Πλαίσιο για τη Βελτίωση της Κυβερνοασφάλειας των Κρίσιμων Υποδομών

Έκδοση 1.1

Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST), Η.Π.Α.

16 Απριλίου 2018

https://doi.org/10.6028/NIST.CSWP.6.gre

Μεταφράστηκε από μέλη του Ελληνικού παραρτήματος του (ISC)^2 / Translated by members of the (ISC)^2 Hellenic Chapter:

Δημήτρης ΓΕΩΡΓΙΟΥ
Ιωάννα ΔΗΜΑ
Γιάννης ΠΑΥΛΟΣΟΓΛΟΥ
Σπύρος ΠΙΤΙΚΑΡΗΣ
Παναγιώτης ΣΟΥΛΟΣ

Η έκδοση 1.1 του Πλαισίου Κυβερνοασφάλειας στην ελληνική γλώσσα μεταφράστηκε εθελοντικά από τα μέλη του Ελληνικού παραρτήματος του (ISC)^2.

Η επίσημη αγγλόφωνη έκδοση αυτής της έκδοσης διατίθεται δωρεάν από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST): https://doi.org/10.6028/NIST.CSWP.6

Translated by Ioanna Dima, Dimitris Georgiou, Yiannis Pavlosoglou, Spiros Pitikaris, and Panagiotis Soulus. Reviewed by TaikaTranslations LLC. Official U.S. Government Translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.6

Σημείωση προς τους αναγνώστες σχετικά με τη νέα έκδοση

Η Έκδοση 1.1 αυτού του Πλαισίου Κυβερνοασφάλειας βελτιώνει, αποσαφηνίζει και ενισχύει την Έκδοση 1.0 που δημοσιεύτηκε τον Φεβρουάριο του 2014. Στην Έκδοση αυτή, ενσωματώνονται σχόλια που ελήφθησαν στα δύο προσχέδια της Έκδοσης 1.1.

Η Έκδοση 1.1 σχεδιάστηκε για να υλοποιηθεί τόσο από νέους όσο και από υφιστάμενους χρήστες του Πλαισίου. Οι υφιστάμενοι χρήστες θα πρέπει να είναι σε θέση να εφαρμόσουν την Έκδοση 1.1 με ελάχιστη ή καθόλου δυσκολία, καθώς ρητός στόχος της παρούσας έκδοσης ήταν η συμβατότητα με την Εκδοση 1.0.

Ο παρακάτω πίνακας συνοψίζει τις αλλαγές που έγιναν μεταξύ της Έκδοσης 1.0 και της Έκδοσης 1.1.

Πίνακας NTR-1 - Σύνοψη αλλαγών μεταξύ της Έκδοσης 1.0 και της Έκδοσης 1.1.

Ενημέρωση	Περιγραφή της Ενημέρωσης
Διευκρινίστηκε ότι όροι όπως "συμμόρφωση" μπορεί να προκαλέσουν σύγχυση και να σημαίνουν κάτι πολύ διαφορετικό για διάφορους ενδιαφερόμενους του Πλαισίου	Αποσαφηνίστηκε η χρησιμότητα του Πλαισίου ως δομή και γλώσσα που οργανώνει και εκφράζει τη συμμόρφωση με τις ξεχωριστές απαιτήσεις κυβερνοασφάλειας κάθε οργανισμού. Ωστόσο, οι διάφοροι τρόποι με τους οποίους μπορεί να χρησιμοποιηθεί το Πλαίσιο από έναν οργανισμό, σημαίνει ότι φράσεις όπως «συμμόρφωση με το Πλαίσιο» μπορεί να προκαλέσουν σύγχυση.
Προστέθηκε μια νέα ενότητα για την αυτοαξιολόγηση	Προστέθηκε η Ενότητα 4.0 *Αυτοαξιολόγηση Κινδύνου Κυβερνοασφάλειας με βάση το Πλαίσιο,* η οποία εξηγεί πώς οι οργανισμοί μπορούν να αξιοποιήσουν το Πλαίσιο για να κατανοήσουν και να αξιολογήσουν τον κίνδυνο κυβερνοασφάλειάς τους, συμπεριλαμβανομένων και ποσοτικών μετρήσεων.
Διευρύνθηκε η εξήγηση της χρήσης του Πλαισίου για σκοπούς που αφορούν στη Διαχείριση Κινδύνων της Εφοδιαστικής Αλυσίδας στον Κυβερνοχώρο	Η Ενότητα 3.3 *Κοινοποίηση των Απαιτήσεων Κυβερνοασφάλειας στα Ενδιαφερόμενα Μέρη*, όπως επεκτάθηκε, βοηθά τους χρήστες να κατανοήσουν καλύτερα τη Διαχείριση Κινδύνων Εφοδιαστικής Αλυσίδας στον Κυβερνοχώρο (SCRM – Cyber Supply Chain Risk Management), ενώ η νέα Ενότητα 3.4 *Αποφάσεις Αγοράς* επισημαίνει τη χρήση του Πλαισίου για την κατανόηση του κινδύνου που σχετίζεται με τυποποιημένα εμπορικά προϊόντα και υπηρεσίες. Πρόσθετα κριτήρια για τη Διαχείριση των Κινδύνων της Εφοδιαστικής Αλυσίδας στον Κυβερνοχώρο (SCRM) προστέθηκαν στις Βαθμίδες Υλοποίησης. Τέλος, προστέθηκε στο Πλαίσιο η Κατηγορία Διαχείρισης Κινδύνων Εφοδιαστικής Αλυσίδας, η οποία περιλαμβάνει πολλαπλές Υποκατηγορίες.
Πραγματοποιήθηκαν βελτιώσεις για την καλύτερη απόδοση της αυθεντικοποίησης, της εξουσιοδότησης και της απόδειξης ταυτότητας	Το περιεχόμενο της Κατηγορίας για τον Έλεγχο Πρόσβασης έχει βελτιωθεί ώστε να περιγράφεται καλύτερα η αυθεντικοποίηση, η εξουσιοδότηση και η απόδειξη ταυτότητας. Αυτό περιλαμβάνει την προσθήκη μιας ξεχωριστής Υποκατηγορίας για την Αυθεντικοποίηση και την προσθήκη μιας ξεχωριστής Υποκατηγορίας για την Απόδειξη Ταυτότητας. Επίσης, η Κατηγορία μετονομάστηκε σε Διαχείριση Ταυτότητας και Έλεγχος Πρόσβασης (PR.AC – Identity Management and Access Control), για να αντιπροσωπεύει καλύτερα το εύρος της Κατηγορίας και των αντίστοιχων Υποκατηγοριών.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Επεξηγήθηκε καλύτερα η σχέση μεταξύ των Βαθμίδων Υλοποίησης και των Προφίλ	Προστέθηκε περιεχόμενο στην Ενότητα 3.2 *Δημιουργία ή Βελτίωση ενός Προγράμματος Κυβερνοασφάλειας* σχετικά με τη χρήση των Βαθμίδων του Πλαισίου στην υλοποίηση του Πλαισίου. Προστέθηκε περιεχόμενο στις Βαθμίδες του Πλαισίου, για να αποδοθεί πώς τα προγράμματα διαχείρισης κινδύνου των οργανισμών ενσωματώνουν τις προτάσεις του Πλαισίου. Επίσης, βελτιώθηκαν οι έννοιες των Βαθμίδων του Πλαισίου. Ενημερώθηκε το Σχήμα 2.0, ώστε να περιλαμβάνει ενέργειες από τις Βαθμίδες του Πλαισίου.
Συμπεριλήφθηκε η Συντονισμένη Γνωστοποίηση Ευπαθειών	Προστέθηκε μια Υποκατηγορία που σχετίζεται με τον κύκλο ζωής των διαδικασιών γνωστοποίησης ευπαθειών.

Όπως και με την Έκδοση 1.0, οι χρήστες της Έκδοσης 1.1 ενθαρρύνονται να προσαρμόσουν το Πλαίσιο για να μεγιστοποιήσουν την επιμέρους αξία στον εκάστοτε οργανισμό.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Ευχαριστίες

Αυτή η δημοσίευση είναι το αποτέλεσμα μιας συνεχιζόμενης συλλογικής προσπάθειας μεταξύ των επιχειρήσεων του κλάδου, του ακαδημαϊκού κόσμου και της κυβέρνησης των Η.Π.Α.. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Η.Π.Α. (NIST) ξεκίνησε το έργο συγκαλώντας οργανισμούς και άτομα από τον ιδιωτικό και τον δημόσιο τομέα το 2013. Αυτό το *Πλαίσιο για τη Βελτίωση της Κυβερνοασφάλειας των Κρίσιμων Υποδομών,* που δημοσιεύτηκε το 2014 και αναθεωρήθηκε το 2017 και το 2018, βασίστηκε σε οκτώ δημόσιες συναντήσεις εργασίας, πολλαπλά Αιτήματα για Σχόλια ή Πληροφορίες (RFC/RFI), και χιλιάδες άμεσες αλληλεπιδράσεις με ενδιαφερόμενα μέρη από όλους τους επαγγελματικούς κλάδους των Ηνωμένων Πολιτειών, καθώς και με εκπροσώπους πολλώνεπαγγελματικών κλάδων από όλο τον κόσμο.

Το έναυσμα για την επικαιροποίηση της Έκδοσης 1.0 και οι αλλαγές που εμφανίζονται στην Έκδοση 1.1 βασίστηκαν σε:

- Ανατροφοδότηση και συχνές ερωτήσεις προς το NIST μετά την κυκλοφορία της έκδοσης 1.0 του Πλαισίου.
- 105 απαντήσεις στο Αίτημα για Πληροφορίες (RFI) του Δεκεμβρίου 2015, *Απόψεις σχετικά με το Πλαίσιο για τη Βελτίωση της Κυβερνοασφάλειας των Κρίσιμων Υποδομών*
- Πάνω από 85 σχόλια για το προτεινόμενο δεύτερο προσχέδιο της Έκδοσης 1.1 που τέθηκε υπό σχολιασμό στις 5 Δεκεμβρίου 2017,
- Πάνω από 120 σχόλια για το προτεινόμενο πρώτο προσχέδιο της Έκδοσης 1.1 που τέθηκε υπό σχολιασμό στις 10 Ιανουαρίου 2017 και
- Προτάσεις από περισσότερους από 1.200 συμμετέχοντες στις συναντήσεις εργασίας που πραγματοποιήθηκαν το 2016 και το 2017 σχετικά με το Πλαίσιο.

Επιπλέον, το NIST εξέδωσε προηγουμένως την έκδοση 1.0 του Πλαισίου Κυβερνοασφάλειας με το συνοδευτικό έγγραφο *"Οδικός Χάρτης του NIST για τη βελτίωση της Κυβερνοασφάλειας των Κρίσιμων Υποδομών"*. Αυτός ο Οδικός Χάρτης τόνιζε βασικούς «τομείς βελτίωσης» για περαιτέρω ανάπτυξη, ευθυγράμμιση και συνεργασία. Μέσω των προσπαθειών του ιδιωτικού και του δημόσιου τομέα, ορισμένοι τομείς βελτίωσης έχουν εξελιχθεί αρκετά, ώστε να συμπεριληφθούν στην Έκδοση 1.1 του Πλαισίου.

Το NIST αναγνωρίζει και ευχαριστεί όλους όσους συνέβαλαν σε αυτό το Πλαίσιο.

Σύνοψη

Οι Ηνωμένες Πολιτείες βασίζονται στην αξιόπιστη λειτουργία των κρίσιμων υποδομών. Οι απειλές κυβερνοασφάλειας εκμεταλλεύονται την αυξημένη πολυπλοκότητα και συνδεσιμότητα των συστημάτων κρίσιμων υποδομών, θέτοντας σε κίνδυνο την ασφάλεια του Έθνους, την οικονομία, καθώς και τη δημόσια ασφάλεια και υγεία. Παρόμοια με τους οικονομικούς κινδύνους και τους κινδύνους φήμης, ο κίνδυνος κυβερνοασφάλειας επηρεάζει και τα κέρδη μιας εταιρείας. Μπορεί να αυξήσει το κόστος και να επηρεάσει τα έσοδα. Μπορεί να βλάψει την ικανότητα ενός οργανισμού να καινοτομεί και να αποκτά και να διατηρεί πελάτες. Η Κυβερνοασφάλεια μπορεί να είναι ένα σημαντικό και ενισχυτικό στοιχείο της συνολικής διαχείρισης κινδύνων ενός οργανισμού.

Για την καλύτερη αντιμετώπιση αυτών των κινδύνων, ο νόμος των ΗΠΑ για την Ενίσχυση της Κυβερνοασφάλειας του 2014[1] (CEA – Cybersecurity Enhancement Act) αναβάθμισε τον ρόλο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) ώστε να περιλαμβάνει τον εντοπισμό και την ανάπτυξη πλαισίων κινδύνων κυβερνοασφάλειας για εθελοντική χρήση από ιδιοκτήτες και φορείς λειτουργίας κρίσιμων υποδομών. Μέσω του CEA, το NIST οφείλει να προσδιορίσει «μια ιεραρχημένη, ευέλικτη, επαναλαμβανόμενη, βασισμένη στην απόδοση και οικονομικά αποδοτική προσέγγιση, συμπεριλαμβανομένων μέτρων και ελέγχων ασφάλειας πληροφοριών που μπορούν να υιοθετηθούν εθελοντικά από ιδιοκτήτες και φορείς λειτουργίας κρίσιμων υποδομών για να τους βοηθήσουν να εντοπίσουν, να αξιολογήσουν και να διαχειριστούν κινδύνους κυβερνοασφάλειας». Αυτό επισημοποίησε την προηγούμενη εργασία του NIST για την ανάπτυξη της Έκδοσης 1.0 του Πλαισίου βάσει του Προεδρικού Διατάγματος (Executive Order - EO) 13636 των ΗΠΑ, με τίτλο «Βελτίωση της Κυβερνοασφάλειας των Κρίσιμων Υποδομών» (Φεβρουάριος 2013), και παρείχε καθοδήγηση για τη μελλοντική εξέλιξη του Πλαισίου. Το Πλαίσιο που αναπτύχθηκε βάσει του Προεδρικού Διατάγματος 13636 και συνεχίζει να εξελίσσεται σύμφωνα με τον νόμο CEA, χρησιμοποιεί μια κοινή γλώσσα για την αντιμετώπιση και τη διαχείριση των κινδύνων κυβερνοασφάλειας με οικονομικά αποδοτικό τρόπο, βάσει επιχειρηματικών και οργανωτικών αναγκών, χωρίς να θέτει πρόσθετες κανονιστικές απαιτήσεις στις επιχειρήσεις.

Το Πλαίσιο επικεντρώνεται στη χρήση επιχειρηματικών κινήτρων δράσης για την καθοδήγηση των δραστηριοτήτων κυβερνοασφάλειας και για την εξέταση των κινδύνων κυβερνοασφάλειας ως μέρος των διαδικασιών διαχείρισης κινδύνων του οργανισμού. Το Πλαίσιο αποτελείται από τρία μέρη: τον Πυρήνα του Πλαισίου, τις Βαθμίδες Υλοποίησης και τα Προφίλ του Πλαισίου. Ο Πυρήνας του Πλαισίου είναι ένα σύνολο δραστηριοτήτων κυβερνοασφάλειας, προτάσεων με στόχο την επίτευξη συγκεκριμένων αποτελεσμάτων και ενημερωτικών αναφορών που είναι κοινά σε όλους τους κλάδους καθώς και στις κρίσιμες υποδομές. Στοιχεία του Πυρήνα παρέχουν λεπτομερή καθοδήγηση για την ανάπτυξη εξατομικευμένων Προφίλ οργανισμών. Μέσω της χρήσης των Προφίλ, το Πλαίσιο θα βοηθήσει έναν οργανισμό να ευθυγραμμίσει και να ιεραρχήσει τις δραστηριότητές του στον τομέα της κυβερνοασφάλειας με τους επιχειρησιακούς στόχους του, τις ανοχές κινδύνου και τους πόρους που διαθέτει. Οι Βαθμίδες παρέχουν στους οργανισμούς έναν μηχανισμό που τους επιτρέπει να κατανοούν τα χαρακτηριστικά της προσέγγισής τους στη διαχείριση του κινδύνου κυβερνοασφάλειας, κάτι που θα βοηθήσει στην ιεράρχηση και την επίτευξη των στόχων κυβερνοασφάλειας.

Το Πλαίσιο αναπτύχθηκε για τη βελτίωση της διαχείρισης κινδύνων κυβερνοασφάλειας σε κρίσιμες

[1] *Βλ.* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) που έγινε νόμος στις 18 Δεκεμβρίου 2014 και βρίσκεται στη διεύθυνση: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

υποδομές, ωστόσο μπορεί να χρησιμοποιηθεί από οργανισμούς σε οποιονδήποτε κλάδο ή κοινότητα. Το Πλαίσιο δίνει τη δυνατότητα στους οργανισμούς – ανεξάρτητα από το μέγεθός τους, τον βαθμό έκθεσης σε κινδύνους κυβερνοασφάλειας ή το πόσο ανεπτυγμένο είναι το επίπεδο κυβερνοασφάλειας του οργανισμού – να εφαρμόζουν τις αρχές και τις βέλτιστες πρακτικές διαχείρισης κινδύνου για τη βελτίωση της ασφάλειας και της ανθεκτικότητας.

Το Πλαίσιο παρέχει μια κοινή οργανωτική δομή για πολλαπλές προσεγγίσεις της κυβερνοασφάλειας, συγκεντρώνοντας πρότυπα, κατευθυντήριες γραμμές και πρακτικές που λειτουργούν αποτελεσματικά σήμερα. Καθώς το Πλαίσιο παραπέμπει σε παγκόσμια αναγνωρισμένα πρότυπα για την κυβερνοασφάλεια, μπορεί να χρησιμεύσει ως πρότυπο για τη διεθνή συνεργασία στην ενίσχυση της κυβερνοασφάλειας σε κρίσιμες υποδομές όπως και σε άλλους κλάδους ή κοινότητες.

Το Πλαίσιο προσφέρει έναν ευέλικτο τρόπο διαχείρισης των θεμάτων κυβερνοασφάλειας, συμπεριλαμβανομένης της επίδρασης της κυβερνοασφάλειας στις διαστάσεις του φυσικού χώρου, του κυβερνοχώρου και του ανθρώπινου δυναμικού. Μπορεί να εφαρμοστεί σε οργανισμούς που βασίζονται στην τεχνολογία και εστιάζουν σε θέματα κυβερνοασφάλειας που αφορούν είτε στην Τεχνολογία Πληροφορικής (IT – Information Technology), στα Συστήματα Βιομηχανικού Ελέγχου (ICS – Industrial Control Systems), στα Κυβερνο-Φυσικά Συστήματα (CPS – Cyber-Physical Systems) ή γενικότερα σε συνδεδεμένες συσκευές, συμπεριλαμβανομένου του Διαδικτύου των Πραγμάτων (IoT – Internet of Things). Το Πλαίσιο μπορεί να βοηθήσει τους οργανισμούς να διαχειριστούν ζητήματα κυβερνοασφάλειας, καθώς επιδρά στην ιδιωτικότητα των πελατών, των εργαζομένων και άλλων μερών. Επιπλέον, η επίτευξη συγκεκριμένων αποτελεσμάτων όπως αυτά ορίζονται από το Πλαίσιο χρησιμεύουν ως στόχοι για δραστηριότητες ανάπτυξης και εξέλιξης του εργατικού δυναμικού.

Το Πλαίσιο δεν αποτελεί μία ενιαία προσέγγιση για τη διαχείριση κινδύνων κυβερνοασφάλειας σε κρίσιμες υποδομές. Οι οργανισμοί θα συνεχίσουν να έχουν εξατομικευμένους κινδύνους – διαφορετικές απειλές, διαφορετικές ευπάθειες, διαφορετική ανοχή στον κίνδυνο. Θα διαφέρουν επίσης ως προς τον τρόπο προσαρμογής των πρακτικών που περιγράφονται στο Πλαίσιο. Οι οργανισμοί μπορούν να καθορίσουν δραστηριότητες που είναι σημαντικές για την παροχή κρίσιμων υπηρεσιών και μπορούν να δώσουν προτεραιότητα σε κάποιες επενδύσεις ώστε να μεγιστοποιήσουν το αποτέλεσμα των δαπανών τους. Σε τελική ανάλυση, το Πλαίσιο στοχεύει στη μείωση και την καλύτερη διαχείριση των κινδύνων κυβερνοασφάλειας.

Για να υποστηριχτούν οι εξατομικευμένες ανάγκες κυβερνοασφάλειας των οργανισμών, υπάρχει μεγάλη ποικιλία τρόπων χρήσης του Πλαισίου. Η απόφαση σχετικά με τον τρόπο εφαρμογής του επαφίεται στον φορέα υλοποίησης. Για παράδειγμα, ένας οργανισμός μπορεί να επιλέξει να χρησιμοποιήσει τις Βαθμίδες Υλοποίησης του Πλαισίου για να διατυπώσει σχεδιαζόμενες πρακτικές διαχείρισης κινδύνου. Ένας άλλος οργανισμός μπορεί να χρησιμοποιήσει τις πέντε Λειτουργίες του Πλαισίου για να αναλύσει ολόκληρο το χαρτοφυλάκιο διαχείρισης κινδύνου. Αυτή η ανάλυση μπορεί να βασιστεί ή και όχι σε πιο λεπτομερείς συνοδευτικές οδηγίες, όπως π.χ. καταλόγους μέτρων ελέγχων. Μερικές φορές γίνεται συζήτηση για τη «συμμόρφωση» με το Πλαίσιο, και το Πλαίσιο χρησιμεύει ως δομή και γλώσσα για την οργάνωση και έκφραση της συμμόρφωσης με τις απαιτήσεις κυβερνοασφάλειας του ίδιου του οργανισμού. Ωστόσο, η ποικιλία των τρόπων με τους οποίους μπορεί να χρησιμοποιηθεί το Πλαίσιο από έναν οργανισμό σημαίνει ότι φράσεις όπως «συμμόρφωση με το Πλαίσιο» μπορεί να προκαλέσουν σύγχυση και να σημαίνουν κάτι πολύ διαφορετικό για διάφορα ενδιαφερόμενα μέρη.

Το Πλαίσιο είναι ένα ζωντανό έγγραφο και θα συνεχίσει να επικαιροποιείται και να βελτιώνεται καθώς οι εμπλεκόμενοι στον κλάδο θα παρέχουν ανατροφοδότηση σχετικά με την εφαρμογή του. Το NIST θα συνεχίσει να συνεργάζεται με τον ιδιωτικό τομέα και τις κρατικές υπηρεσίες σε όλα τα επίπεδα. Καθώς

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

το Πλαίσιο θα εφαρμόζεται ευρύτερα, όλο και περισσότερα διδάγματα θα ενσωματώνονται σε μελλοντικές εκδόσεις. Έτσι θα διασφαλιστεί ότι το Πλαίσιο θα ανταποκρίνεται στις ανάγκες των ιδιοκτητών και των διαχειριστών κρίσιμων υποδομών σε ένα δυναμικό περιβάλλον γεμάτο νέες προκλήσεις, νέες απειλές, κινδύνους καθώς και λύσεις.

Η διευρυμένη και πιο αποτελεσματική χρήση και ανταλλαγή βέλτιστων πρακτικών αυτού του εθελοντικού Πλαισίου αποτελεί το επόμενο βήμα για τη βελτίωση της κυβερνοασφάλειας των κρίσιμων υποδομών του Έθνους μας – παρέχοντας εξελισσόμενη καθοδήγηση σε μεμονωμένους οργανισμούς, ενισχύοντας παράλληλα τον τρόπο τοποθέτησης ως προς την κυβερνοασφάλεια τόσο των κρίσιμων υποδομών του Έθνους όσο και της ευρύτερης οικονομίας και κοινωνίας.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Πίνακας περιεχομένων

Σημείωση προς τους αναγνώστες σχετικά με τη νέα έκδοση ii
Ευχαριστίες iv
Σύνοψη v
1.0 Εισαγωγή στο Πλαίσιο 1
2.0 Βασικές Αρχές Πλαισίου 6
3.0 Πώς να Χρησιμοποιήσετε το Πλαίσιο 13
4.0 Αυτοαξιολόγηση Κινδύνων Κυβερνοασφάλειας μέσω του Πλαισίου 21
Παράρτημα Α: Πυρήνας του Πλαισίου 23
Παράρτημα Β: Γλωσσάριο 42
Παράρτημα Γ: Ακρωνύμια 46

Κατάλογος Σχημάτων

Σχήμα 1: Δομή του Πυρήνα του Πλαισίου 6
Σχήμα 2: Απεικόνιση πληροφοριακών ροών και ροών αποφάσεων εντός ενός οργανισμού 12
Σχήμα 3: Σχέσεις Εφοδιαστικής Αλυσίδας στον Κυβερνοχώρο 17

Κατάλογος Πινάκων

Πίνακας 1: Μοναδικά Αναγνωριστικά Λειτουργιών και Κατηγοριών 24
Πίνακας 2: Ο Πυρήνας του Πλαισίου 25
Πίνακας 3: Γλωσσάριο του Πλαισίου 42

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

1.0 Εισαγωγή στο Πλαίσιο

Οι Ηνωμένες Πολιτείες εξαρτώνται από την αξιόπιστη λειτουργία των κρίσιμων υποδομών τους. Οι απειλές κυβερνοασφάλειας εκμεταλλεύονται την αυξημένη πολυπλοκότητα και συνδεσιμότητα των κρίσιμων συστημάτων υποδομής, θέτοντας σε κίνδυνο την ασφάλεια, την οικονομία, καθώς και τη δημόσια ασφάλεια και υγεία του Έθνους. Παρόμοια με τους οικονομικούς κινδύνους και τους κινδύνους φήμης, ο κίνδυνος κυβερνοασφάλειας επηρεάζει τα κέρδη μιας εταιρείας. Μπορεί να αυξήσει το κόστος και να επηρεάσει τα έσοδα. Μπορεί να βλάψει την ικανότητα ενός οργανισμού να καινοτομεί και να αποκτά και να διατηρεί πελάτες. Η κυβερνοασφάλεια μπορεί να είναι ένα σημαντικό και ενισχυτικό στοιχείο της συνολικής διαχείρισης κινδύνων ενός οργανισμού.

Για να ενισχυθεί η ανθεκτικότητα αυτών των υποδομών, ο νόμος των ΗΠΑ για την Ενίσχυση της Κυβερνοασφάλειας του 2014[2] (CEA – Cybersecurity Enhancement Act) αναβάθμισε τον ρόλο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST) προκειμένου να «διευκολύνει και να υποστηρίξει την ανάπτυξη» πλαισίων κινδύνου κυβερνοασφάλειας. Λόγω του νόμου CEA, το NIST πρέπει να προσδιορίσει «μια προσέγγιση προτεραιοτήτων, ευέλικτη, επαναλαμβανόμενη, βασισμένη στην επίδοση και οικονομικά αποδοτική, η οποία να συμπεριλαμβάνει μέτρα και ελέγχους ασφάλειας πληροφοριών που μπορούν να υιοθετηθούν εθελοντικά από ιδιοκτήτες και φορείς λειτουργίας κρίσιμων υποδομών για να τους βοηθήσει να εντοπίσουν, να αξιολογήσουν και να διαχειριστούν τους κινδύνους κυβερνοασφάλειας». Αυτό επισημοποίησε το προηγούμενο έργο του NIST για την ανάπτυξη της έκδοσης 1.0 του Πλαισίου σύμφωνα με το Προεδρικό Διάταγμα (Executive Order – EO) 13636, με τίτλο «Βελτίωση της Κυβερνοασφάλειας Κρίσιμων Υποδομών», που εκδόθηκε τον Φεβρουάριο του 2013[3], και παρείχε καθοδήγηση για τη μελλοντική εξέλιξη του Πλαισίου.

Ο όρος κρίσιμη υποδομή[4] ορίζεται στον νόμο Patriot Act του 2001[5] των Η.Π.Α. ως «συστήματα και πληροφοριακά αγαθά, είτε φυσικά είτε εικονικά, τέτοιας ζωτικής σημασίας για τις Ηνωμένες Πολιτείες που η ανεπάρκεια ή η καταστροφή τέτοιων συστημάτων και αγαθών θα είχε πολύ σοβαρό αντίκτυπο στην ασφάλεια, την εθνική οικονομική ασφάλεια, την εθνική δημόσια υγεία ή οποιονδήποτε συνδυασμό αυτών των θεμάτων». Λόγω των αυξανόμενων πιέσεων από εξωτερικές και εσωτερικές απειλές, οι οργανισμοί που είναι υπεύθυνοι για κρίσιμες υποδομές πρέπει να έχουν μια συνεπή και επαναλαμβανόμενη προσέγγιση για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων κυβερνοασφάλειας. Αυτή η προσέγγιση είναι απαραίτητη σήμερα ανεξάρτητα από το μέγεθος ενός οργανισμού, την έκθεσή του σε απειλές ή το πόσο ανεπτυγμένο είναι το επίπεδο κυβερνοασφάλειάς του.

Η κοινότητα των κρίσιμων υποδομών περιλαμβάνει ιδιοκτήτες και φορείς λειτουργίας ιδιωτικού και δημόσιου τομέα, καθώς και άλλες οντότητες που έχουν ρόλο στην εξασφάλιση των υποδομών του Έθνους. Τα μέλη κάθε τομέα κρίσιμων υποδομών εκτελούν λειτουργίες που υποστηρίζονται από τις

ευρείες κατηγορίες τεχνολογίας, συμπεριλαμβανομένης της τεχνολογίας πληροφορικής (IT), των συστημάτων βιομηχανικού ελέγχου (ICS), των κυβερνο-φυσικών συστημάτων (CPS) και των συνδεδεμένων συσκευών γενικότερα, συμπεριλαμβανομένου του Διαδικτύου των Πραγμάτων

[2]Βλ. 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) που έγινε νόμος στις 18 Δεκεμβρίου 2014 και βρίσκεται στη διεύθυνση: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Εκτελεστικό διάταγμα αριθ. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, 12 Φεβρουαρίου,2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] Το πρόγραμμα του Υπουργείου Εσωτερικής Ασφάλειας (DHS) για τις κρίσιμες υποδομές παρέχει λίστα των τομέων και κατάλογο των τομέων και των σχετικών κρίσιμων λειτουργιών και αλυσίδων αξίας. http://www.dhs.gov/critical-infrastructure-sectors

[5] Βλέπε 42 U.S.C. § 5195c(e)). Ο αμερικανικός νόμος Patriot Act του 2001 (H.R.3162) έγινε ο νόμος 107-56 στις 26 Οκτωβρίου, 2001 και βρίσκεται στη διεύθυνση: https://www.congress.gov/bill/107th-congress/house-bill/316

(IoT). Αυτή η εξάρτηση από την τεχνολογία, την επικοινωνία και τη διασυνδεσιμότητα έχει αλλάξει και έχει επεκτείνει τις πιθανές ευπάθειες και έχει αυξήσει τον πιθανό κίνδυνο λειτουργίας. Για παράδειγμα, καθώς η τεχνολογία και τα δεδομένα που παράγει και επεξεργάζεται χρησιμοποιούνται όλο και περισσότερο για την παροχή κρίσιμων υπηρεσιών και την υποστήριξη επιχειρησιακών αποφάσεων, θα πρέπει να λαμβάνονται υπόψη οι πιθανές επιπτώσεις ενός περιστατικού κυβερνοασφάλειας σε έναν οργανισμό, στην υγεία και την ασφάλεια των ατόμων, στο περιβάλλον, στις κοινότητες και στην ευρύτερη οικονομία και κοινωνία.

Για τη διαχείριση των κινδύνων κυβερνοασφάλειας, απαιτείται σαφής κατανόηση των επιχειρηματικών κινήτρων του οργανισμού και των ζητημάτων ασφάλειας που σχετίζονται με τη χρήση της τεχνολογίας. Επειδή οι κίνδυνοι, οι προτεραιότητες και τα συστήματα κάθε οργανισμού είναι μοναδικά, τα εργαλεία και οι μέθοδοι που θα χρησιμοποιηθούν για την επίτευξη των αποτελεσμάτων που περιγράφονται από το Πλαίσιο θα διαφέρουν.

Αναγνωρίζοντας τον ρόλο που διαδραματίζει η προστασία της ιδιωτικότητας και των πολιτικών ελευθεριών στην ανάπτυξη του αισθήματος εμπιστοσύνης της κοινωνίας, η μεθοδολογία του Πλαισίου δίνει έμφαση στην προστασία αυτών των δικαιωμάτων κατά τη διεξαγωγή δραστηριοτήτων κυβερνοασφάλειας από οργανισμούς που διαχειρίζονται κρίσιμες υποδομές. Πολλοί οργανισμοί έχουν ήδη διαδικασίες για την εξασφάλιση της ιδιωτικότητας και των πολιτικών ελευθεριών. Η μεθοδολογία έχει σχεδιαστεί για να συμπληρώνει αυτές τις διαδικασίες και να παρέχει καθοδήγηση για τη διευκόλυνση της διαχείρισης κινδύνων ιδιωτικότητας σύμφωνα με την προσέγγιση ενός οργανισμού στη διαχείριση κινδύνων κυβερνοασφάλειας. Η ενσωμάτωση της προστασίας της ιδιωτικότητας και της κυβερνοασφάλειας μπορεί να ωφελήσει τους οργανισμούς αυξάνοντας την εμπιστοσύνη των πελατών, επιτρέποντας πιο τυποποιημένη κοινή χρήση πληροφοριών και απλοποιώντας τις λειτουργίες σε όλα τα νομικά καθεστώτα.

Το Πλαίσιο παραμένει αποτελεσματικό και υποστηρίζει την τεχνική καινοτομία επειδή είναι τεχνολογικά ουδέτερο, ενώ αναφέρεται επίσης σε μια ποικιλία υφιστάμενων προτύπων, κατευθυντήριων γραμμών και πρακτικών που εξελίσσονται με την τεχνολογία. Βασιζόμενοι σε αυτά τα παγκόσμια πρότυπα, κατευθυντήριες γραμμές και πρακτικές τα οποία ο κλάδος αναπτύσσει, διαχειρίζεται και ενημερώνει, τα διαθέσιμα εργαλεία και μέθοδοι για την επίτευξη των αποτελεσμάτων του Πλαισίου θα κλιμακωθούν σε διασυνοριακό επίπεδο, θα αναγνωρίσουν την παγκόσμια φύση των κινδύνων κυβερνοασφάλειας και θα εξελιχθούν με τις τεχνολογικές εξελίξεις και τις επιχειρηματικές απαιτήσεις. Η χρήση υφιστάμενων και αναδυόμενων προτύπων θα επιτρέψει οικονομίες κλίμακας και θα οδηγήσει στην ανάπτυξη αποτελεσματικών προϊόντων, υπηρεσιών και πρακτικών που θα ανταποκρίνονται στις ανάγκες που έχει ήδη προσδιορίσει η αγορά. Ο ανταγωνισμός στην αγορά προωθεί επίσης την ταχύτερη διάδοση αυτών των τεχνολογιών και πρακτικών και προσφέρει πολλά οφέλη στα ενδιαφερόμενα μέρη σε αυτούς τους τομείς.

Με βάση αυτά τα πρότυπα, τις κατευθυντήριες γραμμές και τις πρακτικές, το Πλαίσιο παρέχει μια κοινή ταξινόμηση και μηχανισμό για τους οργανισμούς να:

1) Περιγράψουν την τρέχουσα στάση που τηρούν στα πλαίσια της κυβερνοασφάλειας,

2) Περιγράψουν την κατάσταση-στόχο που έχουν θέσει σχετικά με την κυβερνοασφάλεια,

3) Προσδιορίσουν και ιεραρχήσουν ευκαιρίες βελτίωσης στο πλαίσιο μιας συνεχούς και επαναλαμβανόμενης διαδικασίας,

4) Αξιολογήσουν την πρόοδο προς την κατάσταση-στόχο,

5) Επικοινωνήσουν με όλα τα ενδιαφερόμενα μέρη, εσωτερικά και εξωτερικά, σχετικά με τους

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

κινδύνους κυβερνοασφάλειας.

Το πλαίσιο δεν αποτελεί μία ενιαία προσέγγιση για τη διαχείριση κινδύνων κυβερνοασφάλειας σε κρίσιμες υποδομές. Οι οργανισμοί θα συνεχίσουν να έχουν μοναδικούς κινδύνους - διαφορετικές απειλές, διαφορετικές ευπάθειες, διαφορετικές ανοχές κινδύνου. Επίσης, θα διαφέρουν ως προς τον τρόπο με τον οποίο προσαρμόζονται στις πρακτικές που περιγράφονται στο Πλαίσιο. Οι οργανισμοί μπορούν να καθορίσουν δραστηριότητες που είναι σημαντικές για την παροχή κρίσιμων υπηρεσιών και μπορούν να δώσουν προτεραιότητα στις επενδύσεις για να μεγιστοποιήσουν τον αντίκτυπο κάθε δολαρίου που δαπανάται. Τελικά, το πλαίσιο αποσκοπεί στη μείωση και την καλύτερη διαχείριση των κινδύνων για την ασφάλεια στον κυβερνοχώρο.

Για να ληφθούν υπόψη οι μοναδικές ανάγκες κυβερνοασφάλειας των οργανισμών, υπάρχει μια μεγάλη ποικιλία τρόπων χρήσης του Πλαισίου. Η απόφαση σχετικά με τον τρόπο εφαρμογής του επαφίεται στον οργανισμό που ακολουθεί την υλοποίησή του. Για παράδειγμα, ένας οργανισμός μπορεί να επιλέξει να χρησιμοποιήσει τις Βαθμίδες Υλοποίησης του Πλαισίου για να αρθρώσει τις προβλεπόμενες πρακτικές διαχείρισης κινδύνων. Ένας άλλος οργανισμός μπορεί να χρησιμοποιήσει τις πέντε Λειτουργίες του Πλαισίου για να αναλύσει ολόκληρο το χαρτοφυλάκιό του σχετικά με τη διαχείριση κινδύνων. Αυτή η ανάλυση μπορεί να βασιστεί ή και όχι σε πιο λεπτομερείς συνοδευτικές οδηγίες, όπως καταλόγους στοιχείων ελέγχου. Μερικές φορές υπάρχει συζήτηση σχετικά με τη "συμμόρφωση" με το Πλαίσιο και το Πλαίσιο έχει χρησιμότητα ως δομή και γλώσσα για την οργάνωση και την έκφραση της συμμόρφωσης με τις απαιτήσεις κυβερνοασφάλειας ενός οργανισμού. Ωστόσο, η ποικιλία των τρόπων με τους οποίους το Πλαίσιο μπορεί να χρησιμοποιηθεί από έναν οργανισμό σημαίνει ότι φράσεις όπως "συμμόρφωση με το Πλαίσιο" μπορεί να προκαλέσουν σύγχυση και να σημαίνουν κάτι πολύ διαφορετικό για διάφορους ενδιαφερόμενους.

Το Πλαίσιο συμπληρώνει και δεν αντικαθιστά τη διαδικασία διαχείρισης κινδύνων και το πρόγραμμα κυβερνοασφάλειας ενός οργανισμού. Ο οργανισμός μπορεί να χρησιμοποιήσει τις τρέχουσες διαδικασίες του και να αξιοποιήσει το Πλαίσιο για να εντοπίσει ευκαιρίες για την ενίσχυση και την επικοινωνία της διαχείρισης του κινδύνου κυβερνοασφάλειας, ευθυγραμμιζόμενος παράλληλα με τις πρακτικές του κλάδου. Εναλλακτικά, ένας οργανισμός χωρίς υπάρχον πρόγραμμα ασφάλειας στον κυβερνοχώρο μπορεί να χρησιμοποιήσει το Πλαίσιο ως αναφορά για τη δημιουργία τέτοιου.

Ενώ το Πλαίσιο έχει αναπτυχθεί για τη βελτίωση της διαχείρισης κινδύνων κυβερνοασφάλειας σε κρίσιμες υποδομές, μπορεί να χρησιμοποιηθεί από οργανισμούς σε οποιονδήποτε τομέα της οικονομίας ή της κοινωνίας. Προορίζεται να είναι χρήσιμο σε εταιρείες, κυβερνητικές υπηρεσίες και μη κερδοσκοπικούς οργανισμούς ανεξάρτητα από τον σκοπό στον οποίο εστιάζουν ή το μέγεθός τους. Η κοινή ταξινόμηση προτύπων, κατευθυντήριων γραμμών και πρακτικών που παρέχει επίσης δεν είναι ειδική για κάθε χώρα. Οργανισμοί εκτός των Ηνωμένων Πολιτειών μπορούν επίσης να χρησιμοποιήσουν το Πλαίσιο για να ενισχύσουν τις δικές τους προσπάθειες κυβερνοασφάλειας και το Πλαίσιο μπορεί να συμβάλει στην ανάπτυξη μιας κοινής γλώσσας για τη διεθνή συνεργασία με αντικείμενο την κυβερνοασφάλεια κρίσιμων υποδομών.

1.1 Επισκόπηση του Πλαισίου

Το Πλαίσιο είναι μία προσέγγιση με βάση τον κίνδυνο για τη διαχείριση των κινδύνων κυβερνοασφάλειας και αποτελείται από τρία μέρη: τον Πυρήνα του Πλαισίου, τις Βαθμίδες Υλοποίησης Πλαισίου και τα Προφίλ Πλαισίου. Κάθε στοιχείο του Πλαισίου ενισχύει τη σύνδεση μεταξύ των επιχειρησιακών κινήτρων και των δραστηριοτήτων κυβερνοασφάλειας. Τα στοιχεία αυτά επεξηγούνται παρακάτω.

- Ο *Πυρήνας του Πλαισίου* είναι ένα σύνολο από δραστηριότητες κυβερνοασφάλειας, επιθυμητά

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

αποτελέσματα και εφαρμόσιμες αναφορές που είναι κοινές σε όλους τους τομείς κρίσιμων υποδομών. Ο Πυρήνας παρουσιάζει πρότυπα, κατευθυντήριες γραμμές και πρακτικές του κλάδου με τέτοιο τρόπο που επιτρέπει την επικοινωνία των δραστηριοτήτων κυβερνοασφάλειας και τα αποτελέσματά τους στο σύνολο του οργανισμού, από το επίπεδο διοίκησης έως το επίπεδο υλοποίησης/λειτουργίας. Ο Πυρήνας του Πλαισίου αποτελείται από πέντε ταυτόχρονες και συνεχείς Λειτουργίες – Προσδιορισμός, Προστασία, Εντοπισμός, Ανταπόκριση, Ανάκαμψη. Όταν λαμβάνονται υπόψη όλες μαζί, αυτές οι Λειτουργίες προσφέρουν μία υψηλού επιπέδου, στρατηγική άποψη του κύκλου ζωής της διαχείρισης του κινδύνου κυβερνοασφάλειας ενός οργανισμού. Έπειτα, ο Πυρήνας του Πλαισίου αναγνωρίζει για κάθε Λειτουργία υποκείμενες βασικές Κατηγορίες και Υποκατηγορίες – που είναι διακριτά αποτελέσματα που πρέπει να επιτευχθούν– και τα αντιστοιχεί με παραδειγματικές Πληροφοριακές Αναφορές όπως υπάρχοντα πρότυπα, κατευθυντήριες γραμμές και πρακτικές για κάθε Υποκατηγορία.

- Οι *Βαθμίδες Υλοποίησης Πλαισίου* («Βαθμίδες») παρέχουν το πλαίσιο για το πώς ένας οργανισμός αντιλαμβάνεται τους κινδύνους σχετικά με την κυβερνοασφάλεια και τις διαδικασίες που υπάρχουν για να διαχειριστεί αυτούς τους κινδύνους. Οι Βαθμίδες περιγράφουν τον βαθμό στον οποίο οι πρακτικές διαχείρισης του κινδύνου κυβερνοασφάλειας ενός οργανισμού εμφανίζουν τα χαρακτηριστικά που ορίστηκαν στο Πλαίσιο (π.χ. επίγνωση του κινδύνου και της απειλής, επαναλαμβανόμενες και προσαρμοστικές). Οι Βαθμίδες χαρακτηρίζουν τις πρακτικές ενός οργανισμού σε μία κλίμακα, από Μερική (Βαθμίδα 1) έως Προσαρμοστική (Βαθμίδα 4). Αυτές οι Βαθμίδες αντανακλούν ένα εύρος απαντήσεων από άτυπες αντιδράσεις μέχρι ευέλικτες και ενημερωμένες σχετικά με τον κίνδυνο προσεγγίσεις. Κατά τη διαδικασία επιλογής Βαθμίδας, ο οργανισμός πρέπει να λάβει υπόψη τις τρέχουσες πρακτικές διαχείρισης κινδύνου που εφαρμόζει, το περιβάλλον απειλών, τις νομικές και κανονιστικές απαιτήσεις, επιχειρησιακούς στόχους και οργανωσιακούς περιορισμούς.
- Το *Προφίλ Πλαισίου* («Προφίλ») αναπαριστά τα αποτελέσματα που πρέπει να επιτευχθούν σύμφωνα με τις επιχειρηματικές ανάγκες που ένας οργανισμός έχει επιλέξει από τις Κατηγορίες και Υποκατηγορίες του Πλαισίου. Το Προφίλ μπορεί να χαρακτηριστεί ως την ευθυγράμμιση των προτύπων, κατευθυντήριων γραμμών και πρακτικών με τον Πυρήνα του Πλαισίου για ένα συγκεκριμένο σενάριο υλοποίησης. Τα Προφίλ μπορούν να χρησιμοποιηθούν για να αναγνωριστούν ευκαιρίες βελτίωσης του τρόπου τοποθέτησης (posture) ενός οργανισμού ως προς την κυβερνοασφάλεια συγκρίνοντας ένα «Τρέχον» Προφίλ (την υφιστάμενη κατάσταση) με ένα Προφίλ «Στόχο» (την επιθυμητή κατάσταση). Για να αναπτυχθεί ένα Προφίλ, ο οργανισμός μπορεί να επισκοπήσει όλες τις Κατηγορίες και Υποκατηγορίες και σύμφωνα με τα επιχειρησιακά κίνητρα δράσης και μία αξιολόγηση κινδύνων, να καθορίσει ποιες είναι οι πιο σημαντικές – μπορεί να προσθέτει Κατηγορίες και Υποκατηγορίες όπως απαιτείται για να αντιμετωπίσει τους κινδύνους του οργανισμού. Το Τρέχον Προφίλ μπορεί τότε να χρησιμοποιηθεί για την ιεράρχηση προτεραιοτήτων και τη μέτρηση της προόδου προς το Προφίλ Στόχο, λαμβάνοντας υπόψη κι άλλες επιχειρηματικές ανάγκες συμπεριλαμβανομένων της σχέσης κόστους-αποτελεσματικότητας και της καινοτομίας. Τα Προφίλ μπορούν να χρησιμοποιηθούν για τη διενέργεια αυτοαξιολογήσεων και την επικοινωνία εντός ενός οργανισμού ή μεταξύ οργανισμών.

1.2 Διαχείριση Κινδύνου και το Πλαίσιο Κυβερνοασφάλειας

Η Διαχείριση Κινδύνου είναι η συνεχής διαδικασία αναγνώρισης, αξιολόγησης και ανταπόκρισης στον κίνδυνο. Για να διαχειριστούν τον κίνδυνο, οι οργανισμοί θα πρέπει να κατανοήσουν την πιθανότητα ότι ένα συμβάν θα λάβει χώρα και τις πιθανές επιπτώσεις που θα προκύψουν από αυτό. Με αυτήν την πληροφορία, οι οργανισμοί μπορούν να καθορίσουν το αποδεκτό επίπεδο κινδύνου για να επιτύχουν τους επιχειρησιακούς τους στόχους και μπορούν να το εκφράσουν αυτό ως την ανοχή κινδύνου τους.

Με την κατανόηση της ανοχής κινδύνου, οι οργανισμοί μπορούν να ιεραρχήσουν τις προτεραιότητες των

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

δραστηριοτήτων κυβερνοασφάλειας, γεγονός που θα τους επιτρέπει να αποφασίζουν τεκμηριωμένα για τις δαπάνες κυβερνοασφάλειας. Η υλοποίηση προγραμμάτων διαχείρισης κινδύνου επιτρέπει στους οργανισμούς να ποσοτικοποιούν τις προσαρμογές τους στα προγράμματα κυβερνοασφάλειάς τους και να τις επικοινωνούν. Οι οργανισμοί μπορεί να επιλέξουν να διαχειριστούν τον κίνδυνο με διαφορετικούς τρόπους, συμπεριλαμβανομένων των: μετρίαση του κινδύνου, μεταφορά του κινδύνου, αποφυγή του κινδύνου ή αποδοχή του κινδύνου, ανάλογα με τις πιθανές επιπτώσεις στην παροχή κρίσιμων υπηρεσιών. Το Πλαίσιο χρησιμοποιεί διαδικασίες διαχείρισης κινδύνου για να επιτρέπει στους οργανισμούς να ενημερώνουν και να ιεραρχήσουν τις προτεραιότητες των αποφάσεων σχετικά με την κυβερνοασφάλεια. Υποστηρίζει επαναλαμβανόμενες αξιολογήσεις κινδύνου και επικύρωση των επιχειρηματικών οδηγών για να βοηθήσει τους οργανισμούς να επιλέξουν τις καταστάσεις στόχους για τις διεργασίες κυβερνοασφάλειας που ανταποκρίνονται στα επιθυμητά αποτελέσματα. Επομένως, το Πλαίσιο δίνει στους οργανισμούς την ικανότητα να επιλέγουν δυναμικά και να κατευθύνουν τη βελτίωση στη διαχείριση κινδύνου κυβερνοασφάλειας για τα Πληροφοριακά και Βιομηχανικά περιβάλλοντα.

Το Πλαίσιο είναι προσαρμοστικό ώστε να παρέχει μία ευέλικτη υλοποίηση με βάση τον κίνδυνο η οποία μπορεί να χρησιμοποιηθεί σε ένα ευρύ φάσμα διαδικασιών διαχείρισης κινδύνου κυβερνοασφάλειας. Παραδείγματα διαδικασιών διαχείρισης κινδύνου κυβερνοασφάλειας περιλαμβάνουν το πρότυπο (ISO) 31000:2009[6] του Διεθνούς Οργανισμού Τυποποίησης (ISO), το πρότυπο 27005:2011[7] της Διεθνούς Ηλεκτροτεχνικής Επιτροπής (ISO/IEC), την Ειδική Δημοσίευση (SP) 800-39[8] του NIST και τις κατευθυντήριες γραμμές για τη Διαδικασία Διαχείρισης Κινδύνου Κυβερνοασφάλειας (RMP)[9] του Υποτομέα Ηλεκτρικής Ενέργειας.

1.3 Επισκόπηση Εγγράφου

Το υπόλοιπο αυτού του εγγράφου περιέχει τις παρακάτω ενότητες και παραρτήματα:

- Η Ενότητα 2 περιγράφει τα στοιχεία του Πλαισίου: τον Πυρήνα του Πλαισίου, τα Επίπεδα και τα Προφίλ.
- Η Ενότητα 3 παρουσιάζει παραδείγματα χρήσης του Πλαισίου.
- Η Ενότητα 4 περιγράφει πώς να χρησιμοποιηθεί το Πλαίσιο για αυτοαξιολόγηση και επίδειξη κυβερνοασφάλειας μέσω μετρήσεων.
- Το Παράρτημα Α παρουσιάζει τον Πυρήνα του Πλαισίου σε μορφή πίνακα: Λειτουργίες, Κατηγορίες, Υποκατηγορίες και Πληροφοριακές Αναφορές.
- Το Παράρτημα Β περιέχει ένα λεξικό επιλεγμένων όρων.
- Το Παράρτημα Γ περιέχει λίστα ακρωνύμιων που χρησιμοποιούνται σε αυτό το έγγραφο.

[6] Διεθνής Οργανισμός Τυποποίησης, *Διαχείριση Κινδύνου – Αρχές και κατευθυντήριες γραμμές*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] Διεθνής Οργανισμός Τυποποίησης/Διεθνής Ηλεκτροτεχνική Επιτροπή, Πληροφορική – Τεχνικές ασφάλειας – Διαχείριση κινδύνου ασφάλειας πληροφοριών, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Συλλογική Ομάδα Κρούσης Πρωτοβουλία Μετασχηματισμού, *Διαχείριση Κινδύνου Ασφάλειας Πληροφοριών: Σκοπιά Οργανισμού, Σκοπού και Πληροφοριακού Συστήματος*, NIST Ειδική Δημοσίευση 800-39, Μάρτιος 2011. https://doi.org/10.6028/NIST.SP.800-39

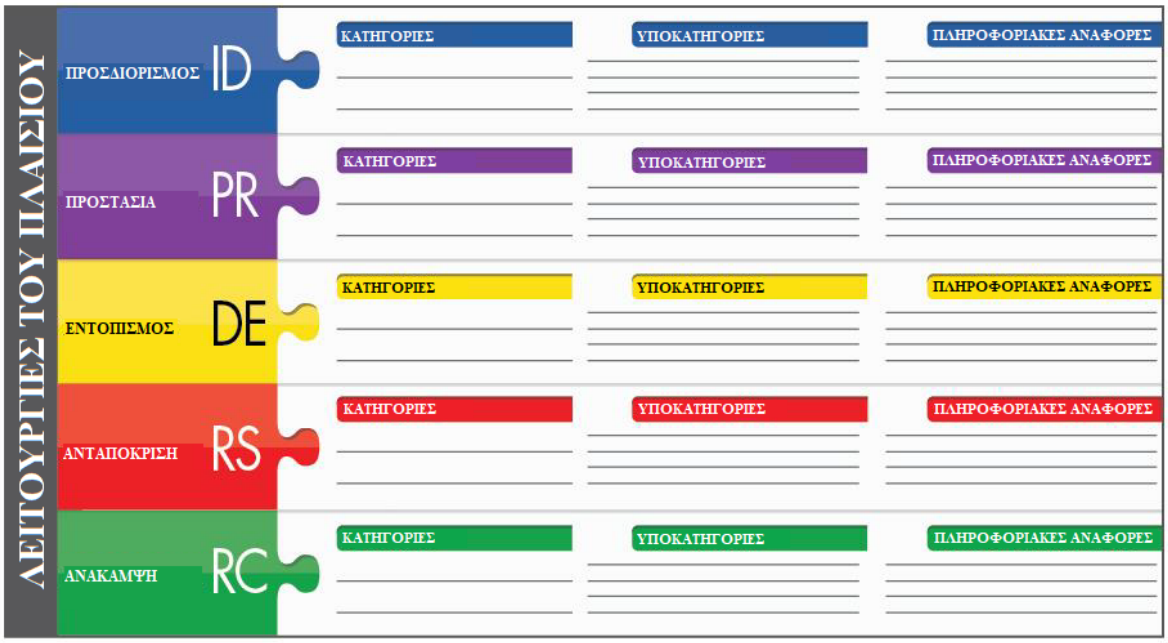
[9] Η. Π. Τμήμα Ενέργειας, Υποτομέας Ηλεκτρισμού Διαδικασία Διαχείρισης Κινδύνου Κυβερνοασφάλειας DOE/OE-0003, Μάιος 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Βασικές Αρχές Πλαισίου

Το Πλαίσιο παρέχει μια κοινή γλώσσα για την κατανόηση, τη διαχείριση και την έκφραση των κινδύνων κυβερνοασφάλειας σε εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη. Μπορεί να χρησιμοποιηθεί για να βοηθήσει στον εντοπισμό και την ιεράρχηση ενεργειών για τη μείωση των κινδύνων κυβερνοασφάλειας και είναι ένα εργαλείο για την ευθυγράμμιση πολιτικών, επιχειρηματικών και τεχνολογικών προσεγγίσεων για τη διαχείριση αυτών των κινδύνων. Επιπρόσθετα, μπορεί να χρησιμοποιηθεί για τη διαχείριση των κινδύνων κυβερνοασφάλειας σε έναν ολόκληρο οργανισμό ή μπορεί να επικεντρωθεί στη διαχείριση κινδύνων που αφορούν στην παροχή κρίσιμων υπηρεσιών εντός ενός οργανισμού. Διαφορετικοί τύποι οντοτήτων – συμπεριλαμβανομένων κλαδικών συντονιστικών δομών που σχετίζονται με κάθε τομέα, ενώσεων και οργανισμών – μπορούν να χρησιμοποιούν το Πλαίσιο για διαφορετικούς σκοπούς, συμπεριλαμβανομένης της δημιουργίας κοινών Προφίλ.

2.1 Πυρήνας του Πλαισίου

Ο Πυρήνας του Πλαισίου παρέχει ένα σύνολο δραστηριοτήτων για την επίτευξη συγκεκριμένων αποτελεσμάτων κυβερνοασφάλειας και παραπέμπει σε παραδείγματα που προσφέρουν καθοδήγηση για την επίτευξη αυτών των αποτελεσμάτων. Ο Πυρήνας δεν αποτελεί μια λίστα ελέγχου ενεργειών που πρέπει να εκτελεστούν. Παρουσιάζει βασικά αποτελέσματα κυβερνοασφάλειας που πρέπει να επιτευχθούν και τα οποία προσδιορίζονται από τα ενδιαφερόμενα μέρη ως χρήσιμα για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Ο Πυρήνας περιλαμβάνει τέσσερα στοιχεία: Λειτουργίες, Κατηγορίες, Υποκατηγορίες και Πληροφοριακές Αναφορές, όπως αυτά απεικονίζονται στο **Σχήμα 1**:



Σχήμα 1: Δομή του Πυρήνα του Πλαισίου

Τα στοιχεία του Πυρήνα του Πλαισίου συλλειτουργούν ως εξής:

- Οι **Λειτουργίες** οργανώνουν βασικές δραστηριότητες κυβερνοασφάλειας στο υψηλότερο επίπεδο. Αυτές οι λειτουργίες είναι ο Προσδιορισμός, η Προστασία, ο Εντοπισμός, η Ανταπόκριση και η Ανάκαμψη. Βοηθούν έναν οργανισμό να εκφράσει τη διαχείριση των κινδύνων κυβερνοασφάλειας οργανώνοντας πληροφορίες, επιτρέποντας αποφάσεις διαχείρισης κινδύνου, αντιμετωπίζοντας απειλές και προχωρώντας σε βελτιώσεις μαθαίνοντας από τις προηγούμενες δραστηριότητες. Επίσης, οι Λειτουργίες ευθυγραμμίζονται με τις υπάρχουσες μεθοδολογίες για τη διαχείριση

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

περιστατικών και αναδεικνύουν τον αντίκτυπο των επενδύσεων κυβερνοασφάλειας. Για παράδειγμα, οι επενδύσεις σε σχεδιασμό και ασκήσεις υποστηρίζουν ενέργειες έγκαιρης ανταπόκρισης και ανάκαμψης, με αποτέλεσμα μειωμένο αντίκτυπο στην παροχή υπηρεσιών.

- Οι **Κατηγορίες** είναι οι υποδιαιρέσεις μιας Λειτουργίας σε ομάδες επιθυμητών αποτελεσμάτων κυβερνοασφάλειας που συνδέονται στενά με προγραμματικές ανάγκες και συγκεκριμένες δραστηριότητες. Παραδείγματα Κατηγοριών περιλαμβάνουν τη "Διαχείριση Πληροφοριακών Αγαθών", τη "Διαχείριση Ταυτότητας και τον Έλεγχο Πρόσβασης" και τις "Διαδικασίες Εντοπισμού".
- Οι **Υποκατηγορίες** διαιρούν περαιτέρω μια Κατηγορία σε συγκεκριμένα αποτελέσματα τεχνικών ή/και διαχειριστικών δραστηριοτήτων που πρέπει να επιτευχθούν. Παρέχουν ένα σύνολο αποτελεσμάτων που, αν και δεν είναι εξαντλητικά, βοηθούν στην υποστήριξη της επίτευξης των αποτελεσμάτων σε κάθε Κατηγορία. Παραδείγματα Υποκατηγοριών περιλαμβάνουν την "Καταλογοποίηση εξωτερικών πληροφοριακών συστημάτων", την "Προστασία δεδομένων-σε-αποθήκευση" και τη "Διερεύνηση των ειδοποιήσεων από τα συστήματα εντοπισμού".
- Οι **Πληροφοριακές Αναφορές** είναι συγκεκριμένες ενότητες προτύπων, κατευθυντήριων γραμμών και πρακτικών κοινών μεταξύ των τομέων υποδομής ζωτικής σημασίας που απεικονίζουν μια μέθοδο για την επίτευξη των αποτελεσμάτων που σχετίζονται με κάθε Υποκατηγορία. Οι Πληροφοριακές Αναφορές που παρουσιάζονται στον Πυρήνα του Πλαισίου είναι επεξηγηματικές και όχι εξαντλητικές. Βασίζονται στις διακλαδικές οδηγίες που αναφέρονται συχνότερα κατά τη διαδικασία ανάπτυξης του Πλαισίου.

Οι πέντε Λειτουργίες του Πυρήνα του Πλαισίου ορίζονται στη συνέχεια. Αυτές οι Λειτουργίες δεν προορίζονται να λειτουργήσουν σειριακά ή να οδηγήσουν σε μια στατική επιθυμητή τελική κατάσταση. Αντίθετα, οι Λειτουργίες θα πρέπει να εκτελούνται ταυτόχρονα και συνεχώς για να διαμορφωθεί μια επιχειρησιακή κουλτούρα που θα αντιμετωπίζει τους δυναμικά εξελισσόμενους κινδύνους κυβερνοασφάλειας. Μία πλήρης λίστα των στοιχείων του Πυρήνα του Πλαισίου παρατίθεται στο Παράρτημα Α.

- **Προσδιορισμός** – Ανάπτυξη μιας οργανωσιακής κατανόησης για τη διαχείριση των κινδύνων κυβερνοασφάλειας σε συστήματα, ανθρώπους, πληροφοριακά αγαθά, δεδομένα και δυνατότητες.

  Οι δραστηριότητες της Λειτουργίας Προσδιορισμού είναι θεμελιώδεις για την αποτελεσματική χρήση του Πλαισίου. Η κατανόηση του επιχειρησιακού πλαισίου, των πόρων που υποστηρίζουν κρίσιμες λειτουργίες και των σχετικών κινδύνων κυβερνοασφάλειας επιτρέπει σε έναν οργανισμό να εστιάσει στις προσπάθειές του και να τις ιεραρχήσει, σύμφωνα με τη στρατηγική διαχείρισης των κινδύνων του και τις επιχειρησιακές του ανάγκες. Παραδείγματα για επιθυμητά αποτελέσματα Κατηγοριών σε αυτή τη Λειτουργία περιλαμβάνουν: Διαχείριση Πληροφοριακών Αγαθών, Επιχειρησιακό Περιβάλλον, Διακυβέρνηση, Αξιολόγηση Κινδύνου και Στρατηγική Διαχείρισης Κινδύνων.

- **Προστασία** – Ανάπτυξη και εφαρμογή κατάλληλων μέτρων για τη διασφάλιση της παροχής κρίσιμων υπηρεσιών.

  Η Λειτουργία Προστασίας υποστηρίζει τη δυνατότητα εξάλειψης ή περιορισμού των επιπτώσεων ενός πιθανού συμβάντος κυβερνοασφάλειας. Παραδείγματα για επιθυμητά αποτελέσματα Κατηγοριών σε αυτή τη Λειτουργία περιλαμβάνουν: Διαχείριση Ταυτότητας και Έλεγχο Πρόσβασης, Ευαισθητοποίηση και Εκπαίδευση, Ασφάλεια Δεδομένων, Διεργασίες και Διαδικασίες Προστασίας Πληροφοριών, Συντήρηση και Τεχνολογίες Προστασίας.

- **Εντοπισμός** – Ανάπτυξη και εφαρμογή κατάλληλων δραστηριοτήτων για τον εντοπισμό της

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

εμφάνισης ενός συμβάντος κυβερνοασφάλειας.

Η Λειτουργία Εντοπισμού επιτρέπει την έγκαιρη ανακάλυψη συμβάντων κυβερνοασφάλειας. Παραδείγματα για επιθυμητά αποτελέσματα Κατηγοριών σε αυτήν τη Λειτουργία περιλαμβάνουν: Ανωμαλίες και Συμβάντα, Συνεχής Παρακολούθηση Ασφάλειας και Διαδικασίες Εντοπισμού.

- **Ανταπόκριση** – Ανάπτυξη και εφαρμογή κατάλληλων δραστηριοτήτων για την ανάληψη δράσης σχετικά με ένα ανιχνευμένο περιστατικό κυβερνοασφάλειας.

  Η Λειτουργία Ανταπόκρισης υποστηρίζει τη δυνατότητα περιορισμού των επιπτώσεων ενός πιθανού περιστατικού κυβερνοασφάλειας. Παραδείγματα για επιθυμητά αποτελέσματα Κατηγοριών σε αυτή τη Λειτουργία περιλαμβάνουν: Σχεδιασμός Ανταπόκρισης, Επικοινωνίες, Ανάλυση, Ελαχιστοποίηση και Βελτιώσεις.

- **Ανάκαμψη** – Ανάπτυξη και εφαρμογή κατάλληλων δραστηριοτήτων για τη διατήρηση σχεδίων ανθεκτικότητας και για την αποκατάσταση τυχόν δυνατοτήτων ή υπηρεσιών που υποβαθμίστηκαν λόγω ενός περιστατικού κυβερνοασφάλειας.

  Η Λειτουργία Ανάκαμψης υποστηρίζει την έγκαιρη επαναφορά σε κανονική λειτουργία για τη μείωση των επιπτώσεων από ένα περιστατικό κυβερνοασφάλειας. Παραδείγματα για επιθυμητά αποτελέσματα Κατηγοριών σε αυτή τη Λειτουργία περιλαμβάνουν: Σχεδιασμός Ανάκαμψης, Βελτιώσεις και Επικοινωνίες.

2.2 Βαθμίδες Υλοποίησης Πλαισίου

Οι Βαθμίδες Υλοποίησης Πλαισίου (“Βαθμίδες”) παρέχουν το πλαίσιο σχετικά με τον τρόπο με τον οποίο ένας οργανισμός βλέπει τον κίνδυνο κυβερνοασφάλειας και τις διαδικασίες που εφαρμόζονται για τη διαχείριση αυτού του κινδύνου. Κυμαινόμενες από το Μερικό (Βαθμίδα 1) έως το Προσαρμοστικό (Βαθμίδα 4), οι Βαθμίδες περιγράφουν έναν αυξανόμενο βαθμό αυστηρότητας και πολυπλοκότητας στις πρακτικές διαχείρισης κινδύνων κυβερνοασφάλειας. Βοηθούν στον προσδιορισμό του βαθμού στον οποίο η διαχείριση κινδύνων κυβερνοασφάλειας επικαιροποιείται με βάση τις επιχειρηματικές ανάγκες και ενσωματώνεται στις συνολικές πρακτικές διαχείρισης κινδύνου ενός οργανισμού. Τα ζητήματα διαχείρισης κινδύνου περιλαμβάνουν πολλές πτυχές της κυβερνοασφάλειας, συμπεριλαμβανομένου του βαθμού στον οποίο οι θεωρήσεις για την ιδιωτικότητα και τις πολιτικές ελευθερίες ενσωματώνονται στη διαχείριση του κινδύνου κυβερνοασφάλειας και στην πιθανή ανταπόκριση στους κινδύνους από έναν οργανισμό.

Η διαδικασία επιλογής Βαθμίδας λαμβάνει υπόψη τις τρέχουσες πρακτικές διαχείρισης κινδύνου ενός οργανισμού, το περιβάλλον απειλών, τις νομικές και ρυθμιστικές απαιτήσεις, τις πρακτικές ανταλλαγής πληροφοριών, τους επιχειρησιακούς στόχους, τις απαιτήσεις κυβερνοασφάλειας της εφοδιαστικής αλυσίδας και τους οργανωσιακούς περιορισμούς. Οι οργανισμοί θα πρέπει να καθορίσουν την επιθυμητή Βαθμίδα, διασφαλίζοντας ότι το επιλεγμένο επίπεδο πληροί τους οργανωσιακούς στόχους, είναι εφικτό να εφαρμοστεί και μειώνει τους κινδύνους κυβερνοασφάλειας σε κρίσιμα πληροφοριακά αγαθά και πόρους σε επίπεδα αποδεκτά από τον οργανισμό. Οι οργανισμοί θα πρέπει να εξετάσουν το ενδεχόμενο να αξιοποιήσουν την εξωτερική καθοδήγηση που μπορεί να ληφθεί από υπηρεσίες και οργανισμούς της Ομοσπονδιακής κυβέρνησης των ΗΠΑ, Κέντρα Διαμοιρασμού και Ανάλυσης Πληροφοριών (Information Sharing and Analysis Centers – ISACs), Οργανισμούς Διαμοιρασμού και Ανάλυσης Πληροφοριών (Information Sharing and Analysis Organizations – ISAOs), υπάρχοντα μοντέλα ωριμότητας ή άλλες πηγές που μπορούν να βοηθήσουν στον προσδιορισμό της επιθυμητής βαθμίδας.

Αν και οι οργανισμοί που προσδιορίζουν ότι βρίσκονται στη Βαθμίδα 1 (Μερικό) ενθαρρύνονται να

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

εξετάσουν το ενδεχόμενο μετάβασης προς τη Βαθμίδα 2 ή μεγαλύτερη, οι Βαθμίδες δεν αντιπροσωπεύουν επίπεδα ωριμότητας. Οι Βαθμίδες προορίζονται να υποστηρίξουν τη λήψη αποφάσεων σχετικά με τον τρόπο διαχείρισης του κινδύνου κυβερνοασφάλειας σε έναν οργανισμό, καθώς και τις διαστάσεις του οργανισμού που έχουν υψηλότερη προτεραιότητα και θα μπορούσαν να λάβουν πρόσθετους πόρους. Η πρόοδος προς υψηλότερες Βαθμίδες ενθαρρύνεται όταν μια ανάλυση κόστους-οφέλους υποδεικνύει μια εφικτή και οικονομικά αποδοτική μείωση των κινδύνων κυβερνοασφάλειας.

Η επιτυχής εφαρμογή του Πλαισίου βασίζεται στην επίτευξη των αποτελεσμάτων που περιγράφονται στο Προφίλ Στόχο του οργανισμού και όχι στον προσδιορισμό Βαθμίδας. Ωστόσο, η επιλογή και ο χαρακτηρισμός Βαθμίδας επηρεάζουν φυσικά και το Προφίλ Πλαισίου. Η πρόταση Βαθμίδας από τους διευθυντές του Επιχειρησιακού/Διαδικαστικού Επιπέδου, όπως αυτή θα εγκριθεί από το Επίπεδο Διοίκησης, θα δώσει τον τόνο για τον τρόπο διαχείρισης της κυβερνοασφάλειας εντός του οργανισμού και θα επηρεάσει την ιεράρχηση των προτεραιοτήτων εντός του Προφίλ Στόχου και τις αξιολογήσεις της προόδου για την αντιμετώπιση των ελλείψεων.

Οι ορισμοί των Βαθμίδων είναι οι εξής:

Βαθμίδα 1: Μερικό

- *Διαδικασία Διαχείρισης Κινδύνου* – Οι οργανωσιακές πρακτικές διαχείρισης κινδύνων κυβερνοασφάλειας δεν είναι επίσημες και η διαχείριση του κινδύνου γίνεται *ad hoc* και μερικές φορές με αντιδραστικό τρόπο. Η ιεράρχηση των δραστηριοτήτων κυβερνοασφάλειας ενδέχεται να μην αντικατοπτρίζει άμεσα τους οργανωσιακούς στόχους κινδύνων, το περιβάλλον απειλών ή τις επιχειρησιακές απαιτήσεις.
- *Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνων* – Υπάρχει περιορισμένη επίγνωση των κινδύνων κυβερνοασφάλειας σε οργανωσιακό επίπεδο. Ο οργανισμός διαχειρίζεται τους κινδύνους κυβερνοασφάλειας σε μη κανονική βάση, κατά περίπτωση, λόγω ποικίλων εμπειριών ή πληροφοριών που αποκτώνται από εξωτερικές πηγές. Ο οργανισμός ενδέχεται να μην διαθέτει διαδικασίες που επιτρέπουν την κοινή χρήση πληροφοριών κυβερνοασφάλειας εντός του οργανισμού.
- *Εξωτερική Συμμετοχή* – Ο οργανισμός δεν κατανοεί το ρόλο του στο ευρύτερο οικοσύστημα όσον αφορά είτε τις εξαρτήσεις είτε τα εξαρτώμενα μέλη του. Ο οργανισμός δεν συνεργάζεται ούτε λαμβάνει πληροφορίες (π.χ. πληροφορίες απειλών, βέλτιστες πρακτικές, τεχνολογίες) από άλλες οντότητες (π.χ. αγοραστές, προμηθευτές, εξαρτημένα άτομα, εξαρτώμενα άτομα, Οργανισμούς Διαμοιρασμού και Ανάλυσης Πληροφοριών (Information Sharing and Analysis Organizations – ISAOs), ερευνητές, κυβερνήσεις), ούτε μοιράζεται πληροφορίες. Ο οργανισμός γενικά δεν γνωρίζει τους κινδύνους κυβερνοασφάλειας της αλυσίδας εφοδιασμού των προϊόντων και των υπηρεσιών που παρέχει και που χρησιμοποιεί.

Βαθμίδα 2: Επίγνωση Κινδύνου

- *Διαδικασία Διαχείρισης 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.
- *Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνων* – Υπάρχει επίγνωση των κινδύνων κυβερνοασφάλειας σε οργανωασιακό επίπεδο, αλλά δεν έχει καθιερωθεί μια προσέγγιση σε επίπεδο οργανισμού για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Οι πληροφορίες για την κυβερνοασφάλεια κοινοποιούνται εντός του οργανισμού σε ανεπίσημη βάση. Η κυβερνοασφάλεια σε οργανωσιακούς στόχους και προγράμματα μπορεί να λαμβάνεται υπόψη σε ορισμένα αλλά όχι

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

σε όλα τα επίπεδα του οργανισμού. Η αξιολόγηση των κινδύνων κυβερνοασφάλειας των οργανωσιακών και εξωτερικών πληροφοριακών αγαθών λαμβάνει χώρα, αλλά συνήθως δεν είναι επαναλαμβανόμενη.

- *Εξωτερική Συμμετοχή* – Γενικά, ο οργανισμός κατανοεί το ρόλο του στο ευρύτερο οικοσύστημα σε σχέση είτε με τις δικές του εξαρτήσεις είτε με τα εξαρτώμενα μέλη του, αλλά όχι και τα δύο. Ο οργανισμός συνεργάζεται με άλλες οντότητες, λαμβάνει ορισμένες πληροφορίες από αυτές και παράγει ορισμένες δικές του πληροφορίες, αλλά ενδέχεται να μην μοιράζεται αυτές τις πληροφορίες με άλλους. Επιπλέον, ο οργανισμός γνωρίζει τους κινδύνους κυβερνοασφάλειας της αλυσίδας εφοδιασμού που σχετίζονται με τα προϊόντα και τις υπηρεσίες που παρέχει και χρησιμοποιεί, αλλά δεν ενεργεί με συνέπεια ή με επίσημο τρόπο σε ό,τι έχει σχέση με αυτούς τους κινδύνους.

Βαθμίδα 3: Επαναλαμβανόμενο

- *Διαδικασία Διαχείρισης Κινδύνου* – Οι πρακτικές διαχείρισης κινδύνου του οργανισμού εγκρίνονται επίσημα και εκφράζονται ως πολιτική. Οι οργανωσιακές πρακτικές κυβερνοασφάλειας επικαιροποιούνται τακτικά με βάση την εφαρμογή των διαδικασιών διαχείρισης κινδύνου στις μεταβαλλόμενες επιχειρησιακές απαιτήσεις και σε ένα μεταβαλλόμενο τοπίο απειλών και τεχνολογίας.
- *Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνων* – Υπάρχει μια προσέγγιση σε επίπεδο οργανισμού για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Οι πολιτικές, οι διεργασίες και οι διαδικασίες που βασίζονται στον κίνδυνο ορίζονται, εφαρμόζονται όπως προβλέπεται και αναθεωρούνται. Υπάρχουν συνεπείς μέθοδοι για την αποτελεσματική ανταπόκριση στους μεταβαλλόμενους κινδύνους. Το προσωπικό διαθέτει τις γνώσεις και τις δεξιότητες για να εκτελεί τους καθορισμένους ρόλους και τις ευθύνες του. Ο οργανισμός παρακολουθεί με συνέπεια και ακρίβεια τους κινδύνους κυβερνοασφάλειας των πληροφοριακών αγαθών του. Ανώτερα στελέχη κυβερνοασφάλειας και ανώτερα στελέχη άλλων τομέων επικοινωνούν τακτικά σχετικά με τους κινδύνους κυβερνοασφάλειας. Τα ανώτερα στελέχη διασφαλίζουν ότι λαμβάνεται υπόψη η κυβερνοασφάλεια σε όλες τις λειτουργίες του οργανισμού.
- *Εξωτερική Συμμετοχή* – Ο οργανισμός κατανοεί τον ρόλο του, τις εξαρτήσεις του και τα εξαρτώμενα μέλη του εντός του ευρύτερου οικοσυστήματος και μπορεί να συμβάλει στην ευρύτερη κατανόηση των κινδύνων από την κοινότητα. Συνεργάζεται με άλλες οντότητες και λαμβάνει τακτικά πληροφορίες από αυτές, οι οποίες λειτουργούν συμπληρωματικά στις πληροφορίες που δημιουργούνται εσωτερικά και μοιράζεται αυτές τις πληροφορίες με άλλες οντότητες. Ο οργανισμός γνωρίζει τους κινδύνους κυβερνοασφάλειας της αλυσίδας εφοδιασμού που σχετίζονται με τα προϊόντα και τις υπηρεσίες που παρέχει και που χρησιμοποιεί. Επιπρόσθετα, συνήθως ενεργεί επίσημα σε ό,τι έχει σχέση με αυτούς τους κινδύνους, συμπεριλαμβανομένων μηχανισμών όπως γραπτές συμφωνίες για την κοινοποίηση βασικών απαιτήσεων, δομές διακυβέρνησης (π.χ. συμβούλια κινδύνου) και εφαρμογή και παρακολούθηση των πολιτικών.

Βαθμίδα 4: Προσαρμοστικό

- *Διαδικασία Διαχείρισης Κινδύνου* – 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 στις μεταβαλλόμενες απειλές και στο μεταβαλλόμενο τεχνολογικό τοπίο και ανταποκρίνεται έγκαιρα και αποτελεσματικά σε εξελιγμένες και εξελισσόμενες απειλές.
- *Πρόγραμμα Ολοκληρωμένης Διαχείρισης Κινδύνων* – Υπάρχει μια προσέγγιση σε ολόκληρο τον οργανισμό για τη διαχείριση των κινδύνων κυβερνοασφάλειας που χρησιμοποιεί πολιτικές,

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

διεργασίες και διαδικασίες που βασίζονται στον κίνδυνο για την αντιμετώπιση πιθανών συμβάντων κυβερνοασφάλειας. Η σχέση μεταξύ των κινδύνων κυβερνοασφάλειας και των οργανωσιακών στόχων είναι σαφώς κατανοητή και λαμβάνεται υπόψη κατά τη λήψη αποφάσεων. Τα ανώτερα 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 στα πλαίσια της οργανωσιακής ανοχής κινδύνου. Η διαχείριση κινδύνων κυβερνοασφάλειας αποτελεί μέρος της οργανωσιακής κουλτούρας και 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 του κινδύνου.

- *Εξωτερική Συμμετοχή* – Ο οργανισμός κατανοεί τον ρόλο του, τις εξαρτήσεις του και τα εξαρτώμενα μέλη του εντός του ευρύτερου οικοσυστήματος και συμβάλλει στην ευρύτερη κατανόηση των κινδύνων από την κοινότητα. Λαμβάνει, παράγει και επανεξετάζει πληροφορίες με προτεραιότητα, οι οποίες τροφοδοτούν τη συνεχή ανάλυση των κινδύνων της, καθώς το τοπίο των απειλών και της τεχνολογίας εξελίσσεται. Ο οργανισμός μοιράζεται αυτές τις πληροφορίες εσωτερικά και εξωτερικά με άλλους συνεργάτες. Ο οργανισμός χρησιμοποιεί πληροφορίες σε πραγματικό χρόνο ή σχεδόν σε πραγματικό χρόνο για να κατανοεί και να ενεργεί με συνέπεια σε ό,τι έχει σχέση με τους κινδύνους κυβερνοασφάλειας της αλυσίδας εφοδιασμού που σχετίζονται με τα προϊόντα και τις υπηρεσίες που παρέχει και που χρησιμοποιεί. Επιπλέον, επικοινωνεί προληπτικά, χρησιμοποιώντας επίσημους (π.χ. συμφωνίες) και άτυπους μηχανισμούς για την ανάπτυξη και τη διατήρηση ισχυρών σχέσεων με την αλυσίδα εφοδιασμού.

2.3 Προφίλ Πλαισίου

Το Προφίλ του Πλαισίου ("Προφίλ") ευθυγραμμίζει τις Λειτουργίες, τις Κατηγορίες και τις Υποκατηγορίες με τις επιχειρηματικές απαιτήσεις, την ανοχή στον κίνδυνο και τους πόρους του οργανισμού. Το Προφίλ επιτρέπει στους οργανισμούς να δημιουργήσουν έναν οδικό χάρτη για τη μείωση του κινδύνου κυβερνοασφάλειας. Ο οδικός χάρτης ευθυγραμμίζεται αποτελεσματικά με τους στόχους του οργανισμού και του κλάδου στον οποίο δραστηριοποιείται, λαμβάνει υπόψη τις νομικές / κανονιστικές απαιτήσεις καθώς και τις βέλτιστες πρακτικές του κλάδου της κυβερνοασφάλειας και αντικατοπτρίζει τις προτεραιότητες του οργανισμού στη διαχείριση κινδύνων. Πολλοί οργανισμοί, δεδομένης της πολυπλοκότητάς τους, μπορεί να επιλέξουν να έχουν πολλαπλά προφίλ, τα οποία θα ευθυγραμμίζονται με συγκεκριμένα στοιχεία και θα ανταποκρίνονται στις εξατομικευμένες ανάγκες τους.

Τα Προφίλ του Πλαισίου μπορούν να χρησιμοποιηθούν για να περιγράψουν την τρέχουσα κατάσταση ή την επιθυμητή κατάσταση-στόχο συγκεκριμένων δραστηριοτήτων κυβερνοασφάλειας. Το Τρέχον Προφίλ υποδεικνύει τα αποτελέσματα που επιτυγχάνονται στον τομέα της κυβερνοασφάλειας την παρούσα χρονική στιγμή. Το Προφίλ Στόχος υποδεικνύει τα αποτελέσματα που είναι απαραίτητα για την επίτευξη των επιθυμητών στόχων διαχείρισης κινδύνων κυβερνοασφάλειας. Τα Προφίλ υποστηρίζουν τις επιχειρησιακές απαιτήσεις και βοηθούν στην κοινοποίηση των κινδύνων τόσο εντός του ίδιου όσο και μεταξύ διαφορετικών οργανισμών. Το Πλαίσιο, όπως περιγράφεται στο παρόν κείμενο, δεν υποδεικνύει Προφίλ, παρέχοντας μεγαλύτερη ευελιξία στο στάδιο της υλοποίησης.

Η Σύγκριση των Προφίλ (π.χ. το Τρέχον Προφίλ και το Προφίλ Στόχος) μπορεί να αποκαλύψει κενά που πρέπει να αντιμετωπιστούν για την επίτευξη των στόχων διαχείρισης κινδύνων κυβερνοασφάλειας. Ένα σχέδιο δράσης για την αντιμετώπιση αυτών των κενών, συμβάλει στον οδικό χάρτη που περιγράφεται παραπάνω, ώστε να ικανοποιηθούν οι απαιτήσεις μιας δεδομένης Κατηγορίας ή Υποκατηγορίας. Οι

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

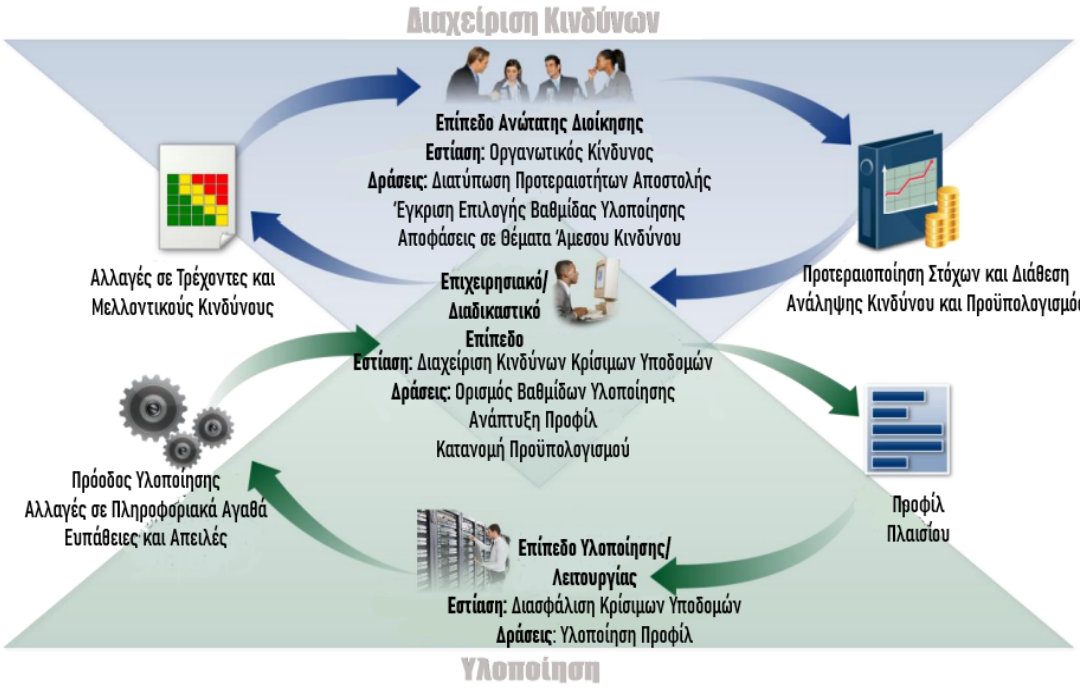
επιχειρηματικές ανάγκες και οι διαδικασίες διαχείρισης κινδύνων του οργανισμού θέτουν τις προτεραιότητες στη διαδικασία μετριασμού αυτών των κενών. Αυτή η ως προς τον κίνδυνο προσέγγιση επιτρέπει σε έναν οργανισμό να εκτιμήσει τους πόρους που απαιτούνται για την επίτευξη των στόχων κυβερνοασφάλειας (π.χ. στελέχωση, χρηματοδότηση) θέτοντας προτεραιότητες με οικονομικά αποδοτικό τρόπο. Τέλος, το Πλαίσιο αποτελεί μία ως προς τον κίνδυνο προσέγγιση όπου η εφαρμοσιμότητα και η εκπλήρωση των μέτρων μίας συγκεκριμένης Υποκατηγορίας υπόκειται στο πεδίο εφαρμογής του Προφίλ του Πλαισίου.

2.4 Συντονισμός της Υλοποίησης του Πλαισίου

Το **Σχήμα 2** περιγράφει μια κοινή ροή πληροφοριών και αποφάσεων στα ακόλουθα επίπεδα εντός ενός οργανισμού:

- Διοίκηση
- Επιχειρησιακό/Διαδικαστικό
- Υλοποίηση/Λειτουργία

Το επίπεδο διοίκησης επικοινωνεί τις προτεραιότητες της αποστολής, τους διαθέσιμους πόρους και τη συνολική ανοχή στον κίνδυνο στο επιχειρησιακό/διαδικαστικό επίπεδο. Το επιχειρησιακό/διαδικαστικό επίπεδο χρησιμοποιεί αυτές τις πληροφορίες ως δεδομένα για τη διαδικασία διαχείρισης κινδύνων και, στη συνέχεια, συνεργάζεται με το επίπεδο υλοποίησης/λειτουργίας για να επικοινωνήσει τις επιχειρηματικές ανάγκες και να δημιουργήσει ένα Προφίλ. Το επίπεδο υλοποίησης/λειτουργίας επικοινωνεί την πρόοδο υλοποίησης του Προφίλ στο επιχειρησιακό/διαδικαστικό επίπεδο. Το επιχειρησιακό/διαδικαστικό επίπεδο χρησιμοποιεί αυτές τις πληροφορίες για τη διενέργεια εκτίμησης επιπτώσεων. Οι επικεφαλής του επιχειρησιακού/διαδικαστικού επιπέδου αναφέρουν τα αποτελέσματα αυτής της εκτίμησης επιπτώσεων αφενός στο επίπεδο διοίκησης για να ενημερωθεί η συνολική διαδικασία διαχείρισης κινδύνων του οργανισμού, και αφετέρου στο επιχειρησιακό/διαδικαστικό επίπεδο για να ενημερωθεί το ίδιο για τον επιχειρηματικό αντίκτυπο.



Σχήμα 2: Απεικόνιση πληροφοριακών ροών και ροών αποφάσεων εντός ενός οργανισμού

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

3.0 Πώς να Χρησιμοποιήσετε το Πλαίσιο

Ένας οργανισμός μπορεί να χρησιμοποιήσει το Πλαίσιο ως βασικό μέρος της συστηματικής διαδικασίας του για τον εντοπισμό, την αξιολόγηση και τη διαχείριση κινδύνων κυβερνοασφάλειας. Το Πλαίσιο δεν έχει σχεδιαστεί για να αντικαταστήσει υπάρχουσες διαδικασίες. Ένας οργανισμός μπορεί να χρησιμοποιήσει την τρέχουσα διαδικασία του υπερθέτοντάς τη στο Πλαίσιο, έτσι ώστε να προσδιορίσει κενά στην τρέχουσα προσέγγιση κινδύνων κυβερνοασφάλειας και να αναπτύξει έναν οδικό χάρτη βελτίωσης. Χρησιμοποιώντας το Πλαίσιο ως εργαλείο διαχείρισης κινδύνων κυβερνοασφάλειας, ένας οργανισμός μπορεί να προσδιορίσει δραστηριότητες που είναι πιο σημαντικές για την παροχή κρίσιμων υπηρεσιών και να δώσει προτεραιότητα σε δαπάνες με σκοπό τη μεγιστοποίηση της απόδοσης της επένδυσης.

Το πλαίσιο έχει σχεδιαστεί ώστε να συμπληρώνει τις υφιστάμενες επιχειρηματικές δραστηριότητες και τις λειτουργίες κυβερνοασφάλειας. Μπορεί να χρησιμεύσει ως θεμέλιο για ένα νέο πρόγραμμα κυβερνοασφάλειας ή ως μηχανισμός για τη βελτίωση ενός υπάρχοντος προγράμματος. Το Πλαίσιο αποτελεί ένα μέσο έκφρασης των απαιτήσεων κυβερνοασφάλειας προς επιχειρηματικούς εταίρους και πελάτες, και μπορεί να βοηθήσει στον εντοπισμό κενών στις πρακτικές κυβερνοασφάλειας ενός οργανισμού. Επίσης, αποτελεί ένα γενικό σύνολο εκτιμήσεων και διαδικασιών για την εξέταση των επιπτώσεων ιδιωτικότητας και πολιτικών ελευθερίων στη λειτουργία ενός προγράμματος κυβερνοασφάλειας.

Το Πλαίσιο μπορεί να εφαρμοστεί σε όλες τις φάσεις του κύκλου ζωής της μελέτης, του σχεδιασμού, της κατασκευής/αγοράς, της υλοποίησης, της λειτουργίας καθώς και της απόσυρσης. Το στάδιο της μελέτης ξεκινά τον κύκλο οποιουδήποτε συστήματος και θέτει τις βάσεις για όλα όσα ακολουθούν. Τα πρωταρχικά ζητήματα κυβερνοασφάλειας θα πρέπει να δηλώνονται και να περιγράφονται όσο το δυνατόν σαφέστερα. Το σχέδιο θα πρέπει να αναγνωρίζει ότι οι παράμετροι και οι απαιτήσεις είναι πιθανό να εξελιχθούν κατά το υπόλοιπο του κύκλου ζωής. Το στάδιο του σχεδιασμού θα πρέπει να λαμβάνει υπόψη τις απαιτήσεις κυβερνοασφάλειας ως μέρος μιας ευρύτερης διαθεματικής διαδικασίας ανάπτυξης συστημάτων.[10] Βασικό ορόσημο του σταδίου σχεδιασμού είναι η επικύρωση των προδιαγραφών κυβερνοασφάλειας του συστήματος έναντι των αναγκών και της θέσης του οργανισμού απέναντι στον κίνδυνο, όπως αυτά αποτυπώνονται σε ένα Προφίλ του Πλαισίου. Τα επιθυμητά αποτελέσματα κυβερνοασφάλειας που ιεραρχούνται σε ένα Προφίλ Στόχο θα πρέπει να ενσωματώνονται όταν α) αναπτύσσεται το σύστημα κατά το στάδιο κατασκευής και β) όταν αγοράζεται ή γίνεται εξωτερική ανάθεση του συστήματος κατά τη φάση προμήθειας. Το ίδιο Προφίλ Στόχος χρησιμεύει ως κατάλογος χαρακτηριστικών κυβερνοασφάλειας του συστήματος, τα οποία θα πρέπει να αξιολογούνται κατά τη θέση του σε λειτουργία για την επαλήθευση όλων των λειτουργιών. Τα επιθυμητά αποτελέσματα κυβερνοασφάλειας που καθορίζονται με τη χρήση του Πλαισίου θα πρέπει στη συνέχεια να χρησιμεύουν ως βάση για τη συνεχή λειτουργία του συστήματος. Αυτό περιλαμβάνει περιστασιακά την επαναξιολόγηση, την αποτύπωση αποτελεσμάτων σε ένα Τρέχον Προφίλ, έτσι ώστε να επαληθευτεί ότι οι απαιτήσεις κυβερνοασφάλειας πληρούνται ακόμα. Συνήθως, ένα πολύπλοκο πλέγμα εξαρτήσεων (π.χ. αντισταθμιστικών και κοινών σημείων ελέγχου) μεταξύ των συστημάτων σημαίνει ότι τα επιθυμητά αποτελέσματα που τεκμηριώνονται στα Προφίλ Στόχων των σχετικών συστημάτων θα πρέπει να εξετάζονται προσεκτικά όταν τα συστήματα αποσύρονται.

Οι ακόλουθες ενότητες παρουσιάζουν τρόπους με τους οποίους διάφοροι οργανισμοί μπορούν να χρησιμοποιήσουν το Πλαίσιο.

[10] Ειδική Έκδοση 800-160 του NIST Τόμος 1, *Μηχανική Ασφάλειας Συστημάτων, Σκέψεις για μια Διεπιστημονική Προσέγγιση στη Μηχανική Αξιόπιστων Ασφαλών Συστημάτων*, Ross και άλλοι, Νοέμβριος 2016 (ενημέρωση στις 21 Μαρτίου, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

3.1 Βασική Επισκόπηση των Πρακτικών Κυβερνοασφάλειας

Το Πλαίσιο μπορεί να χρησιμοποιηθεί για να συγκριθούν οι υφιστάμενες δραστηριότητες κυβερνοασφάλειας ενός οργανισμού με αυτές που περιγράφονται στον Πυρήνα του Πλαισίου. Δημιουργώντας ένα Τρέχον Προφίλ, οι οργανισμοί μπορούν να εξετάσουν τον βαθμό στον οποίο επιτυγχάνουν τα αποτελέσματα που περιγράφονται στις Κατηγορίες και Υποκατηγορίες του Πυρήνα, σε συνάρτηση με τις πέντε κύριες Λειτουργίες: Προσδιορισμός, Προστασία, Εντοπισμός, Ανταπόκριση και Ανάκαμψη. Ένας οργανισμός μπορεί να ανακαλύψει ότι ήδη επιτυγχάνει τα επιθυμητά αποτελέσματα, δηλαδή ότι διαχειρίζεται την κυβερνοασφάλεια με τρόπο ισόμετρο με τον γνωστό για αυτόν κίνδυνο. Εναλλακτικά, ένας οργανισμός μπορεί να προσδιορίσει ότι έχει ευκαιρίες να (ή χρειάζεται να) βελτιωθεί. Ο οργανισμός μπορεί λοιπόν να χρησιμοποιήσει αυτή την πληροφορία για να αναπτύξει ένα πλάνο δράσης ώστε να ενισχύσει τις υφιστάμενες πρακτικές κυβερνοασφάλειας και να μειώσει τον κίνδυνο κυβερνοασφάλειας. Επιπλέον, ένας οργανισμός μπορεί να ανακαλύψει ότι επενδύει υπέρ του δέοντος για να επιτύχει συγκεκριμένα αποτελέσματα. Ο οργανισμός μπορεί να χρησιμοποιήσει αυτή τη πληροφορία για να προτεραιοποιήσει εκ νέου τους πόρους.

Αν και δεν αντικαθιστούν τη διαδικασία διαχείρισης κινδύνου, αυτές οι πέντε κύριες Λειτουργίες θα παρέχουν έναν συνοπτικό τρόπο στα ανώτερα στελέχη και σε άλλους ώστε να κατανοήσουν τις θεμελιώδεις έννοιες του κινδύνου κυβερνοασφάλειας για να μπορούν να αξιολογήσουν πώς ο οργανισμός διαχειρίζεται τους κινδύνους που έχουν αναγνωριστεί και πώς ο οργανισμός τους συμμορφώνεται σε υψηλό επίπεδο με τα υφιστάμενα πρότυπα, τις κατευθυντήριες γραμμές και τις πρακτικές κυβερνοασφάλειας. Το Πλαίσιο μπορεί επίσης να βοηθήσει έναν οργανισμό να απαντήσει σε θεμελιώδεις ερωτήσεις, όπως «Πώς τα πάμε;». Στη συνέχεια, μπορούν να κινηθούν με πιο τεκμηριωμένο τρόπο για να ενισχύσουν τις πρακτικές κυβερνοασφάλειάς τους, όπου και όταν αυτό κρίνεται απαραίτητο.

3.2 Δημιουργία ή Βελτίωση ενός Προγράμματος Κυβερνοασφάλειας

Τα παρακάτω βήματα δείχνουν πώς ένας οργανισμός μπορεί να χρησιμοποιήσει το Πλαίσιο για να δημιουργήσει ένα νέο πρόγραμμα κυβερνοασφάλειας ή να βελτιώσει ένα υφιστάμενο πρόγραμμα. Τα βήματα αυτά θα πρέπει να επαναλαμβάνονται ανάλογα με τις ανάγκες του οργανισμού για τη συνεχή βελτίωση του επιπέδου κυβερνοασφάλειας.

Βήμα 1: Καθορισμός Προτεραιοτήτων και Πεδίο Εφαρμογής. Ο οργανισμός προσδιορίζει τους επιχειρησιακούς στόχους του και τις οργανωσιακές προτεραιότητες υψηλού επιπέδου. Με αυτές τις πληροφορίες, ο οργανισμός λαμβάνει στρατηγικές αποφάσεις σχετικά με τις υλοποιήσεις κυβερνοασφάλειας και καθορίζει το πεδίο εφαρμογής των συστημάτων και αγαθών που υποστηρίζουν την επιλεγμένη επιχειρηματική γραμμή ή διαδικασία. Το Πλαίσιο μπορεί να προσαρμοστεί για να υποστηρίξει τις διάφορες επιχειρηματικές γραμμές ή διαδικασίες εντός ενός οργανισμού, οι οποίες μπορεί να έχουν διαφορετικές επιχειρηματικές ανάγκες καθώς και διαφορετική σχετική ανοχή σε κινδύνους. Η ανοχή κινδύνου μπορεί να αντικατοπτρίζεται σε μια στοχευόμενη Βαθμίδα Υλοποίησης.

Βήμα 2: Προσανατολισμός. Αφού καθοριστεί το πεδίο εφαρμογής του προγράμματος κυβερνοασφάλειας για την επιχειρηματική γραμμή ή τη διαδικασία, ο οργανισμός προσδιορίζει τα σχετικά συστήματα και αγαθά, τις κανονιστικές απαιτήσεις και τη συνολική προσέγγιση κινδύνου. Στη συνέχεια, ο οργανισμός συμβουλεύεται πηγές για τον εντοπισμό απειλών και ευπαθειών που αφορούν τα εν λόγω συστήματα και αγαθά.

Βήμα 3: Δημιουργία Τρέχοντος Προφίλ. Ο οργανισμός αναπτύσσει ένα Τρέχον Προφίλ υποδεικνύοντας ποια αποτελέσματα Κατηγοριών και Υποκατηγοριών από τον Πυρήνα του Πλαισίου επιτυγχάνονται επί του παρόντος. Εάν ένα αποτέλεσμα έχει επιτευχθεί εν μέρει, η σημείωση αυτού του γεγονότος θα βοηθήσει στην υποστήριξη των επόμενων βημάτων παρέχοντας βασικές πληροφορίες.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Βήμα 4: Διεξαγωγή Αξιολόγησης Κινδύνων. Η αξιολόγηση αυτή μπορεί να καθοδηγείται από τη συνολική διαδικασία διαχείρισης κινδύνων του οργανισμού ή από προηγούμενες δραστηριότητες αξιολόγησης κινδύνων. Ο οργανισμός αναλύει το περιβάλλον λειτουργίας προκειμένου να διακρίνει την πιθανότητα ενός συμβάντος κυβερνοασφάλειας και τον αντίκτυπο που θα μπορούσε να έχει το συμβάν στον οργανισμό. Είναι σημαντικό οι οργανισμοί να εντοπίζουν τους αναδυόμενους κινδύνους και να χρησιμοποιούν πληροφορίες σχετικά με τις απειλές στον κυβερνοχώρο από εσωτερικές και εξωτερικές πηγές για να κατανοήσουν καλύτερα την πιθανότητα και τον αντίκτυπο των συμβάντων κυβερνοασφάλειας.

Βήμα 5: Δημιουργία Προφίλ Στόχου. Ο οργανισμός δημιουργεί ένα Προφίλ Στόχο που επικεντρώνεται στην αξιολόγηση των Κατηγοριών και Υποκατηγοριών του Πλαισίου περιγράφοντας τα επιθυμητά αποτελέσματα κυβερνοασφάλειας του οργανισμού. Οι οργανισμοί μπορούν επίσης να αναπτύξουν τις δικές τους πρόσθετες Κατηγορίες και Υποκατηγορίες και να λάβουν υπόψη τους μοναδικούς κινδύνους του κάθε οργανισμού. Ο οργανισμός μπορεί επίσης να λάβει υπόψη τις επιρροές και τις απαιτήσεις των εξωτερικών ενδιαφερόμενων μερών, όπως οι κλαδικές οντότητες, οι πελάτες και οι επιχειρηματικοί εταίροι, κατά τη δημιουργία ενός Προφίλ Στόχου. Το Προφίλ Στόχος θα πρέπει να αντικατοπτρίζει κατάλληλα τα κριτήρια εντός της στοχευόμενης Βαθμίδας Υλοποίησης.

Βήμα 6: Καθορισμός, Ανάλυση και Ιεράρχηση Ελλείψεων. Ο οργανισμός συγκρίνει το Τρέχον Προφίλ και το Προφίλ Στόχο για να προσδιορίσει τις ελλείψεις. Στη συνέχεια, δημιουργεί ένα σχέδιο δράσης με προτεραιότητες για να να αντιμετωπίσει τα κενά - που αντικατοπτρίζει τα επιχειρησιακά κίνητρα δράσης, το κόστος και τα οφέλη, καθώς και τους κινδύνους - για την επίτευξη των αποτελεσμάτων στο Προφίλ Στόχο. Στη συνέχεια, ο οργανισμός καθορίζει τους πόρους, συμπεριλαμβανομένης της χρηματοδότησης και του εργατικού δυναμικού, που απαιτούνται για την αντιμετώπιση των ελλείψεων. Η χρήση των Προφίλ με αυτόν τον τρόπο ενθαρρύνει τον οργανισμό να λαμβάνει τεκμηριωμένες αποφάσεις σχετικά με τις δραστηριότητες κυβερνοασφάλειας , υποστηρίζει τη διαχείριση κινδύνων και επιτρέπει στον οργανισμό να πραγματοποιεί οικονομικά αποδοτικές, στοχευμένες βελτιώσεις.

Βήμα 7: Εφαρμογή Σχεδίου Δράσης. Ο οργανισμός καθορίζει τις ενέργειες τις οποίες πρέπει να πραγματοποιήσει για να αντιμετωπίσει τις ελλείψεις, εάν υπάρχουν, που εντοπίστηκαν στο προηγούμενο βήμα και στη συνέχεια προσαρμόζει τις υφιστάμενες πρακτικές κυβερνοασφάλειας προκειμένου να επιτύχει το Προφίλ Στόχο. Για περαιτέρω καθοδήγηση, το Πλαίσιο προσδιορίζει παραδείγματα Πληροφοριακών Αναφορών σχετικά με τις Κατηγορίες και τις Υποκατηγορίες, αλλά οι οργανισμοί θα πρέπει να καθορίσουν ποια πρότυπα, κατευθυντήριες γραμμές και πρακτικές, συμπεριλαμβανομένων εκείνων που είναι ειδικά για τον τομέα, λειτουργούν καλύτερα για τις δικές τους ανάγκες.

Ένας οργανισμός επαναλαμβάνει τα βήματα όσο χρειάζεται για να αξιολογεί και να βελτιώνει συνεχώς την κυβερνοασφάλειά του. Για παράδειγμα, οι οργανισμοί μπορεί να διαπιστώσουν ότι η συχνότερη επανάληψη του βήματος προσανατολισμού βελτιώνει την ποιότητα των αξιολογήσεων κινδύνου. Επιπλέον, οι οργανισμοί μπορούν να παρακολουθούν την πρόοδο μέσω επαναλαμβανόμενων ενημερώσεων του Τρέχοντος Προφίλ, συγκρίνοντας στη συνέχεια το Τρέχον Προφίλ με το Προφίλ Στόχο. Οι οργανισμοί μπορούν επίσης να χρησιμοποιήσουν αυτή τη διαδικασία για να ευθυγραμμίσουν το πρόγραμμα κυβερνοασφάλειάς τους με την επιθυμητή Βαθμίδα Υλοποίησης του Πλαισίου.

3.3 Κοινοποίηση των Απαιτήσεων Κυβερνοασφάλειας στα Ενδιαφερόμενα Μέρη

Το Πλαίσιο παρέχει μια κοινή γλώσσα για την κοινοποίηση των απαιτήσεων στα αλληλεξαρτώμενα ενδιαφερόμενα μέρη που είναι υπεύθυνα για την παράδοση βασικών προϊόντων και υπηρεσιών σε κρίσιμες υποδομές. Σχετικά παραδείγματα περιλαμβάνουν:

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

- Ένας οργανισμός μπορεί να χρησιμοποιήσει ένα Προφίλ Στόχο για να εκφράσει απαιτήσεις διαχείρισης κινδύνων κυβερνοασφάλειας σε έναν εξωτερικό πάροχο υπηρεσιών (π.χ. έναν πάροχο υπηρεσιών υπολογιστικού νέφους (cloud) στον οποίο εξάγει δεδομένα).
- Ένας οργανισμός μπορεί να εκφράσει την κατάσταση στην οποία βρίσκεται από άποψη κυβερνοασφάλειας μέσω ενός Τρέχοντος Προφίλ για να αναφέρει αποτελέσματα ή να συγκριθεί με τις απαιτήσεις απόκτησης.
- Ένας ιδιοκτήτης/φορέας λειτουργίας (διαχειριστής) κρίσιμης υποδομής, έχοντας προσδιορίσει έναν εξωτερικό συνεργάτη από τον οποίο εξαρτάται αυτή η υποδομή, μπορεί να χρησιμοποιήσει ένα Προφίλ Στόχο για να εκφράσει τις απαιτούμενες Κατηγορίες και Υποκατηγορίες.
- Ένας τομέας κρίσιμων υποδομών μπορεί να δημιουργήσει ένα Προφίλ Στόχο που μπορεί να χρησιμοποιηθεί μεταξύ των συστατικών στοιχείων του ως αρχικό βασικό προφίλ για τη δημιουργία προσαρμοσμένων Προφίλ Στόχων.
- Ένας οργανισμός μπορεί να διαχειριστεί καλύτερα τους κινδύνους κυβερνοασφάλειας μεταξύ των ενδιαφερόμενων μερών, αξιολογώντας τη θέση τους στις κρίσιμες υποδομές και στην ευρύτερη ψηφιακή οικονομία χρησιμοποιώντας τις Βαθμίδες Υλοποίησης.

Η επικοινωνία είναι ιδιαίτερα σημαντική μεταξύ των ενδιαφερόμενων μερών σε όλα τα επίπεδα των εφοδιαστικών αλυσίδων. Οι εφοδιαστικές αλυσίδες είναι πολύπλοκες, παγκοσμίως κατανεμημένες και αποτελούν διασυνδεδεμένα σύνολα πόρων και διαδικασιών μεταξύ πολλαπλών επιπέδων εντός των οργανισμών. Οι εφοδιαστικές αλυσίδες ξεκινούν με τη διάθεση προϊόντων και υπηρεσιών και εκτείνονται στο σχεδιασμό, την ανάπτυξη, την κατασκευή, την επεξεργασία, τη διαχείριση και την παράδοση προϊόντων και υπηρεσιών στον τελικό χρήστη. Δεδομένων αυτών των πολύπλοκων και διασυνδεδεμένων σχέσεων, η διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας (Supply Chain Risk Management-SCRM) είναι μια κρίσιμη οργανωσιακή λειτουργία[11].

Η διαχείριση των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας είναι το σύνολο των δραστηριοτήτων που είναι απαραίτητες για τη διαχείριση των κινδύνων κυβερνοασφάλειας που σχετίζονται με εξωτερικά ενδιαφερόμενα μέρη. Πιο συγκεκριμένα, η διαχείριση των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας συμπεριλαμβάνει τόσο την επίδραση σε ζητήματα κυβερνοασφάλειας που έχει ένας οργανισμός σε εξωτερικά μέρη όσο και την επίδραση που έχουν τα εξωτερικά μέρη σε έναν οργανισμό.

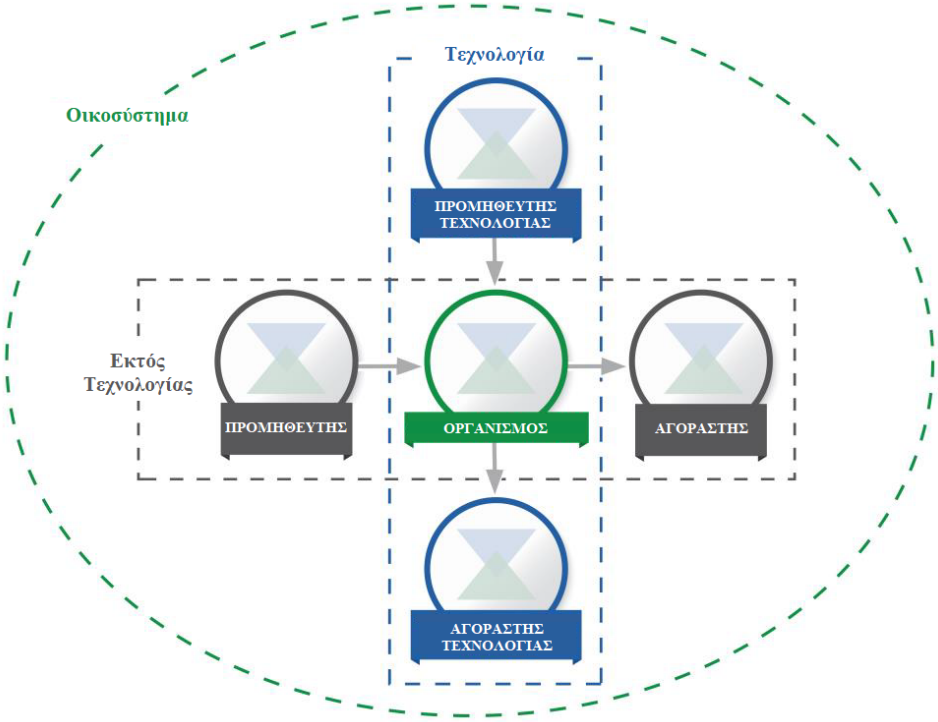
Ένας πρωταρχικός στόχος της διαχείρισης των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας είναι ο εντοπισμός, η αξιολόγηση και η μείωση «προϊόντων και υπηρεσιών που μπορεί να περιέχουν δυνητικά κακόβουλες λειτουργίες, είναι πλαστά ή είναι ευάλωτα λόγω μη βέλτιστων πρακτικών παραγωγής και ανάπτυξης εντός της αλυσίδας εφοδιασμού»[12]. Οι δραστηριότητες της διαχείρισης των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας μπορεί να περιλαμβάνουν:

- Καθορισμό απαιτήσεων κυβερνοασφάλειας για προμηθευτές,
- Θέσπιση απαιτήσεων κυβερνοασφάλειας μέσω επίσημης συμφωνίας (π.χ. συμβάσεις),
- Κοινοποίηση στους προμηθευτές των τρόπων με τους οποίους αυτές οι απαιτήσεις κυβερνοασφάλειας θα επαληθευτούν και θα επικυρωθούν,
- Επαλήθευση ότι οι απαιτήσεις κυβερνοασφάλειας πληρούνται μέσω μιας ποικιλίας μεθοδολογιών αξιολόγησης, και

[11] Η Κοινοποίηση των Απαιτήσεων Κυβερνοασφάλειας στα Ενδιαφερόμενα Μέρη (Ενότητα 3.3) και οι Αποφάσεις Αγοράς (Ενότητα 3.4) αφορούν μόνο δύο χρήσεις του πλαισίου για την διαχείριση των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας (SCRM) και δεν αποσκοπούν στην ολοκληρωμένη αντιμετώπιση του SCRM στον κυβερνοχώρο.
[12] Ειδική Δημοσίευση του NIST 800-161, με τίτλο Πρακτικές Διαχείρισης Κινδύνου Εφοδιαστικής Αλυσίδας για Ομοσπονδιακά Πληροφοριακά Συστήματα και Οργανισμούς, Boyens et al, Απρίλιος 2015, https://doi.org/10.6028/NIST.SP.800-161

- Διοίκηση και διαχείριση των παραπάνω δραστηριοτήτων.

Όπως απεικονίζεται στο Σχήμα 3, η διαχείριση των κινδύνων κυβερνοασφάλειας της εφοδιαστικής αλυσίδας περιλαμβάνει προμηθευτές και αγοραστές τεχνολογικών προϊόντων/υπηρεσιών, καθώς και προμηθευτές και αγοραστές μη τεχνολογικών προϊόντων/υπηρεσιών, όπου τα τεχνολογικά προϊόντα/υπηρεσίες αποτελούνται κατά ελάχιστο από τεχνολογίες πληροφοριών (Information Technology - IT), συστήματα βιομηχανικού ελέγχου (Industrial Control Systems - ICS), κυβερνο-φυσικά συστήματα (Cyber-Physical Systems - CPS) , και συνδεδεμένες συσκευές γενικότερα, συμπεριλαμβανομένου του Διαδικτύου των Πραγμάτων (Internet of Things - IoT). Το Σχήμα 3 απεικονίζει έναν οργανισμό σε μία δεδομένη χρονική στιγμή. Ωστόσο, μέσω της κανονικής πορείας των επιχειρηματικών δραστηριοτήτων, οι περισσότεροι οργανισμοί θα λειτουργούν ταυτόχρονα αφενός ως προμηθευτές και αφετέρου ως αγοραστές σε σχέση με άλλους οργανισμούς ή τελικούς χρήστες.



Σχήμα 3: Σχέσεις Εφοδιαστικής Αλυσίδας στον Κυβερνοχώρο

Τα μέρη που περιγράφονται στο Σχήμα 3 αποτελούν το οικοσύστημα κυβερνοασφάλειας ενός οργανισμού. Αυτές οι σχέσεις υπογραμμίζουν τον κρίσιμο ρόλο που έχει η διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας στον κυβερνοχώρο στην αντιμετώπιση των κινδύνων κυβερνοασφάλειας σε κρίσιμες υποδομές και στην ευρύτερη ψηφιακή οικονομία. Αυτές οι σχέσεις, τα προϊόντα και οι υπηρεσίες που παρέχουν και οι κίνδυνοι που παρουσιάζουν θα πρέπει να εντοπίζονται και να ενσωματώνονται από τους οργανισμούς στις ικανότητες προστασίας από συμβάντα και εντοπισμού συμβάντων, καθώς και στα πρωτόκολλα ανταπόκρισης και ανάκαμψης.

Στο παραπάνω σχήμα, ο "Αγοραστής" αναφέρεται στα άτομα ή στους οργανισμούς που καταναλώνουν ένα δεδομένο προϊόν ή υπηρεσία από έναν οργανισμό, συμπεριλαμβανομένων τόσο κερδοσκοπικών όσο και μη κερδοσκοπικών οργανισμών. Ο "Προμηθευτής" περιλαμβάνει παρόχους προϊόντων και υπηρεσιών που χρησιμοποιούνται για εσωτερικούς σκοπούς ενός οργανισμού (π.χ. υποδομή πληροφορικής) ή ενσωματώνονται στα προϊόντα ή τις υπηρεσίες που παρέχονται στον Αγοραστή. Αυτοί οι όροι ισχύουν τόσο για τεχνολογικά προϊόντα και υπηρεσίες όσο και για μη τεχνολογικά προϊόντα και υπηρεσίες.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Είτε λαμβάνοντας υπόψη μεμονωμένες Υποκατηγορίες του Πυρήνα είτε τις περιεκτικές εκτιμήσεις ενός Προφίλ, το Πλαίσιο προσφέρει στους οργανισμούς και στους συνεργάτες τους μια μέθοδο για να διασφαλιστεί ότι το νέο προϊόν ή υπηρεσία ανταποκρίνεται σε κρίσιμα επιθυμητά αποτελέσματα ασφάλειας. Επιλέγοντας πρώτα επιθυμητά αποτελέσματα που σχετίζονται με το πλαίσιο (π.χ. μετάδοση Προσωπικών Στοιχείων Αναγνώρισης (PII), παράδοση κρίσιμης υπηρεσίας, υπηρεσίες επαλήθευσης δεδομένων, ακεραιότητα προϊόντος ή υπηρεσίας), ο οργανισμός μπορεί μετά να αξιολογήσει τους συνεργάτες του με βάση αυτά τα κριτήρια. Για παράδειγμα, εάν πρόκειται να αγοραστεί ένα σύστημα που θα παρακολουθεί τη Λειτουργική Τεχνολογία (OT) για να ανιχνεύσει ανωμαλίες στις επικοινωνίες δικτύου, η διαθεσιμότητα μπορεί να είναι ένας ιδιαίτερα σημαντικός προς επίτευξη στόχος κυβερνοασφάλειας και θα πρέπει να οδηγεί σε αξιολόγηση του Προμηθευτή Τεχνολογίας σε σχέση με τις ισχύουσες Υποκατηγορίες (π.χ., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Αποφάσεις Αγοράς

Δεδομένου ότι ένα Προφίλ Στόχος του Πλαισίου είναι μια λίστα προτεραιοποιημένων οργανωσιακών απαιτήσεων κυβερνοασφάλειας, τα Προφίλ Στόχοι μπορούν να χρησιμοποιηθούν για την τεκμηρίωση αποφάσεων σχετικά με την αγορά προϊόντων και υπηρεσιών. Αυτή η συναλλαγή διαφέρει από την Κοινοποίηση των Απαιτήσεων Κυβερνοασφάλειας στα Ενδιαφερόμενα Μέρη (όπως αναφέρεται στην Ενότητα 3.3) καθώς ενδέχεται να μην είναι δυνατή η επιβολή ενός συνόλου απαιτήσεων κυβερνοασφάλειας στον προμηθευτή. Ο στόχος πρέπει να είναι η λήψη της καλύτερης αγοραστικής απόφασης μεταξύ πολλών προμηθευτών, δεδομένης μιας προσεκτικά καθορισμένης λίστας απαιτήσεων κυβερνοασφάλειας. Συχνά, αυτό σημαίνει κάποιο βαθμό συμβιβασμού, συγκρίνοντας με το Προφίλ Στόχο πολλαπλά προϊόντα ή υπηρεσίες με γνωστές ελλείψεις.

Μόλις αγοραστεί ένα προϊόν ή μια υπηρεσία, το Προφίλ μπορεί επίσης να χρησιμοποιηθεί για την παρακολούθηση και την αντιμετώπιση του υπολειπόμενου κινδύνου κυβερνοασφάλειας. Για παράδειγμα, εάν η υπηρεσία ή το προϊόν που αγοράστηκε δεν πληρούσε όλους τους στόχους που περιγράφονται στο Προφίλ Στόχο, ο οργανισμός μπορεί να αντιμετωπίσει τον υπολειπόμενο κίνδυνο μέσω άλλων διαχειριστικών ενεργειών. Το Προφίλ παρέχει επίσης στον οργανισμό μια μέθοδο για να αξιολογήσει εάν το προϊόν πληροί τα επιθυμητά αποτελέσματα κυβερνοασφάλειας μέσω περιοδικών μηχανισμών ελέγχου και δοκιμών.

3.5 Προσδιορισμός Ευκαιριών για Νέες ή Αναθεωρημένες Πληροφοριακές Αναφορές

Το Πλαίσιο μπορεί να χρησιμοποιηθεί για τον εντοπισμό ευκαιριών για νέα ή αναθεωρημένα πρότυπα, κατευθυντήριες γραμμές ή πρακτικές όπου πρόσθετες Πληροφοριακές Αναφορές θα βοηθούσαν τους οργανισμούς να αντιμετωπίσουν τις αναδυόμενες ανάγκες. Ένας οργανισμός που εφαρμόζει μια δεδομένη Υποκατηγορία ή αναπτύσσει μια νέα Υποκατηγορία, μπορεί να ανακαλύψει ότι υπάρχουν λίγες Πληροφοριακές Αναφορές, εάν υπάρχουν, για μια σχετική δραστηριότητα. Για την αντιμετώπιση αυτής της ανάγκης, ο οργανισμός μπορεί να συνεργαστεί με ηγέτες τεχνολογίας ή/και φορείς προτύπων για να συντάξει, να αναπτύξει και να συντονίσει πρότυπα, κατευθυντήριες γραμμές ή πρακτικές.

3.6 Μεθοδολογία για την Προστασία της Ιδιωτικότητας και των Πολιτικών Ελευθεριών

Αυτή η ενότητα περιγράφει μια μεθοδολογία για την αντιμετώπιση των επιπτώσεων στην ιδιωτικότητα του ατόμου και στις πολιτικές ελευθερίες που μπορεί να προκύψουν από την κυβερνοασφάλεια. Αυτή η μεθοδολογία προορίζεται να είναι ένα γενικό σύνολο εκτιμήσεων και διεργασιών δεδομένου ότι οι επιπτώσεις στην ιδιωτικότητα και τις πολιτικές ελευθερίες μπορεί να διαφέρουν ανά τομέα ή με την πάροδο του χρόνου και οι οργανισμοί μπορούν να αντιμετωπίσουν αυτές τις εκτιμήσεις και διεργασίες με μια σειρά τεχνικών εφαρμογών. Ωστόσο, όλες οι δραστηριότητες σε ένα πρόγραμμα κυβερνοασφάλειας

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

δεν συνεπάγονται την προστασία της ιδιωτικότητας και των πολιτικών ελευθεριών. Ενδέχεται να χρειαστεί να αναπτυχθούν τεχνικά πρότυπα ιδιωτικότητας, οδηγίες και πρόσθετες βέλτιστες πρακτικές για την υποστήριξη βελτιωμένων τεχνικών υλοποιήσεων.

Η ιδιωτικότητα και η κυβερνοασφάλεια έχουν ισχυρή σύνδεση. Οι δραστηριότητες κυβερνοασφάλειας ενός οργανισμού μπορούν επίσης να δημιουργήσουν κινδύνους για την ιδιωτικότητα και τις πολιτικές ελευθερίες όταν προσωπικές πληροφορίες χρησιμοποιούνται, συλλέγονται, υποβάλλονται σε επεξεργασία, διατηρούνται ή αποκαλύπτονται. Μερικά παραδείγματα περιλαμβάνουν: δραστηριότητες κυβερνοασφάλειας που έχουν ως αποτέλεσμα την υπερβολική συλλογή ή την υπερβολική διατήρηση προσωπικών πληροφοριών, αποκάλυψη ή χρήση προσωπικών πληροφοριών που δεν σχετίζονται με δραστηριότητες κυβερνοασφάλειας, και δραστηριότητες κυβερνοασφάλειας μετριασμού που οδηγούν σε άρνηση παροχής υπηρεσιών ή άλλες παρόμοιες δυνητικά αρνητικές επιπτώσεις, συμπεριλαμβανομένων ορισμένων τύπων εντοπισμού ή παρακολούθησης περιστατικών που μπορεί να εμποδίσουν την ελευθερία της έκφρασης ή του συνεταιρίζεσθαι.

Η κυβέρνηση και οι αντιπρόσωποί της έχουν την ευθύνη να προστατεύουν τις πολιτικές ελευθερίες που προκύπτουν από δραστηριότητες κυβερνοασφάλειας. Όπως αναφέρεται στη μεθοδολογία που ακολουθεί, η κυβέρνηση ή οι αντιπρόσωποί της που κατέχουν ή διαχειρίζονται κρίσιμες υποδομές θα πρέπει να διαθέτουν μια διαδικασία για την υποστήριξη της συμμόρφωσης των δραστηριοτήτων κυβερνοασφάλειας με τους ισχύοντες νόμους, κανονισμούς και συνταγματικές απαιτήσεις περί απορρήτου.

Για την αντιμετώπιση των επιπτώσεων στην ιδιωτικότητα, οι οργανισμοί μπορούν να εξετάσουν πώς το πρόγραμμα κυβερνοασφάλειάς τους μπορεί να ενσωματώσει αρχές απορρήτου όπως: ελαχιστοποίηση δεδομένων κατά τη συλλογή, αποκάλυψη και διατήρηση υλικού προσωπικών πληροφοριών που σχετίζεται με ένα περιστατικό κυβερνοασφάλειας, χρήση περιορισμών εκτός των δραστηριοτήτων κυβερνοασφάλειας σε οποιεσδήποτε πληροφορίες συλλέγονται ειδικά για δραστηριότητες κυβερνοασφάλειας, διαφάνεια για ορισμένες δραστηριότητες κυβερνοασφάλειας, ατομική συναίνεση και επανόρθωση για δυσμενείς επιπτώσεις που προκύπτουν από τη χρήση προσωπικών πληροφοριών σε δραστηριότητες κυβερνοασφάλειας, ποιότητα, ακεραιότητα και ασφάλεια δεδομένων, λογοδοσία και έλεγχος.

Καθώς οι οργανισμοί αξιολογούν τον Πυρήνα του Πλαισίου σύμφωνα με το Παράρτημα Α, οι ακόλουθες διαδικασίες και δραστηριότητες μπορούν να θεωρηθούν ως μέσο για την αντιμετώπιση των προαναφερόμενων επιπτώσεων στην ιδιωτικότητα και τις πολιτικές ελευθερίες:

Διακυβέρνηση των κινδύνων κυβερνοασφάλειας

- Η αξιολόγηση ενός οργανισμού για τους κινδύνους κυβερνοασφάλειας και τις πιθανές αντιδράσεις στον κίνδυνο λαμβάνει υπόψη τις επιπτώσεις του προγράμματος κυβερνοασφάλειάς του στην ιδιωτικότητα.
- Άτομα με ευθύνες απορρήτου που σχετίζονται με την κυβερνοασφάλεια αναφέρονται στην κατάλληλη διοίκηση και είναι κατάλληλα εκπαιδευμένα.
- Υπάρχει διαδικασία για την υποστήριξη της συμμόρφωσης των δραστηριοτήτων κυβερνοασφάλειας με τους ισχύοντες νόμους, κανονισμούς περί απορρήτου και συνταγματικές απαιτήσεις.
- Υπάρχει διαδικασία αξιολόγησης της εφαρμογής των παραπάνω οργανωσιακών μέτρων και ελέγχων.

Προσεγγίσεις για τον προσδιορισμό, την αυθεντικοποίηση και την εξουσιοδότηση ατόμων για πρόσβαση σε οργανωσιακά πληροφοριακά αγαθά και συστήματα

- Λαμβάνονται μέτρα για τον εντοπισμό και την αντιμετώπιση των επιπτώσεων στην ιδιωτικότητα των

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

μέτρων διαχείρισης ταυτότητας και ελέγχου πρόσβασης στο βαθμό που περιλαμβάνουν συλλογή, αποκάλυψη ή χρήση προσωπικών πληροφοριών.

Μέτρα ευαισθητοποίησης και εκπαίδευσης

- Οι ισχύουσες πληροφορίες από τις πολιτικές ιδιωτικότητας του οργανισμού περιλαμβάνονται στις δραστηριότητες εκπαίδευσης και ευαισθητοποίησης για την κυβερνοασφάλεια του εργατικού δυναμικού.
- Οι πάροχοι υπηρεσιών που σχετίζονται με την κυβερνοασφάλεια στον οργανισμό ενημερώνονται για τις ισχύουσες πολιτικές ιδιωτικότητας του οργανισμού.

Ανίχνευση μη ομαλής δραστηριότητας και παρακολούθηση συστημάτων και πληροφοριακών αγαθών

- Υπάρχει διαδικασία για τη διεξαγωγή επανεξέτασης της ιδιωτικότητας κατά τον εντοπισμό ανώμαλης δραστηριότητας σε έναν οργανισμό και κατά την παρακολούθηση της κυβερνοασφάλειας.

Δραστηριότητες ανταπόκρισης, συμπεριλαμβανομένης της ανταλλαγής πληροφοριών ή άλλων προσπαθειών μετριασμού των κινδύνων

- Υπάρχει διαδικασία για να αξιολογηθεί και να εξεταστεί εάν, πότε, πώς και σε ποιο βαθμό προσωπικές πληροφορίες κοινοποιούνται εκτός του οργανισμού ως μέρος των δραστηριοτήτων κυβερνοασφάλειας που αφορούν σε ανταλλαγή πληροφοριών.
- Υπάρχει διαδικασία για τη διεξαγωγή επανεξέτασης της ιδιωτικότητας κατά τη διάρκεια των προσπαθειών μετριασμού των κινδύνων κυβερνοασφάλειας ενός οργανισμού.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

4.0 Αυτοαξιολόγηση Κινδύνων Κυβερνοασφάλειας μέσω του Πλαισίου

Το Πλαίσιο Κυβερνοασφάλειας έχει σχεδιαστεί για να μειώνει τον κίνδυνο βελτιώνοντας τη διαχείριση των κινδύνων κυβερνοασφάλειας σε σχέση πάντα με τους οργανωτικούς στόχους. Ιδανικά, οι οργανισμοί που χρησιμοποιούν το Πλαίσιο θα είναι σε θέση να μετρήσουν και να αποδώσουν τιμές στον κίνδυνο μαζί με το κόστος και τα οφέλη των μέτρων που λαμβάνουν για τη μείωση του κινδύνου σε αποδεκτά επίπεδα. Όσο καλύτερα ένας οργανισμός είναι σε θέση να μετρήσει τον κίνδυνο, το κόστος και τα οφέλη των στρατηγικών και των προόδων κυβερνοασφάλειας, τόσο πιο ορθολογική, αποτελεσματική και πολύτιμη θα είναι η προσέγγιση και οι επενδύσεις του στην κυβερνοασφάλεια.

Με την πάροδο του χρόνου, η αυτοαξιολόγηση και η μέτρηση αναμένεται να βελτιώσουν τη λήψη αποφάσεων σχετικά με τις επενδυτικές προτεραιότητες. Για παράδειγμα, η μέτρηση - ή τουλάχιστον ο ισχυρός χαρακτηρισμός - πτυχών της κατάστασης και των τάσεων κυβερνοασφάλειας ενός οργανισμού με την πάροδο του χρόνου μπορεί να επιτρέψουν σε αυτόν τον οργανισμό να κατανοήσει και να μεταφέρει σημαντικές πληροφορίες κινδύνου σε εξαρτώμενους υπαλλήλους, προμηθευτές, αγοραστές και άλλα μέρη. Ένας οργανισμός μπορεί να το επιτύχει αυτό εσωτερικά ή αναζητώντας μια αξιολόγηση τρίτου μέρους. Εάν γίνουν σωστά και με εκτίμηση των περιορισμών, αυτές οι μετρήσεις μπορούν να αποτελέσουν τη βάση για ισχυρές σχέσεις εμπιστοσύνης, τόσο εντός όσο και εκτός ενός οργανισμού.

Για να εξετάσει την αποτελεσματικότητα των επενδύσεων, ένας οργανισμός πρέπει πρώτα να έχει σαφή κατανόηση των οργανωτικών του στόχων, της σχέσης μεταξύ αυτών των στόχων και των υποστηρικτικών αποτελεσμάτων ασφάλειας στον κυβερνοχώρο και του τρόπου εφαρμογής και διαχείρισης αυτών των διακριτών αποτελεσμάτων ασφάλειας στον κυβερνοχώρο. Ενώ οι μετρήσεις όλων αυτών των στοιχείων δεν εμπίπτουν στο πεδίο εφαρμογής του Πλαισίου, τα αποτελέσματα του Πυρήνα του Πλαισίου για την ασφάλεια στον κυβερνοχώρο υποστηρίζουν την αυτοαξιολόγηση της επενδυτικής αποτελεσματικότητας και των δραστηριοτήτων κυβερνοασφάλειας με τους ακόλουθους τρόπους:

- Διαλέγοντας πως διαφορετικές λειτουργίες κυβερνοασφάλειας του οργανισμού θα πρέπει να επηρεάζουν την επιλογή των Βαθμίδων Υλοποίησης Στόχων,
- Αξιολογώντας τη προσέγγιση του οργανισμού στη διαχείριση κινδύνων κυβερνοασφάλειας μέσω του προσδιορισμού των Υφιστάμενων Βαθμίδων Εφαρμογής,
- Προσδιορίζοντας τον βαθμό στον οποίο συγκεκριμένα βήματα ασφάλειας στον κυβερνοχώρο επιτυγχάνουν τα επιθυμητά αποτελέσματα μέσω της αξιολόγησης των Τρεχόντων Προφίλ, και
- Μετρώντας τον βαθμό υλοποίησης των καταλόγων ελέγχου ή της τεχνικής καθοδήγησης που αναφέρονται ως ενημερωτικές αναφορές.

Η ανάπτυξη μετρήσεων απόδοσης κυβερνοασφάλειας εξελίσσεται. Οι οργανισμοί θα πρέπει να είναι σκεπτικοί, δημιουργικοί και προσεκτικοί σε σχέση με τους τρόπους με τους οποίους χρησιμοποιούν μετρήσεις με σκοπό να βελτιστοποιήσουν τη χρήση, αποφεύγοντας παράλληλα υποταγές σε τεχνητούς δείκτες της τρέχουσας κατάστασης και στοχεύοντας πάντα στη βελτίωση της διαχείρισης κινδύνων κυβερνοασφάλειας. Οποιαδήποτε κριτική κινδύνου κυβερνοασφάλειας απαιτεί πειθαρχία και θα πρέπει να επανεξετάζεται περιοδικά. Κάθε φορά που χρησιμοποιούνται μετρήσεις ως μέρος της διαδικασίας του Πλαισίου, οι οργανισμοί ενθαρρύνονται να προσδιορίζουν με σαφήνεια και να γνωρίζουν γιατί αυτές οι μετρήσεις είναι σημαντικές και πώς θα συμβάλουν στη συνολική διαχείριση του κινδύνου κυβερνοασφάλειας. Θα πρέπει επίσης να είναι σαφείς σχετικά με τους περιορισμούς των μετρήσεων που χρησιμοποιούνται.

Για παράδειγμα, η παρακολούθηση των μέτρων ασφαλείας και των επιχειρηματικών αποτελεσμάτων μπορεί να παρέχει σημαντικές πληροφορίες σχετικά με τον τρόπο με τον οποίο οι αλλαγές στους

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

λεπτομερείς ελέγχους ασφαλείας επηρεάζουν την ολοκλήρωση των οργανωτικών στόχων. Η επαλήθευση της επίτευξης ορισμένων οργανωτικών στόχων απαιτεί την ανάλυση των δεδομένων μόνο μετά την επίτευξη αυτού του στόχου. Αυτός ο τύπος παρελθοντικού μέτρου είναι πιο απόλυτος. Ωστόσο, είναι συχνά πιο πολύτιμο να προβλεφθεί εάν μπορεί να προκύψει ένας κίνδυνος κυβερνοασφάλειας και τον αντίκτυπο που αυτός μπορεί να έχει, χρησιμοποιώντας ένα μέτρο που θα επέλθει.

Οι οργανισμοί ενθαρρύνονται να καινοτομούν και να προσαρμόζουν τον τρόπο με τον οποίο ενσωματώνουν μετρήσεις στην εφαρμογή του Πλαισίου με πλήρη εκτίμηση της χρησιμότητας και των περιορισμών τους.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Παράρτημα Α: Πυρήνας του Πλαισίου

Αυτό το παράρτημα παρουσιάζει τον Πυρήνα του Πλαισίου: μια λίστα με Λειτουργίες, Κατηγορίες, Υποκατηγορίες και Πληροφοριακές Αναφορές που περιγράφουν συγκεκριμένες δραστηριότητες κυβερνοασφάλειας που είναι κοινές μεταξύ όλων των τομέων που αφορούν σε κρίσιμες υποδομές . Η μορφή παρουσίασης του Πυρήνα του Πλαισίου που έχει επιλεχθεί δεν προτείνει συγκεκριμένη σειρά υλοποίησης ούτε υπονοεί συγκεκριμένο βαθμό σημασίας των Κατηγοριών, Υποκατηγοριών και Πληροφοριακών Αναφορών. Ο Πυρήνας του Πλαισίου που παρουσιάζεται σε αυτό το παράρτημα αντιπροσωπεύει ένα κοινό σύνολο δραστηριοτήτων για τη διαχείριση των κινδύνων κυβερνοασφάλειας. Αν και το Πλαίσιο δεν εξαντλεί όλα τα περιθώρια, μπορεί να επεκταθεί περαιτέρω, επιτρέποντας σε οργανισμούς, τομείς και άλλες οντότητες να χρησιμοποιούν Υποκατηγορίες και Ενημερωτικές Αναφορές που είναι οικονομικά αποδοτικές και αποτελεσματικές και που τους επιτρέπουν να διαχειρίζονται τους κινδύνους κυβερνοασφάλειας που αντιμετωπίζουν. Οι δραστηριότητες μπορούν να επιλεχθούν από τον Πυρήνα του Πλαισίου κατά τη διαδικασία δημιουργίας Προφίλ και επιπλέον Κατηγορίες, Υποκατηγορίες και Ενημερωτικές Αναφορές μπορούν να προστεθούν στο Προφίλ. Η επιλογή αυτών των δραστηριοτήτων κατά τη δημιουργία Προφίλ καθορίζεται από τις διαδικασίες διαχείρισης κινδύνων ενός οργανισμού, τις νομικές/κανονιστικές απαιτήσεις, τους επιχειρησιακούς στόχους και τους οργανωσιακούς περιορισμούς. Οι προσωπικές πληροφορίες θεωρούνται συστατικό των δεδομένων ή των πληροφοριακών αγαθών που αναφέρονται στις Κατηγορίες κατά την αξιολόγηση κινδύνων ασφάλειας και προστασίας.

Ενώ τα επιδιωκόμενα αποτελέσματα που προσδιορίζονται στις Λειτουργίες, τις Κατηγορίες και τις Υποκατηγορίες είναι τα ίδια για τις Τεχνολογίες Πληροφορικής (IT-Information Technology) και για τα Συστήματα Βιομηχανικού Ελέγχου (ICS-Industrial Control Systems), τα λειτουργικά περιβάλλοντα και οι εκτιμήσεις για τις Τεχνολογίες Πληροφορικής και για τα Συστήματα Βιομηχανικού Ελέγχου διαφέρουν. Τα Συστήματα Βιομηχανικού Ελέγχου έχουν άμεση επίδραση στον φυσικό κόσμο, συμπεριλαμβανομένων πιθανών κινδύνων για την υγεία και την ασφάλεια των ατόμων, καθώς και επιπτώσεων στο περιβάλλον. Επιπλέον, τα Συστήματα Βιομηχανικού Ελέγχου έχουν μοναδικές απαιτήσεις απόδοσης και αξιοπιστίας σε σύγκριση με τις Τεχνολογίες Πληροφορικής , και οι στόχοι της ασφάλειας και της αποτελεσματικότητας πρέπει να λαμβάνονται υπόψη κατά την εφαρμογή μέτρων κυβερνοασφάλειας.

Για ευκολία στη χρήση, σε κάθε στοιχείο του Πυρήνα του Πλαισίου δίνεται ένα μοναδικό αναγνωριστικό. Οι Λειτουργίες και οι Κατηγορίες έχουν η καθεμιά ένα μοναδικό αλφαβητικό αναγνωριστικό, όπως φαίνεται στον Πίνακα 1. Οι Υποκατηγορίες σε κάθε Κατηγορία αναφέρονται αριθμητικά. Το μοναδικό αναγνωριστικό για κάθε Υποκατηγορία περιλαμβάνεται στον Πίνακα 2. Πρόσθετο υποστηρικτικό υλικό, συμπεριλαμβανομένων Πληροφοριακών Αναφορών, σχετικά με το Πλαίσιο μπορεί να βρεθεί στον ιστότοπο του NIST στη διεύθυνση http://www.nist.gov/cyberframework/.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Πίνακας 1: Μοναδικά Αναγνωριστικά Λειτουργιών και Κατηγοριών

Μοναδικό Αναγνωριστικό Λειτουργίας	Λειτουργία	Μοναδικό Αναγνωριστικό Κατηγορίας	Κατηγορία
ID	Προσδιορισμός (Identify)	ID.AM	Διαχείριση Αγαθών (Asset Management)
		ID.BE	Επιχειρηματικό Περιβάλλον (Business Environment)
		ID.GV	Διακυβέρνηση (Governance)
		ID.RA	Εκτίμηση Κινδύνων (Risk Assessment)
		ID.RM	Στρατηγική Διαχείρισης Κινδύνων (Risk Management Strategy)
		ID.SC	Διαχείριση Κινδύνων Εφοδιαστικής Αλυσίδας (Supply Chain Risk Management)
PR	Προστασία (Protect)	PR.AC	Διαχείριση Ταυτότητας και Έλεγχος Πρόσβασης (Identity Management and Access Control)
		PR.AT	Ευαισθητοποίηση και Εκπαίδευση (Awareness and Training)
		PR.DS	Ασφάλεια Δεδομένων (Data Security)
		PR.IP	Διεργασίες και Διαδικασίες Προστασίας Πληροφοριών (Information Protection Processes and Procedures)
		PR.MA	Συντήρηση (Maintenance)
		PR.PT	Τεχνολογίες Προστασίας (Protective Technology)
DE	Εντοπισμός (Detect)	DE.AE	Ανομοιομορφίες και Συμβάντα (Anomalies and Events)
		DE.CM	Συνεχής Παρακολούθηση Ασφάλειας (Security Continuous Monitoring)
		DE.DP	Διαδικασίες Ανίχνευσης (Detection Processes)
RS	Ανταπόκριση (Respond)	RS.RP	Σχεδιασμός Ανταπόκρισης (Response Planning)
		RS.CO	Επικοινωνίες (Communications)
		RS.AN	Ανάλυση (Analysis)
		RS.MI	Ελαχιστοποίηση (Mitigation)
		RS.IM	Βελτιώσεις (Improvements)
RC	Ανάκαμψη (Recover)	RC.RP	Σχεδιασμός Ανάκαμψης (Recovery Planning)
		RC.IM	Βελτιώσεις (Improvements)
		RC.CO	Επικοινωνίες (Communications)

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Πίνακας 2: Ο Πυρήνας του Πλαισίου

Λειτουργία	Κατηγορία	Υποκατηγορία	Πληροφοριακές Αναφορές
ΑΝΑΓΝΩΡΙΣΗ (ID)	**Διαχείριση πληροφορικών αγαθών (ID.AM):** Τα δεδομένα, το προσωπικό, οι συσκευές, τα συστήματα και οι υποδομές που επιτρέπουν στον οργανισμό να επιτύχει τους επιχειρησιακούς του σκοπούς, αναγνωρίζονται και αντιμετωπίζονται σύμφωνα με τη σχετική σημασία που έχουν ως προς τους οργανωσιακούς στόχους και τη στρατηγική διαχείρισης κινδύνου του οργανισμού.	**ID.AM-1:** Οι φυσικές συσκευές και συστήματα εντός του οργανισμού καταγράφονται	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Οι πλατφόρμες λογισμικού και εφαρμογών εντός του οργανισμού καταγράφονται	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Οι επικοινωνίες και ροές δεδομένων του οργανισμού χαρτογραφούνται	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Εξωτερικά συστήματα πληροφοριών καταλογογραφούνται	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Οι πόροι (π.χ. υλικό, συσκευές, δεδομένα, χρόνος, προσωπικό και λογισμικό) ιεραρχούνται με βάση την ταξινόμηση, την κρισιμότητα και την επιχειρησιακή τους αξία	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Οι ρόλοι και αρμοδιότητες κυβερνοασφάλειας καθιερώνονται για ολόκληρο το εργατικό δυναμικό και τρίτα ενδιαφερόμενα μέρη (π.χ. προμηθευτές, πελάτες, συνεργάτες)	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Επιχειρηματικό περιβάλλον (ID.BE): Η αποστολή του οργανισμού, οι στόχοι, τα ενδιαφερόμενα μέρη και οι δραστηριότητές του κατανοούνται και ιεραρχούνται. Οι πληροφορίες αυτές χρησιμοποιούνται για τη διαμόρφωση ρόλων	**ID.BE-1: Ο** ρόλος του οργανισμού στην αλυσίδα εφοδιασμού προσδιορίζεται και κοινοποιείται	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12

	κυβερνοασφάλειας, αρμοδιοτήτων και αποφάσεων διαχείρισης κινδύνων.	**ID.BE-2:** Η θέση του οργανισμού μεταξύ των κρίσιμων υποδομών και εντός του κλάδου του προσδιορίζεται και κοινοποιείται	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Οι προτεραιότητες για την αποστολή του οργανισμού, τους στόχους και τις δραστηριότητές του καθορίζονται και κοινοποιούνται	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Οι αλληλεξαρτήσεις και κρίσιμες λειτουργίες για την παροχή κρίσιμων υπηρεσιών καθορίζονται	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Οι απαιτήσεις ανθεκτικότητας που υποστηρίζουν την παροχή κρίσιμων υπηρεσιών για όλες τις καταστάσεις λειτουργίας (π.χ. υπό πίεση/ υπό επίθεση, κατά την ανάκαμψη, σε κανονική λειτουργία) καθορίζονται	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA14
	Διακυβέρνηση (ID.GV): Οι πολιτικές, οι διεργασίες και οι διαδικασίες για τη διαχείριση και την παρακολούθηση των απαιτήσεων του οργανισμού σε κανονιστικό, νομικό, περιβαλλοντικό και λειτουργικό επίπεδο, καθώς και για τη διαχείριση κινδύνου, γίνονται αντικείμενο κατανόησης και ενημερώνουν τη διαχείριση των κινδύνων κυβερνοασφάλειας	**ID.GV-1:** Η πολιτική κυβερνοασφάλειας για τον οργανισμό καθιερώνεται και κοινοποιείται.	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-2: Οι ρόλοι και οι αρμοδιότητες κυβερνοασφάλειας συντονίζονται και ευθυγραμμίζονται με εσωτερικούς ρόλους και εξωτερικούς συνεργάτες	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Οι νομικές και κανονιστικές απαιτήσεις σχετικά με την ασφάλεια στον κυβερνοχώρο, συμπεριλαμβανομένων των υποχρεώσεων ιδιωτικότητας και πολιτικών ελευθεριών, γίνονται αντικείμενο κατανόησης και διαχείρισης	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: Οι κίνδυνοι κυβερνοασφάλειας αντιμετωπίζονται με διαδικασίες διακυβέρνησης και διαχείρισης κινδύνου	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Clause 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM9, PM-10, PM-11

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

	Αξιολόγηση κινδύνου (ID.RA): Ο οργανισμός κατανοεί τους κίνδυνους κυβερνοασφάλειας για τη λειτουργία του (συμπεριλαμβανομένων των κινδύνων που άπτονται της αποστολής του, των επιμέρους λειτουργιών, της εικόνας ή της φήμης του), για τα πληροφοριακά αγαθά του, και τα άτομα.	**ID.RA-1:** Οι ευπάθειες των πληροφοριακών αγαθών εντοπίζονται και τεκμηριώνονται	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Πληροφορίες για τις απειλές στον κυβερνοχώρο λαμβάνονται από φόρουμ ανταλλαγής πληροφοριών και από άλλες πηγές	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Οι απειλές εντοπίζονται και τεκμηριώνονται, τόσο οι εσωτερικές όσο και οι εξωτερικές	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM16
		ID.RA-4: Ο πιθανός επιχειρηματικός αντίκτυπος και η πιθανότητα του προσδιορίζεται	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM9, PM-11
		ID.RA-5: Οι απειλές, οι ευπάθειες, η πιθανότητα και ο αντίκτυπος, χρησιμοποιούνται για τον προσδιορισμό του κινδύνου	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Τα μέτρα αντιμετώπισης του κινδύνου εντοπίζονται και ιεραρχούνται	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Στρατηγική Διαχείρισης Κινδύνων (ID.RM): Οι προτεραιότητες, οι περιορισμοί, η ανοχή στον κίνδυνο και οι παραδοχές του οργανισμού καθορίζονται προκειμένου να χρησιμοποιηθούν για την υποστήριξη αποφάσεων που σχετίζονται με λειτουργικούς κινδύνους.	**ID.RM-1:** Οι διαδικασίες διαχείρισης κινδύνων που αποτελούν αντικείμενο συμφωνίας και διαχείρισης μεταξύ των ενδιαφερομένων στον οργανισμό καθιερώνονται	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Η ανοχή του οργανισμού στον κίνδυνο καθορίζεται και εκφράζεται με σαφήνεια	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: Ο προσδιορισμός της ανοχής κινδύνου του οργανισμού καθορίζεται από τον ρόλο του οργανισμού μεταξύ των κρίσιμων υποδομών και από την ανάλυση κινδύνου ανά τομέα	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM11
	Διαχείριση Κινδύνου Εφοδιαστικής Αλυσίδας (ID.SC): Οι προτεραιότητες, οι περιορισμοί, η ανοχή στον κίνδυνο και οι παραδοχές του οργανισμού καθορίζονται προκειμένου να χρησιμοποιηθούν για την υποστήριξη αποφάσεων που σχετίζονται με τη διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας. Ο οργανισμός έχει καθιερώσει και εφαρμόσει τις διαδικασίες για τον εντοπισμό, την αξιολόγηση και διαχείριση των κινδύνων της εφοδιαστικής αλυσίδας.	**ID.SC-1:** Οι διαδικασίες διαχείρισης του κινδύνου εφοδιαστικής αλυσίδας προσδιορίζονται, καθορίζονται, αξιολογούνται και αποτελούν αντικείμενο διαχείρισης και συμφωνίας μεταξύ των ενδιαφερόμενων μερών.	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Προμηθευτές και συνεργαζόμενα τρίτα μέρη σε πληροφοριακά συστήματα, εξοπλισμό και υπηρεσίες εντοπίζονται, ιεραρχούνται και αξιολογούνται με τη χρήση μιας διαδικασίας αξιολόγησης των κινδύνων της εφοδιαστικής αλυσίδας στον κυβερνοχώρο	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA14, SA-15, PM-9
		ID.SC-3: Οι συμβάσεις με προμηθευτές και τρίτους συνεργάτες χρησιμοποιούνται για την εφαρμογή κατάλληλων μέτρων που αποσκοπούν στην ικανοποίηση των στόχων των προγραμμάτων κυβερνοασφάλειας και του Σχεδίου Διαχείρισης των Κινδύνων της Εφοδιαστικής Αλυσίδας	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM9
		ID.SC-4: Προμηθευτές και τρίτοι συνεργάτες αξιολογούνται συστηματικά με τη χρήση ελέγχων, αποτελεσμάτων δοκιμών ή με άλλες μορφές αξιολόγησης, για να επιβεβαιωθεί ότι τηρούν τις συμβατικές τους υποχρεώσεις	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU16, PS-7, SA-9, SA-12
		ID.SC-5: Ο σχεδιασμός και οι δοκιμές απόκρισης και ανάκαμψης διεξάγονται με τους προμηθευτές και τρίτους παρόχους υπηρεσιών	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			NIST SP 800-53 Rev. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
ΠΡΟΣΤΑΣΙΑ (PR)	**Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης (PR.AC):** Η πρόσβαση σε φυσικά και λογικά πληροφοριακά αγαθά και σχετικές εγκαταστάσεις περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες, διεργασίες και συσκευές και η διαχείριση της ταυτότητας γίνεται σύμφωνα με την εκτίμηση των κινδύνων που σχετίζονται με μη εξουσιοδοτημένη πρόσβαση σε δραστηριότητες και συναλλαγές για τις οποίες χρειάζονται δικαιώματα.	**PR.AC-1:** Οι ταυτότητες και τα διαπιστευτήρια εκδίδονται, διαχειρίζονται, επαληθεύονται, ανακαλούνται και ελέγχονται όταν αυτά αφορούν εξουσιοδοτημένες συσκευές, εξουσιοδοτημένους χρήστες καθώς και εξουσιοδοτημένες διαδικασίες	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Η φυσική πρόσβαση σε πληροφοριακά αγαθά διαχειρίζεται και προστατεύεται	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Η απομακρυσμένη πρόσβαση διαχειρίζεται	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Η ενσωμάτωση της αρχής της ελαχιστοποίησης δικαιωμάτων και της αρχής του διαχωρισμού των καθηκόντων εφαρμόζεται στη διαχείριση των δικαιωμάτων πρόσβασης και των εξουσιοδοτήσεων	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Η ακεραιότητα του δικτύου προστατεύεται (π.χ. διαχωρισμός δικτύου, τμηματοποίηση δικτύου)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

		PR.AC-6: Οι ταυτότητες αποδεικνύονται μέσω ελέγχων και συνδέονται με διαπιστευτήρια τα οποία μπορούν να επιβεβαιωθούν μέσω αλληλεπιδράσεων	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Η αυθεντικοποίηση χρηστών, συσκευών και άλλων πληροφοριακών αγαθών (π.χ. όταν υπάρχει ένας παράγοντας αυθεντικοποίησης, πολλαπλοί παράγοντες αυθεντικοποίησης) πραγματοποιείται ανάλογα με τους κινδύνους των συναλλαγών (π.χ. κινδυνοι που σχετίζονται με την ασφάλεια και την ιδιωτικότητα ατόμων και άλλοι οργανωτικοί κίνδυνοι)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Ευαισθητοποίηση και Εκπαίδευση (PR.AT): Το προσωπικό και οι συνεργάτες του οργανισμού λαμβάνουν μαθήματα ευαισθητοποίησης στον τομέα της κυβερνοασφάλειας και εκπαιδεύονται για να εκτελούν τα καθήκοντα και τις ευθύνες τους που σχετίζονται με την κυβερνοασφάλεια. σύμφωνα με τις σχετικές πολιτικές, διαδικασίες και συμφωνίες.	**PR.AT-1:** Όλοι οι χρήστες ενημερώνονται και εκπαιδεύονται	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA** 62443-2-1:2009 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Οι προνομιούχοι χρήστες κατανοούν τους ρόλους και τις ευθύνες τους	**CIS CSC** 5, 17, 18 **COBIT** 5 APO07.02, DSS05.04, DSS06.03 **ISA** 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Ενδιαφερόμενοι τρίτοι (π.χ, προμηθευτές, πελάτες, συνεργάτες) κατανοούν τους ρόλους και τις ευθύνες τους	**CIS CSC** 17 **COBIT** 5 APO07.03, APO07.06, APO10.04, APO10.05 **ISA** 62443-2-1:2009 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Τα ανώτερα στελέχη κατανοούν τους ρόλους και τις ευθύνες τους	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

		PR.AT-5: Το προσωπικό φυσικής ασφάλειας και κυβερνοασφάλειας κατανοεί τους ρόλους και τις ευθύνες του.	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Ασφάλεια Δεδομένων (PR.DS): Η διαχείριση των πληροφοριών και των αρχείων (δεδομένων) γίνεται σύμφωνα με τη στρατηγική αντιμετώπισης κινδύνων του οργανισμού με σκοπό την προστασία της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών.	**PR.DS-1:** Τα δεδομένα προστατεύονται κατά την αποθήκευση	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Τα δεδομένα προστατεύονται κατά τη μεταφορά	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Η διαχείριση των πληροφοριακών αγαθών διεξάγεται με επίσημο τρόπο σε όλη τη διάρκεια της απομάκρυνσης, των μετακινήσεων και της απόρριψής τους.	**CIS CSC** 1 **COBIT 5** BAI09.03 ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Διατηρείται επαρκής χωρητικότητα για τη διασφάλιση της διαθεσιμότητας	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Εφαρμόζονται μέτρα προστασίας κατά της διαρροής δεδομένων	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

		PR.DS-6: Χρησιμοποιούνται μηχανισμοί ελέγχου για την επαλήθευση της ακεραιότητας λογισμικού, υλικολογισμικού και πληροφοριών	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: Το(α) περιβάλλον(τα) ανάπτυξης και δοκιμών χωρίζεται από το περιβάλλον παραγωγής	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Χρησιμοποιούνται μηχανισμοί ελέγχου για την επαλήθευση της ακεραιότητας του υλικού	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Διεργασίες και Διαδικασίες Προστασίας Πληροφοριών (PR.IP): Οι πολιτικές ασφάλειας (που αφορούν τον σκοπό, το πεδίο εφαρμογής, τους ρόλους, τις αρμοδιότητες, τη δέσμευση της διοίκησης και τον συντονισμό μεταξύ των οντοτήτων του οργανισμού), οι διεργασίες και οι διαδικασίες διατηρούνται και χρησιμοποιούνται για τη διαχείριση της προστασίας πληροφοριακών συστημάτων και πληροφοριακών αγαθών	**PR.IP-1:** Δημιουργείται και διατηρείται μια βασική διαμόρφωση συστημάτων τεχνολογίας πληροφορικής/βιομηχανικού ελέγχου που ενσωματώνει αρχές ασφάλειας (π.χ. έννοια της ελάχιστης λειτουργικότητας)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Εφαρμόζεται ένας Κύκλος Ζωής Ανάπτυξης Συστήματος για τη διαχείριση συστημάτων	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Εφαρμόζονται διαδικασίες ελέγχου αλλαγής διαμόρφωσης	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Αντίγραφα ασφάλειας πληροφοριών δημιουργούνται, τηρούνται και ελέγχονται	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Τηρούνται πολιτικές και κανονισμοί σχετικά με το φυσικό περιβάλλον λειτουργίας των πληροφοριακών αγαθών του οργανισμού	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Τα δεδομένα καταστρέφονται σύμφωνα με την πολιτική	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Βελτιώνονται οι διαδικασίες προστασίας	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Διαμοιράζεται η αποτελεσματικότητα των τεχνολογιών προστασίας	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Τα σχέδια ανταπόκρισης (Ανταπόκριση σε Περιστατικά Ασφάλειας και Επιχειρησιακή Συνέχεια) και τα σχέδια ανάκαμψης (Ανάκαμψη από Περιστατικά Ασφάλειας και Ανάκαμψη από Καταστροφές) εφαρμόζονται και διαχειρίζονται από υπεύθυνες ομάδες	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Τα σχέδια ανταπόκρισης και ανάκαμψης ελέγχονται	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Η κυβερνοασφάλεια περιλαμβάνεται στις πρακτικές που ακολουθούν τα τμήματα ανθρώπινων πόρων (π.χ. κατάργηση πρόσβασης, έλεγχος προσωπικού)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: Αναπτύσσεται και εφαρμόζεται σχέδιο διαχείρισης ευπαθειών	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Συντήρηση (PR.MA): Η συντήρηση και οι επισκευές των εξαρτημάτων των συστημάτων βιομηχανικού ελέγχου και των πληροφοριακών συστημάτων πραγματοποιούνται σύμφωνα με τις πολιτικές και τις διαδικασίες	**PR.MA-1:** Η συντήρηση και η επισκευή των πληροφοριακών αγαθών του οργανισμού πραγματοποιείται και καταγράφεται, με εγκεκριμένα και ελεγχόμενα εργαλεία	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Η απομακρυσμένη συντήρηση των πληροφοριακών αγαθών του οργανισμού εγκρίνεται, καταγράφεται και εκτελείται με τρόπο που αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση.	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4
	Τεχνολογία Προστασίας (PR.PT): Οι τεχνικές λύσεις ασφάλειας διαχειρίζονται για να διασφαλιστεί η ασφάλεια και η ανθεκτικότητα των συστημάτων και των πληροφοριακών αγαθών σύμφωνα με τις σχετικές πολιτικές, διαδικασίες και συμφωνίες.	**PR.PT-1:** Τα αρχεία ελέγχου/καταγραφής καθορίζονται, τεκμηριώνονται, εφαρμόζονται και επανεξετάζονται σύμφωνα με την πολιτική.	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Τα εξωτερικά μέσα προστατεύονται και η χρήση τους περιορίζεται σύμφωνα με την πολιτική	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Η αρχή της ελάχιστης λειτουργικότητας ενσωματώνεται με τη διαμόρφωση των συστημάτων έτσι ώστε να παρέχουν μόνο τις βασικές δυνατότητες	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6,

			4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Τα δίκτυα επικοινωνίας και ελέγχου προστατεύονται	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Εφαρμόζονται μηχανισμοί (π.χ. failsafe, load balancing, hot swap) για την επίτευξη των απαιτήσεων ανθεκτικότητας σε κανονικές και δυσμενείς καταστάσεις.	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
ΕΝΤΟΠΙΣΜΟΣ (DE)	**Ανομοιομορφίες και Συμβάντα (DE.AE):** Η ανομοιόμορφή δραστηριότητα ανιχνεύεται και γίνεται κατανοητή η πιθανή επίπτωση των γεγονότων.	**DE.AE-1:** Υπάρχουν και διαχειρίζονται βασικές γραμμές αναφοράς των λειτουργιών δικτύου και των αναμενόμενων ροών δεδομένων για τους χρήστες και τα συστήματα.	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Τα εντοπισμένα συμβάντα αναλύονται για την κατανόηση των στόχων και των μεθόδων επίθεσης	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Τα δεδομένα συμβάντων συλλέγονται και συσχετίζονται από πολλαπλές πηγές και αισθητήρες	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Η πιθανή επίπτωση των γεγονότων γίνεται κατανοητή	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Τα όρια προειδοποίησης συμβάντων καθορίζονται	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Συνεχής Παρακολούθηση Ασφάλειας (DE.CM): Το πληροφοριακό σύστημα και πληροφοριακά αγαθά παρακολουθούνται για τον εντοπισμό συμβάντων κυβερνοασφάλειας και για να επαληθεύσουν την αποτελεσματικότητα των προστατευτικών μέτρων.	**DE.CM-1:** Το δίκτυο παρακολουθείται για τον εντοπισμό πιθανών συμβάντων κυβερνοασφάλειας	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: Το φυσικό περιβάλλον παρακολουθείται για τον εντοπισμό πιθανών συμβάντων κυβερνοασφάλειας	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Η δραστηριότητα του προσωπικού παρακολουθείται για τον εντοπισμό πιθανών συμβάντων κυβερνοασφάλειας	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Ο κακόβουλος κώδικας εντοπίζεται	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Ο μη εξουσιοδοτημένος φορητός κώδικάς εντοπίζεται	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			ISO/IEC 27001:2013 A.12.5.1, A.12.6.2 **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: Οι δραστηριότητες των εξωτερικών παροχών υπηρεσιών παρακολουθούνται για τον εντοπισμό πιθανών συμβάντων κυβερνοασφάλειας	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Πραγματοποιείται παρακολούθηση για μη εξουσιοδοτημένο προσωπικό, συνδέσεις, συσκευές και λογισμικό	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Εκτελούνται σαρώσεις ευπάθειας	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Διαδικασίες Ανίχνευσης (DE.DP): Διατηρούνται και δοκιμάζονται διαδικασίες ανίχνευσης ώστε να διασφαλιστεί η επίγνωση των μη ομαλών συμβάντων.	**DE.DP-1:** Οι ρόλοι και οι αρμοδιότητες για τον εντοπισμό καθορίζονται πλήρως για να διασφαλιστεί η λογοδοσία	**CIS CSC 19** **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Οι δραστηριότητες ανίχνευσης συμμορφώνονται με όλες τις ισχύουσες απαιτήσεις	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3:Δοκιμάζονται οι διαδικασίες ανίχνευσης	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Κοινοποιούνται πληροφορίες εντοπισμού συμβάντων	**CIS CSC 19** **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Βελτιώνονται συνεχώς οι διαδικασίες ανίχνευσης	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
ΑΝΤΑΠΟΚΡΙΣΗ (RS)	**Σχεδιασμός Ανταπόκρισης (RS.RP):** Εκτελούνται και συντηρούνται διεργασίες και διαδικασίες ανταπόκρισης, ώστε να διασφαλίζεται η ανταπόκριση σε περιστατικά κυβερνοασφάλειας που ανιχνεύονται.	**RS.RP-1:** Το σχέδιο ανταπόκρισης εκτελείται κατά τη διάρκεια ή μετά από ένα περιστατικό.	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 ISA 62443-2-1:2009 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Επικοινωνίες (RS.CO): Οι δραστηριότητες ανταπόκρισης συντονίζονται με εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς (π.χ. εξωτερική υποστήριξη από τις υπηρεσίες επιβολής του νόμου).	**RS.CO-1:** Οι ρόλοι και η σειρά των επιχειρήσεων έχουν γνωστοποιηθεί στο προσωπικό σε περίπτωση που απαιτηθεί ανταπόκριση	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Τα περιστατικά αναφέρονται σύμφωνα με τα καθιερωμένα κριτήρια	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Οι πληροφορίες ανταλλάσσονται σύμφωνα με τα σχέδια ανταπόκρισης	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Τα σχέδια ανταπόκρισης συντονίζονται σύμφωνα με τα ενδιαφερόμενα μέρη	**CIS CSC** 19 **COBIT 5** DSS03.04 ISA 62443-2-1:2009 4.3.4.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Για την επίτευξη ευρύτερης επίγνωσης της κατάστασης στον κυβερνοχώρο πραγματοποιείται εθελοντική ανταλλαγή πληροφοριών με εξωτερικούς ενδιαφερόμενους φορείς	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Ανάλυση (RS.AN): Διεξάγεται ανάλυση ώστε να εξασφαλιστεί η αποτελεσματική ανταπόκριση και να υποστηριχθούν οι δραστηριότητες ανάκαμψης.	**RS.AN-1:** Ερευνώνται οι ειδοποιήσεις από συστήματα εντοπισμού	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

			NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Γίνεται κατανοητός ο αντίκτυπος του συμβάντος	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Πραγματοποιούνται έρευνες ψηφιακών πειστηρίων	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Τα περιστατικά κατηγοριοποιούνται σύμφωνα με τα σχέδια ανταπόκρισης	**CIS CSC** 19 **COBIT 5** DSS02.02 ISA 62443-2-1:2009 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Καθορίζονται διαδικασίες για τη λήψη, ανάλυση και ανταπόκριση των ευπαθειών που αποκαλύπτονται στον οργανισμό από εσωτερικές και εξωτερικές πηγές (π.χ. από εσωτερικές δοκιμές, από ανακοινώσεις για θέματα ασφάλειας ή από ερευνητές ασφαλείας).	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Μετριασμός (RS.MI): Εκτελούνται δραστηριότητες για την πρόληψη της επέκτασης ενός συμβάντος, τον μετριασμό των επιπτώσεών του και την επίλυση του περιστατικού.	**RS.MI-1:** Τα περιστατικά περιορίζονται	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Τα περιστατικά μετριάζονται	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Οι πρόσφατα εντοπισμένες ευπάθειες μετριάζονται ή τεκμηριώνονται ως αποδεκτοί κίνδυνοι.	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Βελτιώσεις (RS.IM): Οι οργανωτικές δραστηριότητες ανταπόκρισης βελτιώνονται με την ενσωμάτωση διδαγμάτων που προέκυψαν από τις τρέχουσες και από προηγούμενες δραστηριότητες εντοπισμού ή/και ανταπόκρισης.	**RS.IM-1:** Τα διδάγματα που αντλήθηκαν ενσωματώνονται στα σχέδια ανταπόκρισης	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Οι στρατηγικές ανταπόκρισης ενημερώνονται	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

ΑΝΑΚΑΜΨΗ (RC)	**Σχεδιασμός Ανάκαμψης (RC.RP):** Οι διαδικασίες και διεργασίες ανάκαμψης εκτελούνται και συντηρούνται για να εξασφαλιστεί η αποκατάσταση των συστημάτων ή των πληροφοριακών αγαθών που επηρεάζονται από περιστατικά κυβερνοασφάλειας.	**RC.RP-1:** Το σχέδιο ανάκαμψης εκτελείτε κατά τη διάρκεια ή μετά από ένα περιστατικό κυβερνοασφάλειας	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Βελτιώσεις (RC.IM): Ο σχεδιασμός και οι διαδικασίες ανάκαμψης βελτιώνονται με την ενσωμάτωση των διδαγμάτων που αντλήθηκαν από το παρελθόν σε μελλοντικές δραστηριότητες.	**RC.IM-1:** Τα διδάγματα από το παρελθόν ενσωματώνονται στα σχέδια ανάκαμψης	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Ενημερώνονται οι στρατηγικές ανάκαμψης	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Επικοινωνίες (RC.CO): Οι δραστηριότητες αποκατάστασης συντονίζονται μεταξύ εσωτερικών και εξωτερικών μερών (π.χ. συντονιστικά κέντρα, Πάροχοι Υπηρεσιών Διαδικτύου, Ιδιοκτήτες επιτιθέμενων συστημάτων, θύματα, άλλες Ομάδες Ανταπόκρισης Περιστατικών Κυβερνοασφάλειας (CSIRT), και κατασκευαστές).	**RC.CO-1:** Διαχειρίζονται οι δημόσιες σχέσεις	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Η φήμη αποκαθίσταται μετά από ένα περιστατικό	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Οι δραστηριότητες ανάκαμψης κοινοποιούνται σε εσωτερικά και εξωτερικά ενδιαφερομένα μέρη, καθώς και στις ομάδες Διοίκησης και Διαχείρισης	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

Πληροφορίες σχετικά με τις Πληροφοριακές Αναφορές που αναφέρονται στο Παράρτημα Α μπορούν να βρεθούν στις ακόλουθες τοποθεσίες:

- Στόχοι Ελέγχων Πληροφορικής και Συναφούς Τεχνολογίας (Control Objectives for Information and Related Technologies - COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Κρίσιμοι Έλεγχοι Ασφάλειας του Κέντρου για την Ασφάλεια στο Διαδίκτυο (Center for Internet Security - CIS) για Αποτελεσματική Άμυνα στον Κυβερνοχώρο (CIS Controls): https://www.cisecurity.org
- Αμερικανικό Εθνικό Ινστιτούτο Προτύπων/Διεθνής Εταιρεία Αυτοματισμού (American National Standards Institute/International Society of Automation - ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Ασφάλεια για Συστήματα Βιομηχανικού Αυτοματισμού και Ελέγχου: Καθιέρωση Προγράμματος Ασφάλειας Βιομηχανικού Αυτοματισμού και Συστημάτων Ελέγχου*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Ασφάλεια για Συστήματα Βιομηχανικού Αυτοματισμού και Ελέγχου: Απαιτήσεις και Επίπεδα Ασφάλειας Συστήματος*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Τεχνολογία πληροφορικής -- Τεχνικές ασφάλειας -- Συστήματα διαχείρισης ασφάλειας πληροφοριών – Απαιτήσεις*: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 – Ειδική Έκδοση του NIST 800-53 Έκδοση 4, *Έλεγχοι Ασφάλειας και Απορρήτου για Ομοσπονδιακά Πληροφοριακά Συστήματα και Οργανισμούς*, Απρίλιος 2013 (συμπεριλαμβανομένων των αναθεωρήσεων από 22 Ιανουαρίου, 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Οι Πληροφοριακές Αναφορές είναι αντίστοιχες μόνο με το επίπεδο ελέγχων, αν και οποιαδήποτε βελτίωση στους ελέγχους μπορεί να φανεί χρήσιμη για την επίτευξη ενός αποτελέσματος υποκατηγορίας.

Οι αντιστοιχίσεις μεταξύ των Υποκατηγοριών του Πυρήνα του Πλαισίου και των συγκεκριμένων ενοτήτων στις Πληροφοριακές Αναφορές δεν έχουν σκοπό να καθορίσουν οριστικά εάν οι συγκεκριμένες ενότητες στις Πληροφοριακές Αναφορές παρέχουν το επιθυμητό αποτέλεσμα Υποκατηγορίας.

Οι Πληροφοριακές Αναφορές δεν είναι εξαντλητικές, δεδομένου ότι δεν αντιστοιχίζονται όλα τα στοιχεία (π.χ. έλεγχος, απαίτηση) μιας δεδομένης Πληροφοριακής Αναφοράς σε Υποκατηγορίες του Πυρήνα του Πλαισίου.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Παράρτημα Β: Γλωσσάριο

Αυτό το παράρτημα παρουσιάζει επιλεγμένους όρους που χρησιμοποιούνται σε αυτή τη δημοσίευση.

Πίνακας 3: Γλωσσάριο του Πλαισίου

Buyer	**Πελάτης / Αγοραστής**	Τα άτομα ή οι οργανισμοί που καταναλώνουν ένα δεδομένο προϊόν ή υπηρεσία.
Category	**Κατηγορία**	Η υποδιαίρεση μιας Λειτουργίας σε ομάδες αποτελεσμάτων κυβερνοασφάλειας, στενά συνδεδεμένες με προγραμματικές ανάγκες και συγκεκριμένες δραστηριότητες. Παραδείγματα κατηγοριών αποτελούν η "Διαχείριση πληροφοριακών αγαθών", η "Διαχείριση ταυτότητας και Έλεγχος Πρόσβασης" και οι "Διαδικασίες Εντοπισμού".
Critical Infrastructure	**Κρίσιμες Υποδομές**	Συστήματα και πληροφοριακά αγαθά φυσικά ή εικονικά, τόσο ζωτικής σημασίας για τη χώρα μας (σ.μ.: στο πρωτότυπο αναφέρονται ως χώρα οι Ηνωμένες Πολιτείες) που η δυσλειτουργία ή η καταστροφή τέτοιων συστημάτων και πληροφοριακών αγαθών θα είχε καταλυτική επίδραση στην κυβερνοασφάλεια, στην εθνική οικονομική σταθερότητα, την εθνική δημόσια υγεία ή ασφάλεια ή οποιονδήποτε συνδυασμό αυτών των θεμάτων (σ.μ.: Στην ελληνική νομοθεσία σχετικά με την προστασία των Κρίσιμων Υποδομών ορίζονται ως Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών - Φ.Ε.Β.Υ.).
Cybersecurity	**Κυβερνοασφάλεια**	Η διαδικασία προστασίας των πληροφοριών μέσω της αποτροπής, του εντοπισμού και της ανταπόκρισης σε επιθέσεις.
Cybersecurity Event	**Συμβάν Κυβερνοασφάλειας**	Μια αλλαγή στην κυβερνοασφάλεια που μπορεί να έχει αντίκτυπο στις οργανωσιακές λειτουργίες (συμπεριλαμβανομένης της αποστολής του οργανισμού, των δυνατοτήτων του ή της φήμης του).
Cybersecurity Incident	**Περιστατικό Κυβερνοασφάλειας**	Ένα περιστατικό κυβερνοασφάλειας που έχει καθοριστεί ότι έχει αντίκτυπο στον οργανισμό, προκαλώντας την ανάγκη ανταπόκρισης και ανάκαμψης.
Detect (function)	**Εντοπισμός (λειτουργία)**	Ανάπτυξη και εφαρμογή των κατάλληλων δραστηριοτήτων για τον προσδιορισμό της

		εμφάνισης ενός περιστατικού κυβερνοασφάλειας.
Framework	**Πλαίσιο**	Μια εστιασμένη προσέγγιση για τη μείωση του κινδύνου κυβερνοασφάλειας που αποτελείται από τρία μέρη: τον Πυρήνα του Πλαισίου, το Προφίλ Πλαισίου και τα Επίπεδα Υλοποίησης του Πλαισίου. Γνωστό και ως το «Πλαίσιο Κυβερνοασφάλειας».
Framework Core	**Πυρήνας του Πλαισίου**	Ένα σύνολο δραστηριοτήτων και αναφορών στον τομέα της κυβερνοασφάλειας που είναι κοινές σε τομείς κρίσιμων υποδομών και οργανώνονται γύρω από συγκεκριμένα αποτελέσματα. Ο Πυρήνας του Πλαισίου περιλαμβάνει τέσσερις τύπους στοιχείων: Λειτουργίες, Κατηγορίες, Υποκατηγορίες και Πληροφοριακές Αναφορές.
Framework Implementation Tier	**Βαθμίδα Υλοποίησης Πλαισίου**	Ένα πρίσμα μέσω του οποίου μπορούν να εξεταστούν τα χαρακτηριστικά της προσέγγισης ενός οργανισμού στον κίνδυνο - πώς δηλαδή ένας οργανισμός αντιμετωπίζει τον κίνδυνο κυβερνοασφάλειας και τις διαδικασίες που εφαρμόζονται για τη διαχείριση αυτού του κινδύνου.
Framework Profile	**Προφίλ Πλαισίου**	Αναπαράσταση των αποτελεσμάτων που έχει επιλέξει ένα συγκεκριμένο σύστημα ή οργανισμός από τις Κατηγορίες και τις Υποκατηγορίες του Πλαισίου.
Function	**Λειτουργία**	Ένα από τα κύρια στοιχεία του Πλαισίου. Οι λειτουργίες αποτελούν το υψηλότερο επίπεδο δομής για την οργάνωση βασικών δραστηριοτήτων κυβερνοασφάλειας σε Κατηγορίες και Υποκατηγορίες. Οι πέντε λειτουργίες είναι Προσδιορισμός, Προστασία, Εντοπισμός, Ανταπόκριση και Ανάκαμψη.
Identify (function)	**Προσδιορισμός (λειτουργία)**	Ανάπτυξη της οργανωτικής κατανόησης για τη διαχείριση του κινδύνου κυβερνοασφάλειας για συστήματα, πληροφορικά αγαθά, δεδομένα και δυνατότητες.
Informative Reference	**Πληροφοριακή Αναφορά**	Μια συγκεκριμένη ενότητα προτύπων, κατευθυντήριων γραμμών και πρακτικών κοινών μεταξύ τομέων κρίσιμων υποδομών που απεικονίζει μια μέθοδο για την επίτευξη των αποτελεσμάτων που σχετίζονται με κάθε

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

		Υποκατηγορία. Ένα παράδειγμα πληροφοριακής αναφοράς είναι το ISO/IEC 27001 Control A.10.8.3, το οποίο υποστηρίζει την Υποκατηγορία «Προστασία κατά τη μεταφορά δεδομένων» της κατηγορίας «Ασφάλεια δεδομένων» στη λειτουργία «Προστασία».
Mobile Code	**Φορητός Κώδικας**	Ένα πρόγραμμα (π.χ. σενάριο εντολών, μακροεντολή ή άλλη φορητή οδηγία) που μπορεί να αποσταλεί αμετάβλητο σε μια ετερογενή συλλογή πλατφορμών και να εκτελεστεί με πανομοιότυπη σημασιολογία.
Protect (function)	**Προστασία (λειτουργία)**	Ανάπτυξη και εφαρμογή των κατάλληλων μέτρων προστασίας για τη διασφάλιση της παροχής των υπηρεσιών των κρίσιμων υποδομών.
Privileged User	**Προνομιούχος χρήστης**	Ένας χρήστης που είναι εξουσιοδοτημένος (και, επομένως, αξιόπιστος) να εκτελεί λειτουργίες που σχετίζονται με την ασφάλεια και τις οποίες οι απλοί χρήστες δεν είναι εξουσιοδοτημένοι να εκτελούν.
Recover (function)	**Ανάκαμψη (λειτουργία)**	Ανάπτυξη και εφαρμογή των κατάλληλων δραστηριοτήτων για τη διατήρηση σχεδίων ανθεκτικότητας και την αποκατάσταση τυχόν δυνατοτήτων ή υπηρεσιών που υποβαθμίστηκαν λόγω ενός περιστατικού κυβερνοασφάλειας.
Respond (function)	**Ανταπόκριση (λειτουργία)**	Ανάπτυξη και εφαρμογή των κατάλληλων δραστηριοτήτων για την ανάληψη δράσης σχετικά με ένα εντοπισμένο περιστατικό κυβερνοασφάλειας.
Risk	**Κίνδυνος**	Το μέτρο του βαθμού στον οποίο μια οντότητα απειλείται από μια πιθανή συνθήκη ή περιστατικό και συνήθως είναι συνάρτηση: (i) των δυσμενών επιπτώσεων που θα προέκυπταν εάν η συνθήκη ή το περιστατικό συνέβαινε, και (ii) της πιθανότητας της εμφάνισής του.
Risk Management	**Διαχείριση Κινδύνου**	Η διαδικασία προσδιορισμού, εκτίμησης και ανταπόκρισης στον κίνδυνο.
Subcategory	**Υποκατηγορία**	Η υποδιαίρεση μιας Κατηγορίας σε συγκεκριμένα αποτελέσματα τεχνικών ή/και διαχειριστικών δραστηριοτήτων. Παραδείγματα Υποκατηγοριών περιλαμβάνουν τα "Καταλογογράφηση

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

		εξωτερικών πληροφοριακών συστημάτων", "Προστασία δεδομένων κατά την αποθήκευση" και "Διερεύνηση ειδοποιήσεων από συστήματα εντοπισμού".
Supplier	**Πάροχος**	Οι πάροχοι προϊόντων και υπηρεσιών που χρησιμοποιούνται για εσωτερικούς σκοπούς ενός οργανισμού (π.χ. για την υποδομή πληροφορικής) ή ενσωματώνονται στα προϊόντα ή τις υπηρεσίες που παρέχονται στους αγοραστές αυτού του οργανισμού.
Taxonomy	**Ταξινόμηση**	Ένα σχήμα κατάταξης.

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6

Παράρτημα Γ: Ακρωνύμια

Αυτό το παράρτημα παρουσιάζει επιλεγμένα ακρωνύμια που χρησιμοποιούνται σε αυτή τη δημοσίευση.

ANSI	American National Standards Institute	Αμερικανικό Εθνικό Ινστιτούτο Προτύπων
CEA	Cybersecurity Enhancement Act of 2014	Νόμος των ΗΠΑ για την Ενίσχυση της Κυβερνοασφάλειας του 2014
CIS	Center for Internet Security	Κέντρο για την Ασφάλεια στο Διαδίκτυο
COBIT	Control Objectives for Information and Related Technology	Στόχοι Ελέγχων Πληροφορικής και Συναφούς Τεχνολογίας
CPS	Cyber-Physical Systems	Κυβερνο-Φυσικά Συστήματα
CSC	Critical Security Control	Κρίσιμο Μέτρο Ελέγχου Ασφάλειας
DHS	Department of Homeland Security	Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ
EO	Executive Order	Προεδρικό Διάταγμα
ICS	Industrial Control Systems	Συστήματα Βιομηχανικού Ελέγχου
IEC	International Electrotechnical Commission	Διεθνής Ηλεκτροτεχνική Επιτροπή
IoT	Internet of Things	Διαδίκτυο των Πραγμάτων
IR	Interagency Report	Διϋπηρεσιακή Αναφορά
ISA	International Society of Automation	Διεθνής Ένωση Αυτοματισμού
ISAC	Information Sharing and Analysis Center	Κέντρο Διαμοιρασμού και Ανάλυσης Πληροφοριών των ΗΠΑ
ISAO	Information Sharing and Analysis Organization	Οργανισμός Διαμοιρασμού και Ανάλυσης Πληροφοριών των ΗΠΑ
ISO	International Organization for Standardization	Διεθνής Οργανισμός Τυποποίησης
NIST	National Institute of Standards and Technology	Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ
OT	Operational Technology	Λειτουργική Τεχνολογία
PII	Personally Identifiable Information	Προσωπικά Στοιχεία Αναγνώρισης
RFI	Request for Information	Αίτημα Για Πληροφορίες
RMP	Risk Management Process	Διαδικασία Διαχείρισης Κινδύνου
SCRM	Supply Chain Risk Management	Διαχείριση Κινδύνων Εφοδιαστικής Αλυσίδας
SP	Special Publication	Ειδική Δημοσίευση

Αυτή η δημοσίευση διατίθεται δωρεάν στα αγγλικά από τη διεύθυνση: https://doi.org/10.6028/NIST.CSWP.6