών (Incident Mitigation)	RS.MI

Λειτουργία	**Κατηγορία**	**Αναγνωριστικό Κατηγορίας**
Ανάκαμψη (RC)	Εκτέλεση Σχεδίου Ανάκαμψης από Περιστατικά (Incident Recovery Plan Execution)	RC.RP
	Επικοινωνία Ανάκαμψης από Περιστατικά (Incident Recovery Communication)	RC.CO

Ο Πυρήνας του Πλαισίου, οι Πληροφοριακές Αναφορές, και τα Παραδείγματα Εφαρμογής είναι διαθέσιμα στην ιστοσελίδα του Πλαισίου 2.0 και μέσω του Εργαλείου Αναφοράς του Πλαισίου 2.0, το οποίο επιτρέπει στους χρήστες να τα εξερευνήσουν και να τα εξάγουν σε μορφές αναγνώσιμες από άνθρωπο και μηχανή. Ο Πυρήνας του Πλαισίου 2.0 είναι επίσης διαθέσιμος και σε παλαιά μορφή όμοια με εκείνη του Πλαισίου 1.1.

ΔΙΑΚΥΒΕΡΝΗΣΗ (GV): Καθορίζεται, κοινοποιείται και εποπτεύεται η στρατηγική διαχείρισης κινδύνων κυβερνοασφάλειας του οργανισμού, οι προσδοκίες και η πολιτική του.

- **Οργανωτικό Πλαίσιο (GV.OC):** Γίνονται κατανοητές οι περιστάσεις – αποστολή, προσδοκίες των ενδιαφερόμενων μερών, εξαρτήσεις, και νομικές, κανονιστικές και συμβατικές απαιτήσεις – που περιβάλλουν τις αποφάσεις διαχείρισης κινδύνων κυβερνοασφάλειας του οργανισμού
  - **GV.OC-01:** Η αποστολή του οργανισμού γίνεται κατανοητή και αντικατοπτρίζεται στη διαχείριση κινδύνων κυβερνοασφάλειας
  - **GV.OC-02:** Τα εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη αναγνωρίζονται, και οι ανάγκες και προσδοκίες τους σχετικά με τη διαχείριση κινδύνων κυβερνοασφάλειας γίνονται κατανοητές και λαμβάνονται υπόψη
  - **GV.OC-03:** Ο οργανισμός κατανοεί και διαχειρίζεται τις νομικές, κανονιστικές και συμβατικές απαιτήσεις σχετικά με την κυβερνοασφάλεια – συμπεριλαμβανομένων των υποχρεώσεων ιδιωτικότητας και πολιτικών ελευθεριών
  - **GV.OC-04:** Κρίσιμοι στόχοι, δυνατότητες και υπηρεσίες από τα οποία εξαρτώνται ή τα οποία αναμένουν τα εξωτερικά ενδιαφερόμενα μέρη από τον οργανισμό γίνονται κατανοητά και κοινοποιούνται
  - **GV.OC-05:** Τα αποτελέσματα, οι δυνατότητες και οι υπηρεσίες από τα οποία εξαρτάται ο οργανισμός γίνονται κατανοητά και κοινοποιούνται

- **Στρατηγική Διαχείρισης Κινδύνων (GV.RM):** Οι προτεραιότητες, οι περιορισμοί, και οι δηλώσεις και υποθέσεις ανοχής και διάθεσης ανάληψης κινδύνου του οργανισμού καθορίζονται, κοινοποιούνται και χρησιμοποιούνται για την υποστήριξη των αποφάσεων που σχετίζονται με τους λειτουργικούς κινδύνους
  - **GV.RM-01:** Οι στόχοι διαχείρισης κινδύνων καθορίζονται και συμφωνούνται από τα ενδιαφερόμενα μέρη του οργανισμού
  - **GV.RM-02:** Οι δηλώσεις διάθεσης ανάληψης και ανοχής κινδύνου καθορίζονται, κοινοποιούνται και διατηρούνται
  - **GV.RM-03:** Οι δραστηριότητες και τα αποτελέσματα διαχείρισης κινδύνων κυβερνοασφάλειας συμπεριλαμβάνονται στις διαδικασίες διαχείρισης επιχειρηματικών κινδύνων
  - **GV.RM-04:** Η στρατηγική κατεύθυνση που περιγράφει τις κατάλληλες επιλογές αντιμετώπισης κινδύνου καθορίζεται και κοινοποιείται
  - **GV.RM-05:** Γραμμές επικοινωνίας για κινδύνους κυβερνοασφάλειας εγκαθίστανται σε ολόκληρο τον οργανισμό, συμπεριλαμβανομένων των κινδύνων από προμηθευτές και άλλα τρίτα μέρη
  - **GV.RM-06:** Μια τυποποιημένη μέθοδος για τον υπολογισμό, την τεκμηρίωση, την κατηγοριοποίηση και την προτεραιοποίηση κινδύνων κυβερνοασφάλειας καθορίζεται και κοινοποιείται

- **GV.RM-07:** Οι στρατηγικές ευκαιρίες (δηλ. οι θετικοί κίνδυνοι) προσδιορίζονται και συμπεριλαμβάνονται σε οργανωσιακές συζητήσεις για τους κινδύνους κυβερνοασφάλειας

- **Ρόλοι, Ευθύνες και Αρμοδιότητες (GV.RR):** Ρόλοι, ευθύνες και αρμοδιότητες κυβερνοασφάλειας καθορίζονται και κοινοποιούνται για την ενίσχυση της λογοδοσίας, της αξιολόγησης της απόδοσης και της συνεχούς βελτίωσης
  - **GV.RR-01:** Η ηγεσία του οργανισμού είναι υπεύθυνη για τους κινδύνους κυβερνοασφάλειας, λογοδοτεί για αυτούς και προωθεί μία κουλτούρα που ενισχύει την επίγνωση των κινδύνων, είναι ηθική και βελτιώνεται συνεχώς
  - **GV.RR-02:** Ρόλοι, ευθύνες και αρμοδιότητες που σχετίζονται με τη διαχείριση κινδύνων κυβερνοασφάλειας καθορίζονται, κοινοποιούνται, κατανοούνται και επιβάλλονται
  - **GV.RR-03:** Γίνεται κατανομή επαρκών πόρων ανάλογα με τη στρατηγική κινδύνων κυβερνοασφάλειας του οργανισμού, τους ρόλους, τις ευθύνες και τις πολιτικές
  - **GV.RR-04:** Η κυβερνοασφάλεια περιλαμβάνεται στις πρακτικές του ανθρώπινου δυναμικού

- **Πολιτική (GV.PO):** Η πολιτική κυβερνοασφάλειας του οργανισμού καθορίζεται, κοινοποιείται και επιβάλλεται
  - **GV.PO-01:** Η πολιτική για τη διαχείριση κινδύνων κυβερνοασφάλειας θεσπίζεται με βάση το οργανωτικό πλαίσιο, τη στρατηγική κυβερνοασφάλειας και τις προτεραιότητες και κοινοποιείται και επιβάλλεται
  - **GV.PO-02:** Η πολιτική για τη διαχείριση κινδύνων κυβερνοασφάλειας επανεξετάζεται, αναθεωρείται, κοινοποιείται και επιβάλλεται αντικατοπτρίζοντας τις αλλαγές στις απαιτήσεις, τις απειλές, την τεχνολογία και την αποστολή του οργανισμού

- **Εποπτεία (GV.OV):** Τα αποτελέσματα των δραστηριοτήτων διαχείρισης κινδύνων κυβερνοασφάλειας και οι επιδόσεις στο σύνολο του οργανισμού χρησιμοποιούνται για την ενημέρωση, τη βελτίωση και την προσαρμογή της στρατηγικής διαχείρισης κινδύνων
  - **GV.OV-01:** Τα αποτελέσματα της στρατηγικής διαχείρισης κινδύνων κυβερνοασφάλειας επανεξετάζονται έτσι ώστε η στρατηγική και η κατεύθυνση του οργανισμού να ενημερώνονται και να προσαρμόζονται
  - **GV.OV-02:** Η στρατηγική διαχείρισης κινδύνων κυβερνοασφάλειας αναθεωρείται και προσαρμόζεται έτσι ώστε να διασφαλίζει την κάλυψη των οργανωσιακών απαιτήσεων και κινδύνων
  - **GV.OV-03:** Οι επιδόσεις του οργανισμού ως προς τη διαχείριση κινδύνων κυβερνοασφάλειας αξιολογούνται και επανεξετάζονται για την πραγματοποίηση απαιτούμενων προσαρμογών

- **Διαχείριση Κινδύνων Κυβερνοασφάλειας στην Εφοδιαστική Αλυσίδα (GV.SC):** Διαδικασίες διαχείρισης κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα προσδιορίζονται, καθορίζονται, τελούν υπό διαχείριση, παρακολουθούνται και βελτιώνονται από τα ενδιαφερόμενα μέρη του οργανισμού

- **GV.SC-01:** Το πρόγραμμα, η στρατηγική, οι στόχοι, οι πολιτικές και οι διαδικασίες διαχείρισης κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα καθορίζονται και συμφωνούνται από τα ενδιαφερόμενα μέρη του οργανισμού
- **GV.SC-02:** Ρόλοι και αρμοδιότητες σε σχέση με την κυβερνοασφάλεια για προμηθευτές, πελάτες και συνεργάτες καθορίζονται, κοινοποιούνται και συντονίζονται εσωτερικά και εξωτερικά
- **GV.SC-03:** Η διαχείριση κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα είναι ενσωματωμένη στις διαδικασίες κυβερνοασφάλειας και διαχείρισης επιχειρηματικών κινδύνων, αξιολόγησης κινδύνων και βελτίωσης
- **GV.SC-04:** Οι προμηθευτές είναι γνωστοί και ιεραρχούνται βάσει κρισιμότητας
- **GV.SC-05:** Απαιτήσεις για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα καθορίζονται, ιεραρχούνται και ενσωματώνονται σε συμβάσεις ή σε άλλου τύπου συμφωνίες με προμηθευτές και άλλα σχετικά τρίτα μέρη
- **GV.SC-06:** Ο οργανισμός πραγματοποιεί προγραμματισμό και επιδεικνύει τη δέουσα επιμέλεια για τη μείωση των κινδύνων πριν από την έναρξη σχέσεων με επίσημους προμηθευτές ή άλλα τρίτα μέρη
- **GV.SC-07:** Οι κίνδυνοι που ενέχουν οι προμηθευτές, τα προϊόντα και οι υπηρεσίες τους, και άλλα τρίτα μέρη γίνονται κατανοητοί, καταγράφονται, ιεραρχούνται, αξιολογούνται, αντιμετωπίζονται και παρακολουθούνται κατά τη διάρκεια της σχέσης
- **GV.SC-08:** Σχετικοί προμηθευτές και άλλα τρίτα μέρη περιλαμβάνονται στις δραστηριότητες σχεδιασμού αντιμετώπισης περιστατικών ασφάλειας, ανταπόκρισης και ανάκαμψης
- **GV.SC-09:** Οι πρακτικές ασφάλειας της εφοδιαστικής αλυσίδας ενσωματώνονται στα προγράμματα κυβερνοασφάλειας και διαχείρισης επιχειρηματικών κινδύνων και οι επιδόσεις τους παρακολουθούνται σε όλο τον κύκλο ζωής του τεχνολογικού προϊόντος και της υπηρεσίας
- **GV.SC-10:** Τα σχέδια διαχείρισης κινδύνων κυβερνοασφάλειας στην εφοδιαστική αλυσίδα περιλαμβάνουν προβλέψεις για δραστηριότητες που πραγματοποιούνται μετά τη σύναψη μιας συνεργασίας ή μιας συμφωνίας παροχής υπηρεσιών

ΠΡΟΣΔΙΟΡΙΣΜΟΣ (ID): Γίνονται κατανοητοί οι τρέχοντες κίνδυνοι κυβερνοασφάλειας του οργανισμού

- **Διαχείριση Αγαθών (ID.AM):** Αγαθά (π.χ. δεδομένα, υλικό, λογισμικό, συστήματα, εγκαταστάσεις, υπηρεσίες, προσωπικό) που επιτρέπουν στον οργανισμό να επιτύχει τους επιχειρηματικούς σκοπούς του προσδιορίζονται και τελούν υπό διαχείριση σύμφωνα με τη σχετική σημασία τους για τους οργανωτικούς στόχους και τη στρατηγική κινδύνων του οργανισμού
  - **ID.AM-01:** Διατηρούνται καταγραφές του υλικού που διαχειρίζεται ο οργανισμός

- **ID.AM-02:** Διατηρούνται καταγραφές του λογισμικού, των υπηρεσιών και των συστημάτων που διαχειρίζεται ο οργανισμός
- **ID.AM-03:** Διατηρούνται αναπαραστάσεις της εξουσιοδοτημένης δικτυακής επικοινωνίας του οργανισμού και των ροών δεδομένων του εσωτερικού και εξωτερικού δικτύου
- **ID.AM-04:** Διατηρούνται καταγραφές των υπηρεσιών που παρέχονται από προμηθευτές
- **ID.AM-05:** Τα πληροφοριακά αγαθά ιεραρχούνται με βάση την ταξινόμηση, την κρισιμότητα, τους πόρους και τον αντίκτυπο στην αποστολή
- **ID.AM-07:** Διατηρούνται κατάλογοι δεδομένων και αντίστοιχων μεταδεδομένων για καθορισμένους τύπους δεδομένων
- **ID.AM-08:** Τα συστήματα, το υλικό, το λογισμικό, οι υπηρεσίες και τα δεδομένα τελούν υπό διαχείριση καθ' όλη τη διάρκεια του κύκλου ζωής τους

- **Εκτίμηση Κινδύνων (ID.RA):** Οι κίνδυνοι κυβερνοασφάλειας για τον οργανισμό, τα πληροφοριακά αγαθά και τα άτομα γίνονται κατανοητοί από τον οργανισμό
  - **ID.RA-01:** Εντοπίζονται, επικυρώνονται και καταγράφονται οι ευπάθειες των πληροφοριακών αγαθών
  - **ID.RA-02:** Πληροφορίες για απειλές στον κυβερνοχώρο λαμβάνονται από φόρουμ και πηγές ανταλλαγής πληροφοριών
  - **ID.RA-03:** Εντοπίζονται και καταγράφονται οι εσωτερικές και εξωτερικές απειλές για τον οργανισμό
  - **ID.RA-04:** Εντοπίζονται και καταγράφονται οι πιθανές επιπτώσεις και οι πιθανότητες των απειλών να εκμεταλλευτούν τις ευπάθειες
  - **ID.RA-05:** Οι απειλές, οι ευπάθειες, οι πιθανότητες και οι επιπτώσεις χρησιμοποιούνται για την κατανόηση του εγγενούς κινδύνου και ενημερώνουν την προτεραιοποίηση αντιμετώπισης των κινδύνων
  - **ID.RA-06:** Οι τρόποι αντιμετώπισης κινδύνων επιλέγονται, ιεραρχούνται, σχεδιάζονται, παρακολουθούνται και κοινοποιούνται
  - **ID.RA-07:** Οι αλλαγές και οι εξαιρέσεις τελούν υπό διαχείριση, αξιολογούνται ως προς τον αντίκτυπό τους στον κίνδυνο, καταγράφονται και παρακολουθούνται
  - **ID.RA-08:** Θεσπίζονται διαδικασίες για τη λήψη, την ανάλυση και την ανταπόκριση σε γνωστοποιήσεις ευπαθειών
  - **ID.RA-09:** Η αυθεντικότητα και η ακεραιότητα του υλικού και του λογισμικού αξιολογούνται πριν από την απόκτηση και τη χρήση τους
  - **ID.RA-10:** Οι κρίσιμοι προμηθευτές αξιολογούνται πριν από την απόκτηση

- **Βελτίωση (ID.IM):** Εντοπίζονται βελτιώσεις στις οργανωτικές διεργασίες, διαδικασίες και δραστηριότητες διαχείρισης κινδύνων κυβερνοασφάλειας σε όλες τις Λειτουργίες του Πλαισίου

- **ID.IM-01:** Εντοπίζονται βελτιώσεις από τις αξιολογήσεις
- **ID.IM-02:** Εντοπίζονται βελτιώσεις από δοκιμές και ασκήσεις ασφάλειας, συμπεριλαμβανομένων εκείνων που γίνονται σε συντονισμό με τους προμηθευτές και τα σχετικά τρίτα μέρη
- **ID.IM-03:** Εντοπίζονται βελτιώσεις από την εκτέλεση επιχειρησιακών διεργασιών, διαδικασιών και δραστηριοτήτων
- **ID.IM-04:** Τα σχέδια αντιμετώπισης περιστατικών και άλλα σχέδια κυβερνοασφάλειας που επηρεάζουν τη λειτουργία του οργανισμού καταρτίζονται, κοινοποιούνται, διατηρούνται και βελτιώνονται

ΠΡΟΣΤΑΣΙΑ (PR): Αξιοποιούνται μέτρα προστασίας για τη διαχείριση των κινδύνων κυβερνοασφάλειας του οργανισμού

- **Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης (PR.AA):** Η πρόσβαση σε φυσικά και λογικά πληροφοριακά αγαθά περιορίζεται σε εξουσιοδοτημένους χρήστες, υπηρεσίες και υλικό, και ο οργανισμός τη διαχειρίζεται ανάλογα με τον εκτιμώμενο κίνδυνο μη εξουσιοδοτημένης πρόσβασης
  - **PR.AA-01:** Ο οργανισμός διαχειρίζεται ταυτότητες και διαπιστευτήρια για εξουσιοδοτημένους χρήστες, υπηρεσίες και υλικό
  - **PR.AA-02:** Οι ταυτότητες αποδεικνύονται και συνδέονται με διαπιστευτήρια βασισμένα στις αλληλεπιδράσεις
  - **PR.AA-03:** Πραγματοποιείται αυθεντικοποίηση των χρηστών, των υπηρεσιών και του υλικού
  - **PR.AA-04:** Οι ισχυρισμοί ταυτότητας προστατεύονται, διαβιβάζονται και επαληθεύονται
  - **PR.AA-05:** Οι άδειες πρόσβασης, τα δικαιώματα και οι εξουσιοδοτήσεις ορίζονται σε μία πολιτική, και γίνεται διαχείριση, επιβολή και επανεξέταση αυτών, ενσωματώνοντας τις αρχές των ελάχιστων προνομίων και του διαχωρισμού καθηκόντων
  - **PR.AA-06:** Ο οργανισμός διαχειρίζεται, παρακολουθεί και επιβάλλει τη φυσική πρόσβαση στα πληροφοριακά αγαθά ανάλογα με τους κινδύνους
- **Ευαισθητοποίηση και Εκπαίδευση (PR.AT):** Ο οργανισμός παρέχει στο προσωπικό του ευαισθητοποίηση και εκπαίδευση για την κυβερνοασφάλεια, ώστε το προσωπικό να μπορεί να εκτελεί τα σχετικά με την κυβερνοασφάλεια καθήκοντά του
  - **PR.AT-01:** Στο προσωπικό παρέχεται ευαισθητοποίηση και εκπαίδευση ώστε να κατέχει τις γνώσεις και δεξιότητες για την εκτέλεση γενικών εργασιών λαμβάνοντας υπόψη τους κινδύνους κυβερνοασφάλειας

- **PR.AT-02:** Σε άτομα με εξειδικευμένους ρόλους παρέχεται ευαισθητοποίηση και εκπαίδευση ώστε να κατέχουν τις γνώσεις και δεξιότητες για την εκτέλεση των σχετικών με το αντικείμενό τους εργασιών λαμβάνοντας υπόψη τους κινδύνους κυβερνοασφάλειας

- **Ασφάλεια Δεδομένων (PR.DS):** Η διαχείριση των δεδομένων γίνεται σύμφωνα με τη στρατηγική αντιμετώπισης κινδύνων του οργανισμού με σκοπό την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών
  - **PR.DS-01:** Η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων προστατεύεται κατά την αποθήκευσή τους
  - **PR.DS-02:** Η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων προστατεύεται κατά τη μεταφορά τους
  - **PR.DS-10:** Η εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων προστατεύεται κατά τη χρήση τους
  - **PR.DS-11:** Αντίγραφα ασφάλειας των δεδομένων δημιουργούνται, προστατεύονται, διατηρούνται και ελέγχονται

- **Ασφάλεια Πλατφόρμας (PR.PS):** Η διαχείριση του υλικού, του λογισμικού (π.χ., υλικολογισμικό, λειτουργικά συστήματα, εφαρμογές) και των υπηρεσιών φυσικών και εικονικών πλατφορμών είναι συμβατή με τη στρατηγική αντιμετώπισης κινδύνων του οργανισμού με στόχο την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητάς τους
  - **PR.PS-01:** Πρακτικές διαχείρισης διαμόρφωσης συστημάτων καθιερώνονται και εφαρμόζονται
  - **PR.PS-02:** Το λογισμικό συντηρείται, αντικαθίσταται και αφαιρείται ανάλογα με τον κίνδυνο
  - **PR.PS-03:** Το υλικό συντηρείται, αντικαθίσταται και αφαιρείται ανάλογα με τον κίνδυνο
  - **PR.PS-04:** Αρχεία καταγραφής δημιουργούνται και διατίθενται για συνεχή παρακολούθηση
  - **PR.PS-05:** Αποτρέπεται η εγκατάσταση και η εκτέλεση μη εξουσιοδοτημένου λογισμικού
  - **PR.PS-06:** Ασφαλείς πρακτικές ανάπτυξης λογισμικού ενσωματώνονται και η απόδοσή τους παρακολουθείται καθ' όλη τη διάρκεια του κύκλου ζωής ανάπτυξης λογισμικού

- **Ανθεκτικότητα Τεχνολογικής Υποδομής (PR.IR):** Ο οργανισμός διαχειρίζεται τις αρχιτεκτονικές ασφάλειας σύμφωνα με τη στρατηγική αντιμετώπισης κινδύνων του με στόχο την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριακών αγαθών του και της οργανωσιακής ανθεκτικότητας
  - **PR.IR-01:** Τα δίκτυα και τα περιβάλλοντα προστατεύονται από μη εξουσιοδοτημένη λογική πρόσβαση και χρήση

- **PR.IR-02:** Τα τεχνολογικά πληροφοριακά αγαθά του οργανισμού προστατεύονται από περιβαλλοντικές απειλές
- **PR.IR-03:** Εφαρμόζονται μηχανισμοί για την επίτευξη των απαιτήσεων ανθεκτικότητας σε κανονικές και δυσμενείς καταστάσεις
- **PR.IR-04:** Εξασφαλίζεται επαρκής χωρητικότητα πόρων για τη διασφάλιση της διαθεσιμότητας

ΕΝΤΟΠΙΣΜΟΣ (DE): Εντοπίζονται και αναλύονται πιθανές επιθέσεις και παραβιάσεις κυβερνοασφάλειας

- **Συνεχής Παρακολούθηση (DE.CM):** Τα πληροφοριακά αγαθά παρακολουθούνται για να εντοπιστούν ανωμαλίες, ενδείξεις έκθεσης σε κίνδυνο και άλλα δυνητικά ανεπιθύμητα συμβάντα
  - **DE.CM-01:** Τα δίκτυα και οι υπηρεσίες δικτύου παρακολουθούνται για τον εντοπισμό πιθανών ανεπιθύμητων συμβάντων
  - **DE.CM-02:** Το φυσικό περιβάλλον παρακολουθείται για τον εντοπισμό πιθανών ανεπιθύμητων συμβάντων
  - **DE.CM-03:** Η δραστηριότητα του προσωπικού και η χρήση τεχνολογίας παρακολουθούνται για τον εντοπισμό πιθανών ανεπιθύμητων συμβάντων
  - **DE.CM-06:** Οι δραστηριότητες και οι υπηρεσίες των εξωτερικών παρόχων υπηρεσιών παρακολουθούνται για τον εντοπισμό πιθανών ανεπιθύμητων συμβάντων
  - **DE.CM-09:** Το υλικό και λογισμικό των υπολογιστών, τα περιβάλλοντα χρόνου εκτέλεσης και τα δεδομένα τους παρακολουθούνται για τον εντοπισμό πιθανών ανεπιθύμητων συμβάντων
- **Ανάλυση Ανεπιθύμητων Συμβάντων (DE.AE):** Ανωμαλίες, ενδείξεις έκθεσης σε κίνδυνο και άλλα δυνητικά ανεπιθύμητα συμβάντα αναλύονται για τον χαρακτηρισμό των συμβάντων και τον εντοπισμό περιστατικών κυβερνοασφάλειας
  - **DE.AE-02:** Τα πιθανά ανεπιθύμητα συμβάντα αναλύονται για την καλύτερη κατανόηση των σχετικών με αυτά δραστηριοτήτων
  - **DE.AE-03:** Πραγματοποιείται συσχετισμός πληροφοριών από πολλαπλές πηγές
  - **DE.AE-04:** Ο εκτιμώμενος αντίκτυπος και το εύρος των ανεπιθύμητων συμβάντων γίνονται κατανοητά
  - **DE.AE-06:** Πληροφορίες για τα ανεπιθύμητα συμβάντα παρέχονται σε εξουσιοδοτημένο προσωπικό και εργαλεία
  - **DE.AE-07:** Πληροφορίες για τις απειλές κυβερνοασφάλειας και άλλες σχετικές πληροφορίες ενσωματώνονται στην ανάλυση

- **DE.AE-08:** Περιστατικά ασφάλειας δηλώνονται όταν τα ανεπιθύμητα συμβάντα πληρούν τα καθορισμένα κριτήρια

ΑΝΤΑΠΟΚΡΙΣΗ (RS): Αναλαμβάνονται δράσεις για την αντιμετώπιση ενός εντοπισμένου περιστατικού κυβερνοασφάλειας

- **Διαχείριση Περιστατικών (RS.MA):** Γίνεται διαχείριση των αντιδράσεων σε εντοπισμένα περιστατικά κυβερνοασφάλειας
  - **RS.MA-01:** Μόλις δηλωθεί ένα περιστατικό, το σχέδιο αντιμετώπισης περιστατικών εκτελείται σε συντονισμό με τα σχετικά τρίτα μέρη
  - **RS.MA-02:** Οι αναφορές περιστατικών ταξινομούνται και επικυρώνονται
  - **RS.MA-03:** Τα περιστατικά κατηγοριοποιούνται και ιεραρχούνται
  - **RS.MA-04:** Τα περιστατικά κλιμακώνονται ή αναβαθμίζονται όταν είναι απαραίτητο
  - **RS.MA-05:** Εφαρμόζονται τα κριτήρια για την έναρξη ανάκαμψης από περιστατικά
- **Ανάλυση Περιστατικών (RS.AN):** Διεξάγονται έρευνες για να διασφαλιστεί η αποτελεσματική ανταπόκριση και να υποστηρίζονται οι δραστηριότητες ψηφιακής εγκληματολογίας και ανάκαμψης
  - **RS.AN-03:** Πραγματοποιείται ανάλυση για να διαπιστωθεί τι έλαβε χώρα κατά τη διάρκεια ενός περιστατικού και ποια ήταν η βασική αιτία του
  - **RS.AN-06:** Καταγράφονται οι ενέργειες που εκτελούνται κατά τη διάρκεια μιας έρευνας και διατηρείται η ακεραιότητα και η προέλευση των αρχείων
  - **RS.AN-07:** Συλλέγονται δεδομένα και μεταδεδομένα του περιστατικού και διατηρείται η ακεραιότητα και η προέλευσή τους
  - **RS.AN-08:** Το μέγεθος ενός περιστατικού εκτιμάται και επικυρώνεται
- **Αναφορά και Επικοινωνία Ανταπόκρισης σε Περιστατικά (RS.CO):** Οι δραστηριότητες αντιμετώπισης συντονίζονται με τους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς, όπως απαιτείται από νόμους, κανονισμούς ή πολιτικές
  - **RS.CO-02:** Τα εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη ενημερώνονται για περιστατικά
  - **RS.CO-03:** Οι πληροφορίες κοινοποιούνται στους καθορισμένους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς
- **Μετριασμός Περιστατικών (RS.MI):** Λαμβάνονται μέτρα για την πρόληψη της εξάπλωσης ενός συμβάντος και τη μείωση των επιπτώσεών του
  - **RS.MI-01:** Τα περιστατικά περιορίζονται
  - **RS.MI-02:** Τα περιστατικά εξαλείφονται

ΑΝΑΚΑΜΨΗ (RC): Αποκαθίστανται τα πληροφοριακά αγαθά και οι λειτουργίες που επηρεάζονται από ένα περιστατικό κυβερνοασφάλειας

- **Εκτέλεση Σχεδίου Αποκατάστασης από Περιστατικά (RC.RP):** Εκτελούνται δραστηριότητες αποκατάστασης για να διασφαλιστεί η επιχειρησιακή διαθεσιμότητα των συστημάτων και των υπηρεσιών που επηρεάζονται από περιστατικά κυβερνοασφάλειας
  - **RC.RP-01:** Το τμήμα ανάκαμψης του σχεδίου αντιμετώπισης περιστατικών εκτελείται μόλις αυτό ξεκινήσει από τη διαδικασία αντιμετώπισης περιστατικών
  - **RC.RP-02:** Οι ενέργειες ανάκαμψης επιλέγονται, ορίζεται το εύρος τους, ιεραρχούνται και εκτελούνται
  - **RC.RP-03:** Η ακεραιότητα των αντιγράφων ασφάλειας και άλλων πληροφοριακών αγαθών αποκατάστασης επαληθεύεται πριν από τη χρήση τους για επαναφορά
  - **RC.RP-04:** Οι κρίσιμες λειτουργίες αποστολής και η διαχείριση κινδύνων κυβερνοασφάλειας λαμβάνονται υπόψη για την καθιέρωση επιχειρησιακών προτύπων μετά από ένα περιστατικό
  - **RC.RP-05:** Επαληθεύεται η ακεραιότητα των πληροφοριακών αγαθών, αποκαθίστανται τα συστήματα και οι υπηρεσίες και επιβεβαιώνεται η κανονική κατάσταση λειτουργίας
  - **RC.RP-06:** Το τέλος της ανάκαμψης από το περιστατικό κηρύσσεται βάσει κριτηρίων και ολοκληρώνεται η τεκμηρίωση που σχετίζεται με το περιστατικό
- **Επικοινωνία Ανάκαμψης από Περιστατικά (RC.CO):** Οι δραστηριότητες ανάκαμψης συντονίζονται με εσωτερικά και εξωτερικά μέρη
  - **RC.CO-03:** Οι δραστηριότητες ανάκαμψης και η πρόοδος όσον αφορά την αποκατάσταση των λειτουργικών ικανοτήτων κοινοποιούνται σε καθορισμένους εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς
  - **RC.CO-04:** Οι δημόσιες ενημερώσεις σχετικά με την ανάκαμψη από περιστατικά κοινοποιούνται χρησιμοποιώντας εγκεκριμένες μεθόδους και μηνύματα

Παράρτημα Β. Βαθμίδες του Πλαισίου

Ο Πίνακας 2 περιέχει μια εννοιολογική απεικόνιση των Βαθμίδων του Πλαισίου που συζητήθηκαν στην Ενότητα 3. Για έναν οργανισμό, οι Βαθμίδες χαρακτηρίζουν την αυστηρότητα των πρακτικών διακυβέρνησης κινδύνων κυβερνοασφάλειας (ΔΙΑΚΥΒΕΡΝΗΣΗ) και των πρακτικών διαχείρισης κινδύνων κυβερνοασφάλειας (ΠΡΟΣΔΙΟΡΙΣΜΟΣ, ΠΡΟΣΤΑΣΙΑ, ΕΝΤΟΠΙΣΜΟΣ, ΑΝΤΑΠΟΚΡΙΣΗ, και ΑΝΑΚΑΜΨΗ).

Πίνακας 2. Εννοιολογική Απεικόνιση των Βαθμίδων του Πλαισίου

Βαθμίδα	Διακυβέρνηση Κινδύνων Κυβερνοασφάλειας	Διαχείριση Κινδύνων Κυβερνοασφάλειας
Βαθμίδα 1: Μερικής Υλοποίησης	Η εφαρμογή της οργανωσιακής στρατηγικής διαχείρισης κινδύνων κυβερνοασφάλειας γίνεται με ad hoc τρόπο. Η ιεράρχηση είναι ad hoc και δεν βασίζεται επίσημα σε στόχους ή στο περιβάλλον απειλών.	Υπάρχει περιορισμένη επίγνωση των κινδύνων κυβερνοασφάλειας σε οργανωσιακό επίπεδο. Ο οργανισμός διαχειρίζεται τους κινδύνους κυβερνοασφάλειας σε μη κανονική βάση, κατά περίπτωση. Ο οργανισμός ενδέχεται να μην διαθέτει διαδικασίες που επιτρέπουν την κοινή χρήση πληροφοριών κυβερνοασφάλειας εντός του οργανισμού. Ο οργανισμός γενικά δε γνωρίζει τους κινδύνους κυβερνοασφάλειας που σχετίζονται με τους προμηθευτές του και με τα προϊόντα και τις υπηρεσίες που αποκτά και χρησιμοποιεί.
Βαθμίδα 2: Επίγνωσης Κινδύνου	Οι πρακτικές διαχείρισης κινδύνων εγκρίνονται από τη διοίκηση, αλλά ενδέχεται να μην είναι καθιερωμένες ως πολιτικές σε επίπεδο οργανισμού. Η ιεράρχηση των δραστηριοτήτων κυβερνοασφάλειας και των αναγκών προστασίας αντικατοπτρίζει άμεσα τους οργανωσιακούς στόχους κινδύνων, το περιβάλλον απειλών ή τις επιχειρησιακές απαιτήσεις.	Υπάρχει επίγνωση των κινδύνων κυβερνοασφάλειας σε οργανωσιακό επίπεδο, αλλά δεν έχει καθιερωθεί μια προσέγγιση σε επίπεδο οργανισμού για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Η κυβερνοασφάλεια σε οργανωσιακούς στόχους και προγράμματα μπορεί να λαμβάνεται υπόψη σε ορισμένα αλλά όχι σε όλα τα επίπεδα του οργανισμού. Η αξιολόγηση των κινδύνων κυβερνοασφάλειας των οργανωσιακών και εξωτερικών πληροφοριακών αγαθών λαμβάνει χώρα, αλλά συνήθως δεν είναι επαναλαμβανόμενη. Οι πληροφορίες για την κυβερνοασφάλεια κοινοποιούνται εντός του οργανισμού ανεπίσημα. Ο οργανισμός γνωρίζει τους κινδύνους κυβερνοασφάλειας που σχετίζονται με τους προμηθευτές του, τα προϊόντα και τις υπηρεσίες

Βαθμίδα	Διακυβέρνηση Κινδύνων Κυβερνοασφάλειας	Διαχείριση Κινδύνων Κυβερνοασφάλειας
		που αποκτά και χρησιμοποιεί, αλλά δεν ανταποκρίνεται σε αυτούς τους κινδύνους με συνέπεια ή με επίσημο τρόπο.
Βαθμίδα 3: Επαναλαμβανόμενων Πρακτικών	Οι πρακτικές διαχείρισης κινδύνων του οργανισμού εγκρίνονται επίσημα και εκφράζονται ως πολιτική. Οι πολιτικές, οι διεργασίες και οι διαδικασίες που λαμβάνονται εν όψει των κινδύνων, εφαρμόζονται όπως προβλέπεται και αναθεωρούνται. Οι οργανωσιακές πρακτικές κυβερνοασφάλειας επικαιροποιούνται τακτικά με βάση την εφαρμογή των διαδικασιών διαχείρισης κινδύνων παρακολουθώντας τις μεταβολές των επιχειρησιακών απαιτήσεων, των απειλών και του τεχνολογικού τοπίου.	Υπάρχει μια προσέγγιση σε επίπεδο οργανισμού για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Οι πληροφορίες για την κυβερνοασφάλεια κοινοποιούνται τακτικά σε όλο τον οργανισμό. Εφαρμόζονται συνεπείς μέθοδοι για την αποτελεσματική ανταπόκριση στις αλλαγές των κινδύνων. Το προσωπικό διαθέτει τις γνώσεις και τις δεξιότητες για να πληροί τους καθορισμένους ρόλους και να υπηρετεί τα καθήκοντά του. Ο οργανισμός παρακολουθεί με συνέπεια και ακρίβεια τους κινδύνους κυβερνοασφάλειας των πληροφοριακών αγαθών του. Διευθυντικά στελέχη κυβερνοασφάλειας και διευθυντικά στελέχη άλλων τομέων επικοινωνούν τακτικά σχετικά με τους κινδύνους κυβερνοασφάλειας. Τα διευθυντικά στελέχη διασφαλίζουν ότι λαμβάνεται υπόψη η κυβερνοασφάλεια σε όλες τις λειτουργίες του οργανισμού. Η οργανωσιακή στρατηγική διαχείρισης κινδύνου λαμβάνει υπόψη τους κινδύνους κυβερνοασφάλειας που σχετίζονται με τους προμηθευτές, τα προϊόντα και τις υπηρεσίες που αποκτά και χρησιμοποιεί. Το προσωπικό ενεργεί επίσημα σε ό,τι έχει σχέση με αυτούς τους κινδύνους μέσω μηχανισμών όπως γραπτές συμφωνίες για την κοινοποίηση βασικών απαιτήσεων, δομές διακυβέρνησης (π.χ. συμβούλια διαχείρισης κινδύνου) και εφαρμογή και παρακολούθηση των πολιτικών. Οι ενέργειες αυτές υλοποιούνται με συνέπεια και όπως προβλέπεται, εποπτεύονται και επανεξετάζονται συνεχώς.

Βαθμίδα	Διακυβέρνηση Κινδύνων Κυβερνοασφάλειας	Διαχείριση Κινδύνων Κυβερνοασφάλειας
Βαθμίδα 4: Προσαρμοζόμενων Πρακτικών	Υπάρχει μια προσέγγιση σε επίπεδο οργανισμού για τη διαχείριση των κινδύνων κυβερνοασφάλειας, η οποία χρησιμοποιεί πολιτικές, διεργασίες και διαδικασίες που βασίζονται στην αντιμετώπιση πιθανών συμβάντων κινδύνων κυβερνοασφάλειας. Η σχέση μεταξύ των κινδύνων κυβερνοασφάλειας και των οργανωσιακών στόχων είναι σαφώς κατανοητή και λαμβάνεται υπόψη κατά τη λήψη αποφάσεων. Τα διευθυντικά στελέχη παρακολουθούν τους κινδύνους κυβερνοασφάλειας στο ίδιο πλαίσιο με τους οικονομικούς και άλλους οργανωσιακούς κινδύνους. Ο προϋπολογισμός του οργανισμού βασίζεται στην κατανόηση του τρέχοντος και προβλεπόμενου περιβάλλοντος κινδύνου και της ανοχής κινδύνου. Οι επιχειρησιακοί τομείς εφαρμόζουν το εκτελεστικό όραμα και αναλύουν τους κινδύνους σε επίπεδο συστήματος στο πλαίσιο της ανοχής κινδύνου του οργανισμού. Η διαχείριση κινδύνων κυβερνοασφάλειας αποτελεί μέρος της κουλτούρας του οργανισμού. Εξελίσσεται μέσα από την επίγνωση των προηγούμενων δραστηριοτήτων και τη συνεχή επίγνωση των δραστηριοτήτων στα συστήματα και τα δίκτυα. Ο οργανισμός μπορεί γρήγορα και αποτελεσματικά να υπολογίσει τις αλλαγές των επιχειρησιακών στόχων στον τρόπο προσέγγισης και επικοινωνίας των κινδύνων.	Ο οργανισμός προσαρμόζει τις πρακτικές κυβερνοασφάλειάς του με βάση προηγούμενες και τρέχουσες δραστηριότητες κυβερνοασφάλειας, συμπεριλαμβανομένων των διδαγμάτων και των προγνωστικών δεικτών. Μέσα από μια διαδικασία συνεχούς βελτίωσης που ενσωματώνει προηγμένες τεχνολογίες και πρακτικές κυβερνοασφάλειας, ο οργανισμός προσαρμόζεται ενεργά στο μεταβαλλόμενο τεχνολογικό τοπίο και ανταποκρίνεται έγκαιρα και αποτελεσματικά σε εξελιγμένες και εξελισσόμενες απειλές. Ο οργανισμός χρησιμοποιεί πληροφορίες σε πραγματικό ή σχεδόν πραγματικό χρόνο για να κατανοεί και να ενεργεί με συνέπεια σε ό,τι έχει σχέση με τους κινδύνους κυβερνοασφάλειας που σχετίζονται με τους προμηθευτές, τα προϊόντα και τις υπηρεσίες που αποκτά και χρησιμοποιεί. Οι πληροφορίες για την κυβερνοασφάλεια κοινοποιούνται συνεχώς σε όλο τον οργανισμό και σε εξουσιοδοτημένα τρίτα μέρη.

Παράρτημα Γ. Πίνακας Όρων

Κατηγορία του Πλαισίου

Μια ομάδα συναφών αποτελεσμάτων κυβερνοασφάλειας που συνθέτουν συλλογικά μια Λειτουργία του Πλαισίου.

Κοινοτικό Προφίλ του Πλαισίου
Ένα βασικό επίπεδο αποτελεσμάτων του Πλαισίου που δημιουργείται και δημοσιεύεται για την αντιμετώπιση κοινών συμφερόντων και στόχων μεταξύ πολλών οργανισμών. Ένα Κοινοτικό Προφίλ αναπτύσσεται συνήθως για έναν συγκεκριμένο τομέα, υποτομέα, τεχνολογία, τύπο απειλής ή άλλη περίπτωση χρήσης. Ένας οργανισμός μπορεί να χρησιμοποιήσει ένα Κοινοτικό Προφίλ ως βάση για το δικό του Προφίλ-Στόχο.

Πυρήνας του Πλαισίου
Μια ταξινόμηση υψηλού επιπέδου επιθυμητών αποτελεσμάτων κυβερνοασφάλειας που μπορεί να βοηθήσει κάθε οργανισμό να διαχειριστεί τους κινδύνους κυβερνοασφάλειάς του. Τα στοιχεία του είναι μια ιεραρχία Λειτουργιών, Κατηγοριών και Υποκατηγοριών που περιγράφουν λεπτομερώς κάθε αποτέλεσμα.

Τρέχον Προφίλ του Πλαισίου
Ένα μέρος ενός Οργανωτικού Προφίλ που προσδιορίζει τα αποτελέσματα του Πυρήνα που ένας οργανισμός επιτυγχάνει επί του παρόντος (ή προσπαθεί να επιτύχει) και χαρακτηρίζει τον τρόπο ή τον βαθμό επίτευξης κάθε αποτελέσματος.

Λειτουργία του Πλαισίου
Το υψηλότερο επίπεδο οργάνωσης για τα αποτελέσματα της κυβερνοασφάλειας. Υπάρχουν έξι Λειτουργίες του Πλαισίου: Διακυβέρνηση, Προσδιορισμός, Προστασία, Εντοπισμός, Ανταπόκριση και Ανάκαμψη.

Παράδειγμα Υλοποίησης του Πλαισίου
Μια συνοπτική, προσανατολισμένη στη δράση, εννοιολογική απεικόνιση ενός τρόπου που συμβάλλει στην επίτευξη ενός αποτελέσματος του Πυρήνα του Πλαισίου.

Πληροφοριακή Αναφορά του Πλαισίου
Μια αντιστοίχιση που υποδεικνύει μια σχέση μεταξύ ενός αποτελέσματος του Πυρήνα του Πλαισίου και ενός υπάρχοντος προτύπου, κατευθυντήριας γραμμής, κανονισμού ή άλλου περιεχομένου.

Οργανωτικό Προφίλ του Πλαισίου
Ένας μηχανισμός για την περιγραφή του τρέχοντα ή/και του επιδιωκόμενου τρόπου τοποθέτησης ενός οργανισμού ως προς την κυβερνοασφάλεια, σε όρους αποτελεσμάτων του Πυρήνα.

Οδηγός Γρήγορης Εκκίνησης του Πλαισίου
Ένας συμπληρωματικός πόρος που παρέχει σύντομη, εφαρμόσιμη καθοδήγηση για συγκεκριμένα θέματα που σχετίζονται με το Πλαίσιο.

Υποκατηγορία του Πλαισίου
Μια ομάδα πιο συγκεκριμένων αποτελεσμάτων σχετικά με τεχνικές και διαχειριστικές δραστηριότητες κυβερνοασφάλειας, που συνθέτουν μια Κατηγορία του Πλαισίου.

Προφίλ Στόχος του Πλαισίου
Ένα μέρος ενός Οργανωτικού Προφίλ που προσδιορίζει τα επιθυμητά αποτελέσματα του Πυρήνα που έχει επιλέξει και ιεραρχήσει ένας οργανισμός για την επίτευξη των στόχων του ως προς τη διαχείριση κινδύνων κυβερνοασφάλειας.

Βαθμίδα του Πλαισίου
Ένας χαρακτηρισμός της αυστηρότητας των πρακτικών διακυβέρνησης και διαχείρισης κινδύνων κυβερνοασφάλειας ενός οργανισμού. Υπάρχουν τέσσερις Βαθμίδες: Μερικής Υλοποίησης (Βαθμίδα 1), Επίγνωσης Κινδύνου (Βαθμίδα 2), Επαναλαμβανόμενων Πρακτικών (Βαθμίδα 3) και Προσαρμοζόμενων Πρακτικών (Βαθμίδα 4).

Στο παρόν έγγραφο αναφέρονται είδη ορισμένου εμπορικού εξοπλισμού, όργανα, λογισμικό ή υλικά, εμπορικά ή μη εμπορικά, προκειμένου να προσδιοριστεί επαρκώς η πειραματική διαδικασία. Η αναφορά αυτή δεν υποδηλώνει σύσταση ή έγκριση οποιουδήποτε προϊόντος ή υπηρεσίας από το NIST, ούτε υποδηλώνει ότι τα υλικά ή ο εξοπλισμός που προσδιορίζονται είναι απαραίτητα τα καλύτερα διαθέσιμα για το σκοπό αυτό.

Σειρά Τεχνικών Πολιτικών του NIST
Δηλώσεις περί Πνευματικών Δικαιωμάτων, Χρήσης και Αδειοδότησης
Συντακτικό Αναγνωριστικού Δημοσίευσης της Τεχνικής Σειράς NIST

Πώς να παραθέσετε αυτή τη Δημοσίευση της Τεχνικής Σειράς NIST:
National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 gre. https://doi.org/10.6028/NIST.CSWP.29.gre

Στοιχεία επικοινωνίας
cyberframework@nist.gov

National Institute of Standards and Technology
Υπόψη: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000, U.S.A.

Όλα τα σχόλια υπόκεινται σε δημοσιοποίηση σύμφωνα με τον Νόμο περί Ελευθερίας των Πληροφοριών (Freedom of Information Act, FOIA) των Η.Π.Α.

Μεταφράστηκε τον Οκτώβριο του 2024 από μέλη του Ελληνικού παραρτήματος του (ISC)2 / Translated on October 2024 by members of the (ISC)2 Hellenic Chapter:

- Maria BREMPOU,
- Ioanna DIMA,
- Dimitris GEORGIOU,
- Yiannis PAVLOSOGLOU,
- Spiros PITIKARIS,
- Panagiotis SOULOS.