ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟ

Έχει υπογραφεί
ψηφιακά από τον/την:
ILIAS KATSIADAS
2021-05-26
10:39:24+03:00

ΥΨηΔ 26/05/2021
Α. Π.: 15882 ΕΞ 2021

ΠΡΟΘΕΣΜΙΑ 25.05.2021

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΤΜΗΜΑ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ
Ταχ. Δ/νση: Χανδρή 1 & Θεσ/κης
ΤΚ: 18346 Μοσχάτο Αττικής
Πληροφορίες: Ι. Βοζώρης, Α. Διακίδου,
Χ. Κωστοπούλου, Μ. Πατσουράκης,
Τηλ.: 210 4802385
E-mail: dir.strategy.ncsa@mindigital.gr

Προς: Υπηρεσία Συντονισμού
Γραφείο Νομικών και
Κοινοβουλευτικών Θεμάτων

Κοιν:

1. Γραφείο κ. Υπουργού Επικρατείας
2. Γραφείο κ. Γενικού Γραμματέα Τηλεπικοινωνιών και Ταχυδρομείων

Θέμα: Απάντηση σε ερώτηση κοινοβουλευτικού ελέγχου

Σχετ.:

1. Το υπ' αριθμ. πρωτ. 13899 ΕΞ 2021/13.05.2021 έγγραφο της Υπηρεσίας σας

2. Η υπ' αριθμ. 6464/11.05.2021 Ερώτηση των βουλευτών κ..κ. Μ. Κάτση και Α. Γκαρά με θέμα: «Σοβαρά κενά ασφαλείας στα πληροφοριακά συστήματα e-ΕΦΚΑ και Υπουργείου Ψηφιακής Διακυβέρνησης τα καθιστούν ευάλωτα σε κυβερνοεπιθέσεις»

Σε απάντηση του ως άνω, **Σχετ. 1** εγγράφου της Υπηρεσίας σας, με το οποίο διαβιβάστηκε στην Υπηρεσία μας το ανωτέρω **Σχετ. 2**, και στο πλαίσιο των αρμοδιοτήτων μας, σας ενημερώνουμε για τα εξής:

Α. Πλαίσιο οργάνωσης και αρμοδιοτήτων

1. Με τα άρθρα 43 επ. του π.δ. 40/2020, προβλέπεται το πλαίσιο οργάνωσης και αρμοδιοτήτων της Γενικής Διεύθυνσης Κυβερνοασφάλειας. Στο πλαίσιο αυτό η Γενική Διεύθυνση Κυβερνοασφάλειας έχει (μεταξύ άλλων) τις κάτωθι αρμοδιότητες:

- Αποτελεί την Εθνική Αρχή Κυβερνοασφάλειας και εθνικό σημείο επαφής σύμφωνα με τις διατάξεις του ν. 4577/2018 (Α΄199) με τις οποίες ενσωματώνεται στην ελληνική νομοθεσία το πλαίσιο διατάξεων της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με μέτρα για

υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση» (εφεξής Οδηγία NIS).

- Είναι αρμόδια για τη χάραξη της ενιαίας πολιτικής Κυβερνοασφάλειας στο πλαίσιο της ελληνικής και ενωσιακής νομοθεσίας για την Κυβερνοασφάλεια και τις κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, όπως αυτές εκάστοτε ορίζονται νομοθετικά.
- Είναι αρμόδια για τον ορισμό των απαιτήσεων και των κανόνων ασφαλείας για τις οντότητες που υπάγονται στο πεδίο εφαρμογής της Οδηγίας NIS.
- Συνεργάζεται με τις αρμόδιες Ανεξάρτητες και Ρυθμιστικές Αρχές (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών), τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency for Network and Information Security, ENISA) και ακαδημαϊκούς φορείς
- Είναι αρμόδια για τη διασφάλιση της δυνατότητας παροχής των υπαγόμενων στο πεδίο εφαρμογής της Οδηγίας NIS οντοτήτων στο αποδεκτό και προσυμφωνημένο επίπεδο, μετά την εκδήλωση περιστατικών ασφαλείας
- Συνεργάζεται με τις συναρμόδιες για την Κυβερνοασφάλεια αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο
- Συμβάλλει στην ενίσχυση της επιστημονικής έρευνας και ανάπτυξης καινοτόμων υπηρεσιών, εφαρμογών και εξοπλισμού
- Προάγει δράσεις εκπαίδευσης – επιμόρφωσης, ενημέρωσης και ευαισθητοποίησης για θέματα κυβερνοασφάλειας

Περαιτέρω με βάση την Οδηγία NIS η οποία ενσωματώθηκε στο εθνικό μας δίκαιο με τις διατάξεις του ν. 4577/2018 (Α’ 199) και της υ.α. υπ’ αριθμ. 1027/2019 (Β’ 3739), ως αρμοδιότητες της Εθνικής Αρχής Κυβερνοασφάλειας προβλέπονται:

- Να παρακολουθεί την εφαρμογή του Νόμου
- Να ορίζει τις απαιτήσεις για την εφαρμογή μιας Ενιαίας Πολιτικής Ασφάλειας
- Να λειτουργεί ως εθνικό σημείο επαφής για την ασφάλεια συστημάτων δικτύου και πληροφοριών, με καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών-μελών, καθώς και με τις Αρμόδιες Αρχές άλλων κρατών-μελών στο πλαίσιο των μηχανισμών συνεργασίας,
- Να συνεργάζεται με την αρμόδια CSIRT, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του παρόντος νόμου,
- Επιπλέον, δύναται να διενεργεί ελέγχους, στις εγκαταστάσεις, στον τεχνικό εξοπλισμό και στις τεχνολογικές υποδομές των υπαγόμενων στο πεδίο εφαρμογής της Οδηγίας NIS οντοτήτων. Οι έλεγχοι διενεργούνται είτε σε τακτική βάση ή εκτάκτως και βάσει των διαπιστούμενων παραβάσεων να εισηγείται στον Υπουργό Ψηφιακής Διακυβέρνησης, την επιβολή τη λήψη συγκεκριμένων διορθωτικών μέτρων εντός τακτού χρονικού διαστήματος, καθώς και διοικητικές κυρώσεις

Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών («αρμόδια CSIRT»), η οποία καλύπτει τους τομείς του Παραρτήματος Ι και τις υπηρεσίες του Παραρτήματος ΙΙ, και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, είναι η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ.

2. Ειδικά σε σχέση με τη διαχείριση των θεμάτων ασφάλειας των συστημάτων ΤΠΕ του δημοσίου, σας ενημερώνουμε ότι σύμφωνα με το πλαίσιο των διατάξεων του άρθρου 25 παρ. 2 του π.δ. 40/2020 η Γενική Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης (Γ.Γ.Π.Σ.Δ.Δ.) είναι (μεταξύ άλλων) αρμόδια για: «*(ϑ) τη σχεδίαση και την ανάπτυξη του πλαισίου ασφαλείας πληροφοριακών συστημάτων του τομέα αρμοδιότητάς της και ιδίως του Υπουργείου Ψηφιακής Διακυβέρνησης, του Υπουργείου Οικονομικών και των πληροφοριακών συστημάτων που φιλοξενούνται στις υπολογιστικές υποδομές του Υπουργείου Ψηφιακής Διακυβέρνησης. Το πλαίσιο ασφάλειας και ο τρόπος εφαρμογής του συνδιαμορφώνονται σε συνεργασία με αρμόδιες οργανικές μονάδες ασφάλειας πληροφοριακών συστημάτων των συνεργαζόμενων φορέων*».

Ακόμη, σύμφωνα με το άρθρο 27 του ιδίου π.δ. 40/2020, το Αυτοτελές Τμήμα Ασφάλειας της Γ.Γ.Π.Σ.Δ.Δ. έχει τις εξής αρμοδιότητες: « *(α) τη μέριμνα για τη σχεδίαση και ανάπτυξη του πλαισίου ασφαλείας πληροφοριακών συστημάτων των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών, καθώς και των πληροφοριακών συστημάτων άλλων φορέων που φιλοξενούνται στις κεντρικές υπολογιστικές υποδομές του Υπουργείου Ψηφιακής Διακυβέρνησης, με τους οποίους υπάρχει συμφωνία συνεργασίας/επιπέδου εξυπηρέτησης ή άλλο κείμενο στο οποίο προβλέπεται η παροχή υπηρεσιών ασφάλειας, συμπεριλαμβανομένης της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (Α.Α.Δ.Ε.). Στις προαναφερόμενες περιπτώσεις, το πλαίσιο ασφάλειας και ο τρόπος εφαρμογής του συνδιαμορφώνονται σε συνεργασία με αρμόδιες οργανικές μονάδες ασφάλειας πληροφοριακών συστημάτων των φορέων αυτών, (β) τη μέριμνα για τη σχεδίαση κατευθυντήριων γραμμών για το πλαίσιο ασφάλειας πληροφοριακών συστημάτων των φορέων της Δημόσιας Διοίκησης και τη λήψη των απαραίτητων τεχνικών και οργανωτικών μέτρων για την προστασία των δεδομένων, σε συνεργασία και με τις άλλες οργανικές μονάδες του Υπουργείου Ψηφιακής Διακυβέρνησης, (γ) την καθοδήγηση και υποστήριξη των οργανικών μονάδων των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών, καθώς και των Ομάδων και Επιτροπών για την ορθή εφαρμογή του πλαισίου ασφαλείας, …(δ) τη διαχείριση περιστατικών ασφαλείας που καταγράφονται και γνωστοποιούνται στα Υπουργεία Ψηφιακής Διακυβέρνησης και Οικονομικών. Για περιστατικά ασφαλείας τα οποία άπτονται αρμοδιότητας φορέων που φιλοξενούνται και υποστηρίζονται από το Υπουργείο Ψηφιακής Διακυβέρνησης (συμπεριλαμβανομένης της Α.Α.Δ.Ε.), η έρευνα και διαχείριση των περιστατικών διενεργείται από τις αρμόδιες οργανικές μονάδες ασφαλείας αυτών, ενώ η τελική αναφορά περιστατικού συντάσσεται από το Αυτοτελές Τμήμα Ασφάλειας, (ε) τη σχεδίαση και έγκριση διαδικασιών και λοιπών μέτρων ασφαλείας, συμπεριλαμβανομένων και των διαδικασιών και μέτρων φυσικής ασφάλειας, που απαιτούνται από το εφαρμοζόμενο πλαίσιο ασφάλειας, σε συνεργασία με τις εμπλεκόμενες οργανικές μονάδες των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών ή με τις οργανικές μονάδες ασφάλειας άλλων φορέων στην περίπτωση φιλοξενούμενων πληροφοριακών συστημάτων, (στ) την αποκλειστική παροχή πληροφοριών που προκύπτουν από τα αρχεία καταγραφής των πληροφοριακών συστημάτων αρμοδιότητας των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών σε αρμόδια άτομα ή Αρχές στα οποία επιτρέπεται βάσει του ισχύοντος νομικού πλαισίου η αποκάλυψη*

τέτοιων πληροφοριών στο πλαίσιο υπηρεσιακών τους υποθέσεων. Ομοίως, την αποκλειστική συνδρομή σε θέματα ασφάλειας πληροφοριακών συστημάτων και δεδομένων σε αρμόδιες οργανικές μονάδες φορέων που φιλοξενούνται και υποστηρίζονται από το Υπουργείο Ψηφιακής Διακυβέρνησης, στο πλαίσιο διερεύνησης περιστατικών ασφαλείας ή διενέργειας εσωτερικών ελέγχων… (η) τη μέριμνα για την τήρηση του πλαισίου ασφάλειας στο πλαίσιο διενέργειας αλλαγών στα συστήματα αρμοδιότητας των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών, καθώς και τη συμμόρφωση των σχετικών σχεδιαζόμενων τεχνικών λύσεων που προτείνονται από οργανικές μονάδες των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών σύμφωνα με τα οριζόμενα στο εφαρμοζόμενο πλαίσιο ασφάλειας, (θ) την παρακολούθηση και τον συντονισμό δράσεων ανάλυσης επικινδυνότητας και αξιολόγησης ασφάλειας συστημάτων αρμοδιότητας των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών, που εκτελούνται από εξειδικευμένους εξωτερικούς συνεργάτες… (ια) τον κεντρικό συντονισμό έργων μεγάλης κρισιμότητας ως προς την ασφάλεια πληροφοριακών συστημάτων, πρωτίστως έργων αναβάθμισης της ασφάλειας των Υπουργείων Ψηφιακής Διακυβέρνησης και Οικονομικών …»

3. Περαιτέρω, σύμφωνα με τις διατάξεις του άρθρου 2 παρ. 5 του π.δ. 1/2017 (Α' 2), σας ενημερώνουμε ότι η Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT) της Ε.Υ.Π. είναι αρμόδια, εντός του εθνικού πλέγματος Κυβερνοασφάλειας που καθορίζει η Εθνική Αρχή Κυβερνοασφάλειας, για τις κυβερνοεπιθέσεις εναντίον των δημοσίων φορέων της χώρας, που δεν εμπίπτουν στην αρμοδιότητα της Διεύθυνσης Κυβερνοάμυνας του Γ.Ε.ΕΘ.Α. (CSIRT). Ειδικότερα, υποστηρίζει την Προεδρία της Κυβέρνησης και τα Υπουργεία, με εξαίρεση το Υπουργείο Εθνικής Άμυνας, για την πρόληψη, την έγκαιρη προειδοποίηση και την αντιμετώπιση κυβερνοεπιθέσεων, εναντίον τους.

Ακολουθώντας πλήρως το ανωτέρω πλαίσιο, για την περίπτωση των διαπιστωμένων ευπαθειών στις εν λόγω ιστοσελίδες, η Εθνική Αρχή Κυβερνοασφάλειας λειτούργησε ως ακολούθως:

I. Ενημέρωση και ενέργειες της Εθνικής Αρχής Κυβερνοασφάλειας σε σχέση με την περίπτωση του e-ΕΦΚΑ

Στις 7.04.2021 η Αρχή έλαβε ενημέρωση μέσω ηλεκτρονικού ταχυδρομείου από το Αυτοτελές Τμήμα Ασφάλειας της Γενικής Γραμματεία Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης, σχετικά με αναρτημένο στο διαδίκτυο άρθρο που ισχυριζόταν πως μέσω κρίσιμης ευπάθειας που εμφανίζει η ιστοσελίδα του Ηλεκτρονικού Εθνικού Φορέα Κοινωνικής Ασφάλισης ΕΦΚΑ-(ΙΚΑ) δύναται να αποκτηθεί πρόσβαση σε προσωπικά δεδομένα. Προβήκαμε σε άμεση ενημέρωση του Εθνικού CERT ως του αρμόδιο CERT για τον δημόσιο τομέα προς ενημέρωση και ενέργειές του.

II. Ενημέρωση και ενέργειες της Εθνικής Αρχής Κυβερνοασφάλειας σε σχέση με την περίπτωση ιστοσελίδας του Υπουργείου Ψηφιακής Διακυβέρνησης

Η Αρχή ενημερώθηκε για το εν λόγω θέμα μέσω της ανάρτησης του θέματος σε σχετική ιστοσελίδα του διαδικτύου. Κατόπιν, προχώρησε σε επικοινωνία με το διαχειριστή, ζήτησε σχετική ενημέρωση και προχώρησε σε σχετικές συστάσεις για την ασφάλεια του ιστοτόπου του Υπουργείου.

Β. Μέτρα αναβάθμισης του Εθνικού Στρατηγικού Σχεδιασμού. Δράσεις στο πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025.

4. Λαμβάνοντας υπόψη την κρισιμότητα και τις εντεινόμενες προκλήσεις του τομέα της κυβερνοασφάλειας για τον ψηφιακό μετασχηματισμό, το Δεκέμβριο του 2020 η Εθνική Αρχή Κυβερνοασφάλειας προχώρησε στην αναβάθμιση του στρατηγικού σχεδιασμού της χώρας, με την έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025 (ΕΣΚ 2020-2025). Η ΕΣΚ 2020-2025 αναπτύσσεται σε πέντε (5) στρατηγικούς και δεκαπέντε (15) ειδικούς στόχους, καθώς και ένα λεπτομερές πλάνο δράσεις με πάνω από πενήντα (50) εμβληματικές δραστηριότητες, δείκτες και χρονοδιαγράμματα. Ανάμεσα σε αυτές, θεμελιώδη προτεραιότητα για την εφαρμογή της ΕΣΚ 2020-2025 συνιστά η ανάπτυξη ενός **ολοκληρωμένου συστήματος διακυβέρνησης του «ελληνικού κυβερνοχώρου»**, το οποίο αποτελεί και τον πρώτο στρατηγικό στόχο της επικαιροποιημένης στρατηγικής. Στο πλαίσιο αυτού και με γνώμονα τη βελτιστοποίηση της διακυβέρνησης και την επαύξηση της κυβερνοασφάλειας συστημάτων και δικτύων του δημοσίου, κρίσιμη δράση συνιστά η ανάπτυξη ενός **ολοκληρωμένου πλαισίου διαχείρισης της κυβερνοασφάλειας δημοσίων φορέων** (Ειδικός Στόχος 1.Α – Δράση 1.Α.1) προκειμένου να:

- Προλαμβάνονται και αντιμετωπίζονται περιστατικά
- Αξιοποιείται η πιο σύγχρονη τεχνολογία σε δημόσιες υποδομές και υπηρεσίες με ασφαλή τρόπο
- Διαχέεται άμεσα και έγκαιρα η γνώση για τρόπους θωράκισης συστημάτων δικτύου και πληροφοριών

5. Επιπλέον, βασικό πυλώνα της κυβερνοασφάλειας αποτελεί η **αξιολόγηση των κινδύνων** και η **αποτελεσματική διαχείρισή** τους. Στο πλαίσιο του ίδιου στρατηγικού στόχου προβλέπονται δράσεις για τον αποτελεσματικό σχεδιασμό αποτίμησης επικινδυνότητας και διαχείρισης έκτακτης ανάγκης (Ειδικός Στόχος 1.Β - Δράσεις 1.Β.2 & 1.Β.3). Υπό το πρίσμα αυτό καίρια δράση συνιστά η εκπόνηση μελέτης αποτίμησης επικινδυνότητας σε εθνικό επίπεδο που θα οδηγεί στον καθορισμό ενός σχεδίου προστασίας των κρίσιμων υποδομών ανά τομέα ή/και ανά φορέα. Η μελέτη θα λαμβάνει υπόψη της όλες τις πιθανές απειλές, ιδιαίτερα αυτές που σχετίζονται με κακόβουλες ενέργειες (πχ κυβερνοέγκλημα, κυβερνοεπιθέσεις), αλλά και τους κινδύνους που σχετίζονται με φυσικά φαινόμενα, τεχνικές αστοχίες ή δυσλειτουργίες και ανθρώπινα λάθη. Επίσης, θα ληφθούν υπόψη οι απειλές που προκύπτουν από την αλληλεξάρτηση των συστημάτων επικοινωνιών και πληροφοριών των φορέων που συμμετέχουν στην Εθνική Στρατηγική και ιδιαίτερα των κρίσιμων υποδομών, ενώ περαιτέρω θα αξιολογείται η έκταση και η κρισιμότητα των επιπτώσεων σε εθνικό επίπεδο. Παράλληλα, το Εθνικό Σχέδιο Έκτακτης Ανάγκης θα αποτελεί τον οδηγό για την αντιμετώπιση συμβάντων που κρίνονται ως σοβαρές διαταράξεις για τις παρεχόμενες από τους Φορείς υπηρεσίες και υπάγεται στη σφαίρα της διαχείρισης κρίσεων.

6. Παράλληλα, για την **ενδυνάμωση του δημοσίου τομέα**, στο πλαίσιο του Στρατηγικού Στόχου 3 «Βελτιστοποίηση Διαχείρισης Περιστατικών, Καταπολέμησης Του Κυβερνοεγκλήματος και Προστασία της Ιδιωτικότητας» και συγκεκριμένα του ειδικού στόχου 3.Α «**Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων**» υλοποιούνται οι ακόλουθες δράσεις:

- η λειτουργία **συστήματος προστασίας κυβερνητικών ιστοτόπων** - Δράση 3.Α.5,

- η ανάπτυξη προγράμματος **παρακολούθησης και αξιολόγησης επιπέδου ασφάλειας ελληνικού κυβερνοχώρου** (threat intelligence tool) – Δράση 3.Α.6,
- η εγκατάσταση και παραμετροποίηση **open source εργαλείου συστήματος αυτόματης ειδοποίησης για την διαθεσιμότητα των ιστοτόπων και των δικτυακών συσκευών** – Δράση 3.Α.7
- η **εγκατάσταση open source πλατφόρμας για vulnerability assessment και διενέργεια ελέγχων παρείσδυσης** (Penetration tests) – Δράση 3.Α.8

7. Περαιτέρω, στο πλαίσιο μιας ολιστικής προσέγγισης που ακολουθεί η ΕΣΚ 2020-2025, τονίζεται ότι η προστασία των προσωπικών δεδομένων των Ελλήνων πολιτών, προϋποθέτει τη **συμμετρική θωράκιση από κυβερνοαπειλές τόσο των δημόσιων όσο και των ιδιωτικών φορέων**. Η ισχυρή προστασία των δημόσιων πληροφοριακών συστημάτων και βάσεων δεδομένων είναι κενή νοήματος, αν δεν συνυπάρχει με την ύπαρξη εγγυήσεων και την ισχυρή προστασία των συστημάτων ιδιωτικών φορέων, οι οποίοι συγκεντρώνουν ευρύτατο πλήθος σημαντικών για το κοινωνικό σύνολο υπηρεσιών και ευαίσθητων προσωπικών δεδομένων. Σύμφωνα με το ανωτέρω πλαίσιο, η ΕΣΚ 2020 – 2025, ακολουθώντας τις κατευθύνσεις της υπό διαμόρφωση ευρωπαϊκής και της εθνικής νομοθεσίας για την ασφάλεια του διαδικτύου, προσεγγίζει το ζήτημα της αποτελεσματικής προστασίας των συστημάτων ΤΠΕ και των προσωπικών δεδομένων που τηρούνται σε αυτά ως ζήτημα ισόρροπής ανάπτυξης της κυβερνοανθεκτικότητας των δημόσιων και ιδιωτικών φορέων, μέσω της κινητοποίησης ευρωπαϊκών και εθνικών πόρων.

Ειδικότερα, η επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας, σύμφωνα με τους στρατηγικούς στόχους 4. «Ένα σύγχρονο **επενδυτικό περιβάλλον** με έμφαση στην προαγωγή της **Έρευνας και της Ανάπτυξης**» και 5. «Ανάπτυξη **ικανοτήτων**, προαγωγή της **ενημέρωσης και ευαισθητοποίησης**», συνδέεται άρρηκτα με την παροχή κινήτρων για τη διενέργεια επενδύσεων στην ανάπτυξη τεχνολογικών υποδομών και την προώθηση της καινοτομίας, των κατάλληλων οργανωτικών συστημάτων πρόληψης και αντιμετώπισης κυβερνοαπειλών, καθώς και για την ανάπτυξη ικανοτήτων (capacity building) των εργαζομένων και την ενημέρωση των πολιτών για τους κινδύνους της χρήσης του διαδικτύου και τις ενδεδειγμένες πρακτικές που θα πρέπει να ακολουθούν οι ίδιοι για την προστασία των δεδομένων τους. Η αναγκαιότητα διενέργειας επενδύσεων στον τομέα της κυβερνοασφάλειας, έχει αποτυπωθεί στα προγράμματα εργασίας του προγράμματος «Ψηφιακή Ευρώπη» (Digital Europe Program), της Διευκόλυνσης «Συνδέοντας την Ευρώπη» (Connecting Europe Facility) και του «Ταμείου Ανάκαμψης και Ανθεκτικότητας» (Recovery and Resilience Fund), το οποίο χρηματοδοτεί την υλοποίηση των σχετικών δράσεων του Εθνικού Σχεδίου Ανάκαμψης και Ανθεκτικότητας «Ελλάδα 2.0» (βλ. «Άξονα 2.2: Ψηφιακός Μετασχηματισμός του Κράτους» και ειδικότερα τη δράση «Επένδυση στην βελτίωση της Κυβερνοασφάλειας στο Δημόσιο & Δημιουργία Εθνικού Κέντρου Κυβερνοασφάλειας με προϋπολογισμό 32 εκατ. ευρώ). Ακόμη, η υλοποίηση των δράσεων "European Cybershield" και "Support to Implementation of relevant EU Legislation" του Προγράμματος «Ψηφιακή Ευρώπη», θα γίνει υπό την έμμεση διαχείριση του νεότευκτου Ευρωπαϊκού Κέντρου Ικανοτήτων για Βιομηχανικά, Τεχνολογικά και

Ερευνητικά Θέματα Κυβερνοασφάλειας[1] και του δικτύου εθνικών κέντρων συντονισμού (ECCC), τα οποία θα οριστούν κατά το προσεχές διάστημα από τις αρμόδιες αρχές των κρατών μελών.

Γ. Στελέχωση της Εθνικής Αρχής Κυβερνοασφάλειας.

8. Η Εθνική Αρχή Κυβερνοασφάλειας συστάθηκε ως οργανική μονάδα επιπέδου Γενικής Διεύθυνσης με τις διατάξεις του ν. 4635/2019 (Α' 167). Στο πλαίσιο αυτό υλοποιείται προσπάθεια στελέχωσης αυτής με εξειδικευμένο ανθρώπινο δυναμικό. Σύμφωνα με τη με αριθμ. πρωτ. 10630 ΕΞ 2021/09.04.2021 (Β' 1606) απόφαση της Υπηρεσιακής Γραμματέως του Υπουργείου Ψηφιακής Διακυβέρνησης, οι οργανικές θέσεις που προβλέπονται για την Γενική Διεύθυνση Κυβερνοασφάλειας είναι πενήντα επτά (57) και μέχρι σήμερα έχουν στελεχωθεί είκοσι τέσσερις (24), οι οποίες κατανέμονται ως εξής:

- **Γενικός Διευθυντής Κυβερνοασφάλειας:** 1
- Στη **Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας** προβλέπονται δεκαεπτά (17) θέσεις από τις οποίες έχουν στελεχωθεί οι δέκα (10)

Προϊστάμενος Διεύθυνσης: 1| Τμήμα Στρατηγικού Σχεδιασμού: 3| Τμήμα Κανονιστικής Συμμόρφωσης: 4|

Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφαλείας: 1|Τμήμα Κυβερνητικής Δορυφορικής Υπηρεσίας: 1

- Στη **Διεύθυνση Πρόληψης και Προστασίας** προβλέπονται δεκαπέντε (15) θέσεις από τις οποίες έχουν στελεχωθεί οι πέντε (5)

Τμήμα Εποπτείας και Ελέγχου: 2|Τμήμα Ασφαλείας Λογισμικού & Αγαθών Ασφαλείας (Information Assets): 1|Τμήμα Ασφαλείας Υποδομών – Δικτύου: 2

- Στη **Διεύθυνση Επιχειρησιακής Συνέχειας** προβλέπονται έντεκα (11) θέσεις από τις οποίες έχουν στελεχωθεί οι δύο (2)

Τμήμα Ανάλυσης και Παρακολούθησης Απειλών - Περιστατικών Ασφαλείας: 1|Τμήμα Σχεδιασμού Αποκατάστασης: 1

- Στη **Διεύθυνση Συντονισμού Φορέων** προβλέπονται δεκατρείς (13) θέσεις από τις οποίες έχουν στελεχωθεί οι έξι (6)

Προϊστάμενος Διεύθυνσης: 1|Τμήμα Συντονισμού CISO Φορέων: 2 |Τμήμα Διεθνών Θεμάτων και Συνεργασιών: 2 |Τμήμα Εκπαίδευσης και Υποστήριξης: 1

Δ. Στελέχωση θέσης Γενικού Διευθυντή Κυβερνοασφάλειας

9. Σύμφωνα με τις διατάξεις του άρθρου 50 του ν. 4635/2019 στη θέση του Προϊσταμένου της Γενικής Διεύθυνσης Κυβερνοασφάλειας επιλέγεται και τοποθετείται υπάλληλος από το πάσης φύσεως προσωπικό του δημοσίου τομέα, όπως ορίζεται στην παράγραφο 1 του άρθρου 14 του ν. 4270/2014 (Α'

[1]Κείμενο του υπό υιοθέτηση Κανονισμού: https://data.consilium.europa.eu/doc/document/ST-5628-2021-INIT/en/pdf

143), από την Εθνική Υπηρεσία Πληροφοριών, από το ένστολο ή πολιτικό προσωπικό των Υπηρεσιών που υπάγονται στο Υπουργείο Εθνικής Άμυνας, στο Υπουργείο Προστασίας του Πολίτη και στο Λιμενικό Σώμα του Υπουργείου Ναυτιλίας και Νησιωτικής Πολιτικής ή σε εποπτευόμενους από αυτά φορείς, καθώς και από καθηγητές ΑΕΙ, κατά παρέκκλιση του άρθρου 24 του ν. 4009/2011 (Α' 195). Η επιλογή γίνεται μετά την εκδήλωση ενδιαφέροντος από τους υποψηφίους με σχετική αίτηση τους προς το Υπουργείο Ψηφιακής Διακυβέρνησης, μετά τη δημοσίευση δημόσιας πρόσκλησης για την κάλυψη της θέσης αυτής κατόπιν εισήγησης τριμελούς Επιτροπής, η οποία αποτελείται από τον Γενικό Γραμματέα Τηλεπικοινωνιών και Ταχυδρομείων, τον Υπηρεσιακό Γραμματέα του Υπουργείου Ψηφιακής Διακυβέρνησης και τον Γενικό Γραμματέα Ανθρωπίνου Δυναμικού Δημοσίου Τομέα του Υπουργείου Εσωτερικών και ορίζεται με απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης.

Παράλληλα, ο Προϊστάμενος της Γενικής Διεύθυνσης Κυβερνοασφάλειας και οι προϊστάμενοι των οργανικών μονάδων αυτής πρέπει να διαθέτουν, κατ' ελάχιστον, τα ακόλουθα τυπικά και ουσιαστικά προσόντα: α) Πτυχίο Α.Ε.Ι. της ημεδαπής ή ισότιμο σχολών της αλλοδαπής, σύμφωνα με τις διατάξεις του άρθρου 3 του π.δ. 50/2001 (Α' 39) όπως ισχύει, β) Επιστημονική εξειδίκευση στο γνωστικό αντικείμενο της οικείας θέσης ή συναφή με τα καθήκοντα αυτής ή/και τις αρμοδιότητες της αντίστοιχης οργανικής μονάδας, που αποδεικνύεται κατά τις διατάξεις της περίπτωσης β' της παραγράφου 1 του άρθρου 2 του π.δ. 50/2001, όπως ισχύει, γ) Άριστη γνώση της Αγγλικής Γλώσσας, σύμφωνα με τις διατάξεις του άρθρου 28 του π.δ. 50/2001, όπως ισχύει, δ) Επαγγελματική εμπειρία συναφή με τα καθήκοντα της θέσης ή/και με τις αρμοδιότητες της Γενικής Διεύθυνσης Κυβερνοασφάλειας. Για την επιλογή και τοποθέτηση συνεκτιμώνται τα ουσιαστικά προσόντα, η ποιότητα της υπηρεσιακής δραστηριότητάς, και οι εν γένει διοικητικές ικανότητες, ενώ τα στοιχεία αυτά αναφέρονται στην έκθεση αξιολόγησης που συντάσσεται για τον κάθε υποψήφιο.

10. Το ανωτέρω πλαίσιο στελέχωσης της θέσης του επικεφαλής της Εθνικής Αρχής Κυβερνοασφάλειας, ήτοι του Γενικού Διευθυντή Κυβερνοασφάλειας, ανταποκρίνεται σε ένα **ειδικό περιβάλλον απαιτήσεων, δεσμεύσεων και υποχρεώσεων**, προσιδιάζει στη φύση των αρμοδιοτήτων της Εθνικής Αρχής Κυβερνοασφάλειας, και ιδίως στη διαχείριση ευαίσθητων και διαβαθμισμένων πληροφοριών, θεμάτων που αφορούν ουσιώδη εθνικά συμφέροντα, αλλά και συνεργασίες με την Εθνική Υπηρεσία Πληροφοριών και το Υπουργείο Εθνικής Άμυνας. Είναι άλλωστε ένα πλαίσιο το οποίο, λόγω του ότι παραμένει **ανοιχτό προς στελέχωση από ένστολους υπαλλήλους/μη πολιτικό προσωπικό του κράτους**, **δεν μπορεί να ακολουθεί αποκλειστικά και εξ ολοκλήρου** τις **συνήθεις διαδικασίες** που εφαρμόζονται για τους πολιτικούς διοικητικούς υπαλλήλους, δυνάμει των **διατάξεων του Υπαλληλικού Κώδικα (ν.3528/2007, Α' 26)**.

Ε. Πρωτοβουλίες και εξελίξεις

11. Με την πρόταση της Επιτροπής «σχετικά με τα μέτρα για ένα υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148» (πρόταση Οδηγίας NIS 2.0) επίκεινται εκτεταμένες αλλαγές, οι οποίες αναμένεται να επηρεάσουν τον τρόπο άσκησης της δημόσιας πολιτικής κυβερνοασφάλειας στη χώρα μας, όσο και την ίδια τη λειτουργία της Εθνικής Αρχής Κυβερνοασφάλειας. Με την πρόταση της Οδηγίας NIS 2.0 καταργείται η διάκριση σε ΦΕΒΥ-

ΠΨΥ και εντάσσονται τομείς που προηγουμένως ήταν εκτός πεδίου εφαρμογής, συμπεριλαμβανομένων φορέων της δημόσιας διοίκησης. Επιπλέον, προβλέπονται πολιτικές ανάλυσης κινδύνων και ασφάλειας συστημάτων καθώς και εκτεταμένες διαδικασίες εποπτείας και ελέγχων.

12. Παράλληλα, λαμβάνοντας υπόψη την κρισιμότητα θωράκισης συστημάτων ΤΠΕ στην σύγχρονη ψηφιακή εποχή, η Εθνική Αρχή Κυβερνοασφάλειας έχει επεξεργαστεί ολοκληρωμένο πλαίσιο προτάσεων για την αναβάθμιση του συστήματος διακυβέρνησης της δημόσιας πολιτικής κυβερνοασφάλειας στη χώρα με έμφαση την προστασία των συστημάτων ΤΠΕ του δημοσίου, την ενδυνάμωση της Αρχής, και την ενίσχυση των δυνατοτήτων της χώρας να ανταποκριθεί σε αυξημένες προκλήσεις και κυβερνοαπειλές. Συγχρόνως, η Εθνική Αρχή Κυβερνοασφάλειας έχει εκπονήσει εμπεριστατωμένο και ολοκληρωμένο εγχειρίδιο (handbook) το οποίο πρόκειται να διανεμηθεί το προσεχές διάστημα. Στο πλαίσιο υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025 και συγκεκριμένα στο πλαίσιο της Δράσης 1.Α.2: «Ανάπτυξη πλαισίου προαγωγής της αριστείας στον τομέα της κυβερνοασφάλειας (cybersecurity excellence management framework)» έχει ολοκληρωθεί in-house η σύνταξη Εγχειριδίου Κυβερνοασφάλειας (Cybersecurity Handbook). Το εγχειρίδιο αποτελεί έναν οδηγό με βέλτιστες πρακτικές σε τεχνικά και οργανωτικά μέτρα για την προστασία και ανθεκτικότητα των πληροφοριακών συστημάτων του Δημόσιου Τομέα της Χώρας, καθώς και των μεσαίων και μεγάλων επιχειρήσεων του Ιδιωτικού Τομέα. Διαρθρώνεται σε δεκαοκτώ (18) θεματικές ενότητες, όπου κάθε μία αποτελεί μία οικογένεια μέτρων προστασίας. Σε κάθε θεματική ενότητα περιγράφονται οι κίνδυνοι από τη μη εφαρμογή του μέτρου και αναπτύσσονται εξειδικευμένα μέτρα προστασίας (sub-controls) με τη μορφή εστιασμένων ενεργειών εφαρμογής του μέτρου σε συγκεκριμένες λειτουργίες και τύπους συστημάτων. Με το Εγχειρίδιο Κυβερνοασφάλειας η Εθνική Αρχή Κυβερνοασφάλειας φιλοδοξεί να παράσχει έναν εύληπτο και πρακτικό οδηγό για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και πληροφοριών των Φορέων τόσο του δημόσιου όσο και του ιδιωτικού τομέα.

Το εγχειρίδιο στηρίζεται σε ευρέως γνωστά και διεθνώς αποδεκτά πρότυπα και οδηγίες και έχει σκοπό να βελτιώσει την ικανότητα των Οργανισμών να ανθίστανται επαρκώς απέναντι στις σύγχρονες απειλές, να ανταποκρίνονται σε περιστατικά κυβερνοεπιθέσεων με τις κατά το δυνατόν ελάχιστες επιπτώσεις και να προστατεύουν τα κρίσιμα συστήματα, τις προσφερόμενες υπηρεσίες τους, καθώς και τα επιχειρησιακά και προσωπικά δεδομένα που τηρούν και επεξεργάζονται.

Παραμένουμε στη διάθεσή σας για κάθε σχετικό θέμα.

Ο Προϊστάμενος της Διεύθυνσης

Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας

Ι. Αλεξάκης

Εσωτερική διανομή:

1. ΓΔ Κυβερνοασφάλειας

2. Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας/ Τμήμα Α’, Τμήμα Β’