



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΤΜΗΜΑ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΤΜΗΜΑ ΚΑΝΟΝΙΣΤΙΚΗΣ ΣΥΜΜΟΡΦΩΣΗΣ
Ταχ. Δ/ση: Χανδρή 1 & Θεσ/κης
ΤΚ: 18346 Μοσχάτο Αττικής
Πληροφορίες: Μ. Πατσουράκης, Κ. Ρώτας
Τηλ.: 210 4802385, 2060
E-mail: dir.strategy.ncsa@mindigital.gr

Προς: Υπηρεσία Συντονισμού
Γραφείο Νομικών και Κοινοβουλευτικών
Θεμάτων

Κοιν:

- Γραφείο κ. Υπουργού Επικρατείας
- Γραφείο κ. Γενικού Γραμματέα
Τηλεπικοινωνιών και Ταχυδρομείων

Θέμα: Απάντηση σε ερώτηση κοινοβουλευτικού ελέγχου

Σχετ.:

1. Το υπ' αριθμ. πρωτ. 40445 ΕΞ 2021/15.11.2021 έγγραφο της Υπηρεσίας σας
2. Η υπ' αρ. 1156/13.11.2021 Αναφορά των βουλευτών κ.κ. Γ. Καμίνη και Α. Αντωνίου με θέμα: «Τηλεφωνικές απάτες εις βάρος πολιτών και η ανάγκη συντονισμένης κυβερνητικής δράσης για την αντιμετώπισή τους»

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:

1. Σύμφωνα με τις διατάξεις του π.δ. 40/2020 (Α' 85) η Γενική Διεύθυνση Κυβερνοασφάλειας έχει, μεταξύ άλλων, ως στρατηγικό στόχο τη χάραξη 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. Περαιτέρω, η Γενική Διεύθυνση Κυβερνοασφάλειας αποτελεί την Εθνική Αρχή Κυβερνοασφάλειας που έχει οριστεί κατά τις διατάξεις του ν. 4577/2018 (Α' 199) με αποστολή να διαμορφώνει την πολιτική κυβερνοασφάλειας σε συνεργασία με τις συναρμόδιες για την κυβερνοασφάλεια αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο για την επίτευξη των εθνικών στόχων ως προς τη διασφάλιση του υψηλού επιπέδου κυβερνοασφαλείας, και την προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών, σε συμμόρφωση με τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων, (ΓΚΠΔ) (ΕΕL 119, 04.05.2016).

Στο πλαίσιο αυτό, η Γενική Διεύθυνση Κυβερνοασφάλειας συνεργάζεται:

α) με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.), που είναι η καθ' ύλην αρμόδια, συνταγματικά κατοχυρωμένη, Ανεξάρτητη Διοικητική Αρχή, η οποία έχει ως αποστολή της

την εποπτεία της εφαρμογής του ΓΚΠΔ, και της εθνικής νομοθεσίας για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα,

β) με την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) σε θέματα που αφορούν θέματα ασφάλειας και διαφύλαξης του απορρήτου σε θέματα τηλεπικοινωνιών,

γ) με το CSIRT της ΔΙΚΥΒ/ΓΕΕΘΑ και το Εθνικό CERT της ΕΥΠ σε θέματα συμβάντων κυβερνοασφάλειας, και

δ) με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ. σε θέματα πάταξης του κυβερνοεγκλήματος.

2. Αναγνωρίζοντας τις αυξανόμενες προκλήσεις των τελευταίων ετών, ιδίως στο πλαίσιο της εντεινόμενης χρήσης των ψηφιακών υποδομών, μέσων και εφαρμογών λόγω της πανδημίας COVID-19, η Γενική Διεύθυνση Κυβερνοασφάλειας προχώρησε στην αναμόρφωση του εθνικού στρατηγικού σχεδιασμού για την κυβερνοασφάλεια, με την έγκριση της νέας Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025 (υ.α. υπ' αριθμ. 34368/7.12.2020, ΑΔΑ: 61ΒΕ46ΜΤΛΠ-ΦΜ5). Η Εθνική Στρατηγική Κυβερνοασφάλειας 2020 – 2025, πλήρως ευθυγραμμισμένη με τις σύγχρονες διεθνείς και ευρωπαϊκές πρακτικές, αναπτύσσεται σε μία ευρεία δέσμη στρατηγικών στόχων εκφράζοντας την αναγκαιότητα για διαρκή προσαρμογή, πρόληψη και έγκαιρη αντίδραση στις προκλήσεις ενός συνεχώς μεταβαλλόμενου διασυνδεδεμένου ψηφιακού περιβάλλοντος, στοχεύοντας στην προστασία των θεμελιωδών δικαιωμάτων (ιδίως της προστασίας των προσωπικών δεδομένων, της ιδιωτικότητας, της προσωπικότητας, της ισότητας), την πάταξη του κυβερνοεγκλήματος και την ανάπτυξη κουλτούρας ασφαλούς χρήσης, υπό την έννοια της ψηφιακής παιδείας, της διαρκούς ενημέρωσης και ευαισθητοποίησης στους κινδύνους και τις παγίδες των νέων τεχνολογιών.

3. Η πάταξη του κυβερνοεγκλήματος, η προστασία της εμπιστευτικότητας των πληροφοριών και των προσωπικών δεδομένων, και κατ' επέκταση η προστασία και η διαφύλαξη της εμπιστοσύνης του κοινωνικού συνόλου έναντι των απατηλών συμπεριφορών του κυβερνοχώρου μέσω της αξιοποίησης της κοινωνικής μηχανικής (social engineering), όσο και χρήσης εργαλείων υφαρπαγής κωδικών πρόσβασης ("phishing", "smishing", "vishing" κ.λπ.) συνιστά στρατηγική προτεραιότητα. Ήδη η Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025: α. αναγνωρίζει τις εν λόγω απειλές ανάμεσα στα σημαντικότερες μορφές απειλών από πλευράς στρατηγικού σχεδιασμού, υιοθετώντας συγχρόνως και τις πρόσφατες εκθέσεις του Ευρωπαϊκού Οργανισμού για την Κυβερνοασφάλεια (ENISA), και β. συγκαταλέγει τους κυβερνοεγκληματίες (cybercriminals) ανάμεσα στους σημαντικότερους κακόβουλους δρώντες του κυβερνοχώρου. Ειδικότερα, λαμβάνοντας υπόψη το ανωτέρω πλαίσιο και σχετικά με τα ειδικά μέτρα και δράσεις που υλοποιούνται στο πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025, τονίζονται τα εξής:

α. Σε πρώτο επίπεδο, υπό τον ειδικό στόχο 3.Α. «Βελτιστοποίηση μεθόδων, τεχνικών και εργαλείων ανάλυσης, απόκρισης και κοινοποίησης συμβάντων», προβλέπεται ως δράση η συγκρότηση κεντρικού συντονιστικού μηχανισμού για τη διαχείριση αναφορών στο πλαίσιο του ΓΚΠΔ και της NISD (δράση 3.Α.11.).

β. Ακόμη, υπό τον ειδικό στόχο 3.Β. «Ενδυνάμωση μηχανισμών αποτροπής και βελτιστοποίηση της επιχειρησιακής συνεργασίας προβλέπονται ως εμβληματικές δραστηριότητες:

- Η ανάπτυξη δικτύου ενισχυμένης συνεργασίας για την καταπολέμηση του κυβερνοεγκλήματος (δράση 3.Β.1.)

- Η επεξεργασία συνολικής πρότασης για το κυρωτικό πλαίσιο της δημόσιας πολιτικής κυβερνοασφάλειας (δράση 3.Β.2.)

- Η δημιουργία και αξιοποίηση σύγχρονων εργαλείων και τεχνικών για την πάταξη του κυβερνοεγκλήματος (δράση 3.Β.3.)

γ. Περαιτέρω, υπό τον ειδικό στόχο 3.Γ. «Κυβερνοασφάλεια και προστασία της ιδιωτικότητας» προβλέπονται ως δράσεις:

- η ανάπτυξη θεσμικής συνεργασίας με τη συγκρότηση μικτής ομάδας συνεργασίας από στελέχη της Γενικής Διεύθυνσης Κυβερνοασφάλειας, της Α.Δ.Α.Ε. και της Α.Π.Δ.Π.Χ. σε θέματα προστασίας της ιδιωτικότητας (δράση 3.Γ.1.), καθώς και

- η ανάπτυξη και παρακολούθηση πλατφόρμας καταγραφής δεδομένων κυβερνοεπιθέσεων που ενέχουν παραβίαση της ιδιωτικότητας (δράση 3.Γ.2.).

4. Με το ανωτέρω πλαίσιο συνεργασιών τόσο σε επίπεδο προστασίας της εμπιστευτικότητας των πληροφοριών και των προσωπικών δεδομένων, όσο και σε επίπεδο πάταξης του κυβερνοεγκλήματος, εδραιώνεται ένας θεμελιώδης μηχανισμός, με βασικές προτεραιότητες όχι μόνο τη θωράκιση των ζωτικών υποδομών και υπηρεσιών από περιστατικά κυβερνοασφάλειας, αλλά και η ενδυνάμωση της αποτρεπτικής ισχύος του κυρωτικού πλαισίου με σκοπό την προστασία της κοινωνίας και της οικονομίας από εγκληματικές συμπεριφορές του κυβερνοχώρου. Άλλωστε, όπως επισημαίνεται στην ίδια την Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, ανάμεσα στα μέτρα που λαμβάνονται στο εν λόγω πλαίσιο, κρίνεται απαραίτητη η ενίσχυση του νομοθετικού πλαισίου και των αρμόδιων υπηρεσιών που επιφορτίζονται με την εφαρμογή του. Καταληκτικά, μέσα από την εδραίωση του εν λόγω πλαισίου συνεργασίας και αξιολόγησης της αποτροπής των κυρωτικών διατάξεων, τίθεται από στρατηγικής πλευράς, ένα ισχυρό έρεισμα για την πάταξη των κακόβουλων ενεργειών του κυβερνοχώρου, ιδίως εν προκειμένω των περιπτώσεων εξαπάτησης που αξιοποιούν συμπεριφορές τόσο κοινωνικής μηχανικής (social engineering), όσο και χρήσης εργαλείων υφαρπαγής κωδικών πρόσβασης (“phishing”, “smishing”, “vishing” κ.λπ.).

5. Ακόμη, στο πλαίσιο της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020-2025, δίνεται ιδιαίτερη έμφαση στην ανάπτυξη της ενημέρωσης και της ευαισθητοποίησης του γενικού πληθυσμού σε θέματα κυβερνοασφάλειας ως κρίσιμου προληπτικού παράγοντα, ιδιαίτερα για την αντιμετώπιση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, αλλά και προστασίας έναντι των απατηλών συμπεριφορών. Η ενημέρωση και εκπαίδευση των πολιτών στη διαχείριση των προσωπικών τους δεδομένων είναι ύψιστης σημασίας, ιδιαίτερα κατά την περιήγησή τους στο διαδίκτυο και τη χρήση των κοινωνικών δικτύων και αποτελεί πρωταρχική δικλείδα ασφαλείας απέναντι στην παράνομη πρόσβαση και επεξεργασία αυτών από κακόβουλους δρώντες. Υπηρετώντας τον ανωτέρω σκοπό, στην Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 έχει συμπεριληφθεί η υλοποίηση ειδικής δέσμης δράσεων στο πλαίσιο του Στρατηγικού Στόχου 5: «Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης» η οποία περιλαμβάνει:

- την ανάπτυξη εξειδικευμένων σχεδίων δράσης για την προαγωγή της εκπαίδευσης, της ενημέρωσης και της ευαισθητοποίησης (βλ. ιδίως δράσεις 5.Β.2., 5.Γ.1.),

- τη δημιουργία και ευρεία διάδοση ενημερωτικού και εκπαιδευτικού υλικού.

6. Σε ό,τι αφορά το θεσμικό πλαίσιο αρμοδιότητας της Υπηρεσίας μας, σας ενημερώνουμε επιπρόσθετα ότι τόσο οι τράπεζες όσο και οι υποδομές χρηματοπιστωτικών αγορών εντάσσονται στους τομείς του παραρτήματος II της ισχύουσας Οδηγίας NIS (Οδηγία (ΕΕ) 1148/2016), ενώ ήδη η Ευρ. Επιτροπή έχει υποβάλει πρόταση έκδοσης (τομεακού – sector specific) κανονισμού «σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014 και (ΕΕ) αριθ. 909/2014» (Πρόταση κανονισμού DORA, COM(2020) 595 final) με σκοπό την ενδυνάμωση των εν λόγω τομέων έναντι των κυβερνοαπειλών.

Κατά τα λοιπά, για ειδικότερα ζητήματα που αφορούν τη δίωξη των εν λόγω παραβατικών συμπεριφορών, αρμόδια είναι Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ., ενώ για θέματα τηλεπικοινωνιών αρμόδιες είναι η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε.) και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.). Τέλος, για τα θέματα που αφορούν την ενίσχυση της ανθεκτικότητας στον χρηματοπιστωτικό τομέα, αρμόδιο είναι το Υπουργείο Οικονομικών και η Τράπεζα της Ελλάδος.

Παραμένουμε στη διάθεσή σας για κάθε σχετικό θέμα.

Ο Διευθυντής Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας

I. Αλεξάκης

Εσωτερική διανομή:

1. ΓΔ Κυβερνοασφάλειας
2. Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας/ Τμήμα Α', Τμήμα Β'