



Μοσχάτο, 14 Μαΐου 2024

Αρ. πρωτ.: ΓΔΕΣ/οικ.1

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΤΕΛΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Δ/νση: Χανδρή 1 και Θεσσαλονίκης
Τ.Κ.: 183 46 Μοσχάτο
Πληροφορίες: Διευθυντής
Τηλ.: 210 4802936
Email: dir.strategy.ncsa@mindigital.gr

ΠΡΟΣ: ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
Υπηρεσία Συντονισμού
Γραφείο Νομικών & Κοινοβουλευτικών
Θεμάτων

Θέμα: Απάντηση σε Ερώτηση Κοινοβουλευτικού ελέγχου υπ' αρ. 4436/19.4.2024

Σχετ.: Το αρ. πρωτ. 14509ΕΞ2024/ΥΨηΔ 23-04-2024 έγγραφο της Υπηρεσίας σας

Σε συνέχεια του ως άνω σχετικού, με το οποίο διαβιβάστηκε στην Υπηρεσία μας η εν θέματι Ερώτηση με θέμα «Κυβερνοασφάλεια και Διαρροές Προσωπικών Δεδομένων», θέτουμε υπόψη σας, κατά λόγο αρμοδιότητας, τα εξής:

1. Νέα Εθνική Αρχή Κυβερνοασφάλειας

Με τον πρόσφατο ν. 5086/2024 «Εθνική Αρχή Κυβερνοασφάλειας και λουπές διατάξεις» (Α'23) το εθνικό σύστημα διακυβέρνησης για τη δημόσια πολιτική κυβερνοασφάλειας ισχυροποιείται και αναβαθμίζεται σημαντικά, ακολουθώντας τις διεθνείς καλές πρακτικές και τα ευρωπαϊκά πρότυπα. Η χώρα μας έχει πλέον αποκτήσει μια σύγχρονη και ενισχυμένη Εθνική Αρχή Κυβερνοασφάλειας (εφεξής Ε.Α.Κ.), η οποία έχει αναβαθμιστεί εκ βάθρων, λειτουργώντας ως νομικό πρόσωπο δημοσίου δικαίου (Ν.Π.Δ.Δ.) υπό την εποπτεία του Υπουργού Ψηφιακής Διακυβέρνησης και αποτελώντας την ενιαία λειτουργική δομή, που αναλαμβάνει το συντονισμό και την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας, στο πλαίσιο των εθνικών αναγκών και των Ενωσιακών δεσμεύσεων της χώρας, ιδίως ενόψει της ενσωμάτωσης της Οδηγίας (ΕΕ) 2022/2555 («Οδηγία NIS 2») στην εθνική έννομη τάξη.

Βασικός σκοπός της νέας Εθνικής Αρχής Κυβερνοασφάλειας (Ε.Α.Κ.) είναι η οργάνωση, ο συντονισμός και η εφαρμογή ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη Χώρα. Αυτό πραγματοποιείται σε επίπεδο στρατηγικό, αλλά και σε επίπεδο επιχειρησιακό και τεχνικό, δηλαδή, πρόληψης, ανίχνευσης, αντιμετώπισης και αποτροπής κυβερνοεπιθέσεων. Για το σκοπό αυτό, ήδη προβλέπεται σχεδόν ο τριπλασιασμός των θέσεων του προσωπικού της, η περαιτέρω οργανωτική της ανάπτυξη, η οποία είχε επιτευχθεί το πρώτον με τις διατάξεις του ν. 4635/2019 και του π.δ. 40/2020, η ενδυνάμωση της αποστολής και των αρμοδιοτήτων της, καθώς και η σημαντική ενίσχυση του προϋπολογισμού της.

Εν προκειμένω, με τη δημιουργία της Εθνικής Αρχής Κυβερνοασφάλειας αλλά και την επικείμενη μεταφορά της Οδηγίας NIS 2 στην εθνική έννομη τάξη, εντός του επόμενου χρονικού διαστήματος και το αργότερο έως τον Οκτώβριο 2024, υλοποιείται ο σχεδιασμός του Υπουργείου Ψηφιακής Διακυβέρνησης, για τη διαρκή αναβάθμιση των εθνικών ικανοτήτων κυβερνοασφάλειας στο σύνολο των κρίσιμων πυλώνων της δημόσιας πολιτικής κυβερνοασφάλειας:

• **Στρατηγικό επίπεδο - διοίκηση και διακυβέρνηση**, το οποίο συμπεριλαμβάνει το σχεδιασμό και εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας, ενισχύοντας στον πυρήνα του το εθνικό μοντέλο διακυβέρνησης για την κυβερνοασφάλεια και διασφαλίζοντας τον αναγκαίο συντονισμό για την αναγνώριση και τον μετριασμό των κινδύνων στον κυβερνοχώρο σε εθνικό επίπεδο. Την ίδια στιγμή ενισχύονται η διαφάνεια και η λογοδοσία στη δημόσια πολιτική κυβερνοασφάλειας, καθώς με το σύνολο της νομοθεσίας για την κυβερνοασφάλεια (ενδεικτικά, ν.4635/2019, υα 1027/2019, ν. 4961/2022 ν. 5002/2022 και, πρόσφατα ν. 5086/2024), από κοινού με την επικείμενη νομοθετική πρωτοβουλία του Υπουργείου Ψηφιακής Διακυβέρνησης για τη μεταφορά της Οδηγίας NIS 2 στην εθνική έννομη τάξη, διαμορφώνεται ένα πιο συνεκτικό ρυθμιστικό πλαίσιο, καθιερώνοντας ρόλους, διαδικασίες αλλά και ενισχυμένες ευθύνες για τις αρμόδιες εθνικές αρχές και το σύνολο των φορέων που είναι υπεύθυνες για τη λειτουργία κρίσιμων υποδομών.

Ταυτόχρονα, δεδομένου του οριζόντιου χαρακτήρα της δημόσιας πολιτικής κυβερνοασφάλειας, έχουν ήδη συσταθεί με το ν. 5002/2022 (Α' 228), οι κατάλληλες συντονιστικές δομές μεταξύ όλων των εμπλεκόμενων Υπηρεσιών, για τη βελτίωση του συντονισμού στην αντιμετώπιση τυχόν εξαιρετικά σοβαρών περιστατικών κυβερνοασφάλειας, τα οποία ενδέχεται, λόγω της φύσης τους, της πολυπλοκότητας αλλά και της διασύνδεσης των πληροφοριακών συστημάτων, να ενέχουν στρατηγικό κίνδυνο.

• **Επιχειρησιακό επίπεδο - Επιχειρησιακές λειτουργίες**, οι οποίες διασφαλίζουν την υλοποίηση της εθνικής στρατηγικής, δίνοντας ιδιαίτερη έμφαση σε κρίσιμες οντότητες του δημόσιου και του ιδιωτικού τομέα. Αναπτύσσονται λειτουργίες και εφαρμόζονται διαδικασίες για την πρόληψη αλλά και το συντονισμό στην αντιμετώπιση απειλών και κυβερνοεπιθέσεων, καθώς και στη διαχείριση περιστατικών ασφαλείας, μεταξύ άλλων, με την πρόβλεψη για τη λειτουργία του Ενοποιημένου SOC, του οποίου η υλοποίηση έχει ήδη εκκινήσει, του Εθνικού Δικτύου SOC του άρθρου 31 του ν. 5002/2022 και της Ομάδας Απόκρισης συμβάντων στον κυβερνοχώρο (CSIRT), σε συνεργασία με τις συναρμόδιες για την κυβερνοασφάλεια αρχές.

• **Τεχνικές λειτουργίες**, οι οποίες διασφαλίζουν την αξιοποίηση νέων τεχνολογιών και εργαλείων, που απαιτούνται για την επίτευξη των στόχων της εθνικής στρατηγικής. Η διαθεσιμότητα εθνικών και ευρωπαϊκών χρηματοδοτικών πόρων είναι κομβικής σημασίας στην εφαρμογή του επενδυτικού σχεδιασμού για την κυβερνοασφάλεια, ιδιαίτερα σε ό,τι αφορά την ανάπτυξη των απαραίτητων τεχνικών υποδομών, την παροχή κινήτρων για την υιοθέτηση τεχνολογιών αιχμής στην κυβερνοασφάλεια και την ανάπτυξη των απαραίτητων τεχνικών ικανοτήτων για την βέλτιστη αξιοποίηση αυτών από δημόσιους και ιδιωτικούς φορείς. Για αυτό τον σκοπό, η Εθνική Αρχή Κυβερνοασφάλειας, συμμετέχει στην υλοποίηση πλήθους εγκεκριμένων συγχρηματοδοτούμενων έργων κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη», σε συνεργασία με ελληνικούς και ευρωπαϊκούς ακαδημαϊκούς ερευνητικούς και ιδιωτικούς φορείς με σκοπό την βελτίωση του τεχνικού επιπέδου και την προαγωγή της διασυννοιακής συνεργασίας και ανταλλαγής πληροφορήσης στον τομέα της κυβερνοασφάλειας.

• **Έλεγχος και εποπτεία** προκειμένου να διασφαλίζεται η κανονιστική συμμόρφωση των οργανισμών και, πρωτίστως, των κρίσιμων υποδομών της χώρας προς τις απαιτήσεις του ευρωπαϊκού και εθνικού νομοθετικού πλαισίου στον νευραλγικό τομέα της κυβερνοασφάλειας, με την καθιέρωση αποτελεσματικών ελεγκτικών και εποπτικών μηχανισμών και εξασφαλίζοντας την ανεξαρτησία των ελεγκτών και τη διαφάνεια των εφαρμοζόμενων διαδικασιών έναντι των εποπτευόμενων φορέων. Ως εκ τούτου, η Εθνική Αρχή Κυβερνοασφάλειας διαθέτει ελεγκτικές αρμοδιότητες και διενεργεί επιθεωρήσεις με κύριο στόχο τη συνδρομή των υπόχρεων φορέων στην διαρκή ενίσχυση του επιπέδου

κυβερνοασφάλειάς τους και τη συμμόρφωσή τους προς το νομικό πλαίσιο για την κυβερνοασφάλεια, σύμφωνα με τις διατάξεις του ν. 4577/2018 (Α' 199) και του ν. 4961/2022 (Α' 146).

2. Εθνική Στρατηγική Κυβερνοασφάλειας

Η Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 («ΕΣΚ 2020-2025»), περιλαμβάνει πέντε (5) στρατηγικούς στόχους (1. «Ένα λειτουργικό σύστημα διακυβέρνησης» -2.«Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες» -3.«Βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμηση του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας» - 4.«Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης» – 5.«Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης»), οι οποίοι εξειδικεύονται σε δεκαπέντε (15) ειδικούς στόχους και πλήθος εμβληματικών δραστηριοτήτων.

Επιπλέον, η ΕΣΚ 2020 – 2025, συνοδεύεται από αναλυτικό πρόγραμμα δράσης, στο οποίο αποτυπώνεται ο προγραμματισμός της εφαρμογής των δραστηριοτήτων για την επίτευξη των ειδικών στόχων. Η υλοποίηση του σχεδίου δράσης, παρακολουθείται συστηματικά με σκοπό την συνεχή ανάδραση της διαδικασίας στρατηγικού σχεδιασμού, ιδίως εν όψει των προσαρμογών της ΕΣΚ, οι οποίες θα πρέπει να συντελεστούν σε συνέχεια της μεταφοράς της Οδηγίας NIS 2 στην εθνική έννομη τάξη.

Ενδεικτικά αναφέρουμε ότι, στις εμβληματικές δραστηριότητες της ΕΣΚ 2020-2025 εντάσσεται η ανάπτυξη δύο σημαντικών δημόσιων εργαλείων κυβερνοασφάλειας, τα οποία είναι ελεύθερα διαθέσιμα τους οργανισμούς:

α) το Εγχειρίδιο Κυβερνοασφάλειας (cybersecurity handbook), το οποίο αποτελεί ένα λεπτομερή και πλήρη οδηγό για την εφαρμογή βέλτιστων πρακτικών σε τεχνικά και οργανωτικά μέτρα διαχείρισης του κινδύνου, και

β) τον Οδηγό Αυτοαξιολόγησης της Κυβερνοασφάλειας Οργανισμών (Cybersecurity Self-Assessment Tool)», του οποίου η συμπλήρωση από τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών και τους Πάροχους Ψηφιακών Υπηρεσιών είναι υποχρεωτική, βάσει της Υπουργικής Απόφασης 1027/2019 (Β' 3739/08-10-2019).

Τα ανωτέρω εργαλεία, αναπτύχθηκαν από την Εθνική Αρχή Κυβερνοασφάλειας και απευθύνονται πρωτίστως σε κρίσιμες οντότητες οι οποίες διαχειρίζονται υποδομές βαρύνουσας σημασίας για την Χώρα και τις συνεπικουρούν στην εφαρμογή κατάλληλων μέτρων κυβερνοασφάλειας και στη διενέργεια αυτό-αξιολογήσεων του επιπέδου της κυβερνοανθεκτικότητάς τους. Τα αποτελέσματα των αυτό-αξιολογήσεων αυτών, είναι ιδιαιτέρως σημαντικά και για την Εθνική Αρχή Κυβερνοασφάλειας, καθώς για πρώτη φορά η Αρχή έχει στη διάθεση της συγκρίσιμα στοιχεία για το επίπεδο κυβερνοασφάλειας των φορέων της αρμοδιότητας της, παρέχοντας τη δυνατότητα να διαμορφώνει πολιτικές και προτεραιότητες βάσει αυτών των στοιχείων (data-driven policy making). Τα εργαλεία αυτά, είναι διαθέσιμα στην σελίδα του Υπουργείου Ψηφιακής Διακυβέρνησης: <https://mindigital.gr/dioikisi/kyvernoasfaleia>

3. Εκπαίδευση και ευαισθητοποίηση

Η ΕΣΚ 2020-2025 περιλαμβάνει ειδικούς στόχους και εμβληματικές δραστηριότητες για την εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας, όπως το συντονισμό δράσεων μεταξύ των συναρμόδιων φορέων για την ανάπτυξη ικανοτήτων, τη συστηματική και διαρκή εκπαίδευση, αλλά και την ευαισθητοποίηση του συνόλου των ενδιαφερόμενων μερών σε εθνικό επίπεδο, ως βασικά στοιχεία για την εξασφάλιση της εγρήγορσης έναντι των απειλών και της αποτελεσματικής απόκρισης σε κυβερνο-περιστατικά.

Ιδιαίτερα σε ό,τι αφορά στην εκπαίδευση υπαλλήλων της Δημόσιας Διοίκησης σε θέματα κυβερνοασφάλειας, η Εθνική Αρχή Κυβερνοασφάλειας έχει συμμετάσχει στο σχεδιασμό επιμορφωτικών προγραμμάτων των Υπευθύνων Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) των δημόσιων φορέων, οι οποίοι ορίστηκαν για πρώτη φορά στο σύνολο των Υπουργείων με τις διατάξεις του ν. 4961/2022 (Α' 146). Σχετικό πρόγραμμα επιμόρφωσης προσφέρεται ήδη και για το σύνολο των ενδιαφερόμενων δημοσίων υπαλλήλων, κατόπιν συνεργασίας της ΕΑΚ / ΥΨΗΔ με το Ινστιτούτο Επιμόρφωσης του Εθνικού Κέντρου Δημόσιας Διοίκησης & Αυτοδιοίκησης, στο πλαίσιο του οποίου έχουν ήδη επιμορφωθεί εκατοντάδες δημόσιοι υπάλληλοι, ενισχύεται η δημόσια διοίκηση και προετοιμάζεται για την εφαρμογή της Οδηγίας NIS 2.

Επιπρόσθετα, η Ελλάδα έχει αναπτύξει σημαντική πρωτοβουλία, μέσω του Υπουργείου Ψηφιακής Διακυβέρνησης, με στόχο να ηγηθεί του σχηματισμού "Κοινοπραξίας Ευρωπαϊκής Ψηφιακής Υποδομής" (EDIC) μεταξύ αρμόδιων εθνικών αρχών κρατών μελών της Ε.Ε. για την υποστήριξη της πρωτοβουλίας Cybersecurity Skills Academy της Ευρωπαϊκής Επιτροπής [COM (2023) 207 final]. Σκοπός της ανωτέρω πρωτοβουλίας είναι ο σχεδιασμός και εφαρμογή δράσεων, σε συνεργασία με ακαδημαϊκούς, ερευνητικούς και ιδιωτικούς φορείς, οι οποίες θα συμβάλλουν στην άμβλυνση του σημαντικού «χάσματος δεξιοτήτων» ('skills gap') στον τομέα της κυβερνοασφάλειας, το οποίο αναγνωρίζεται ως μία ιδιαιτέρως σημαντική πρόκληση για το σύνολο των κρατών μελών της Ε.Ε..

4. Αντιμετώπιση περιστατικών στον κυβερνοχώρο

Αναφορικά με τη διαχείριση των περιστατικών, αυτή πραγματοποιείται σύμφωνα με τον σχεδιασμό έκτακτης ανάγκης στον κυβερνοχώρο, από στις συναρμόδιες Υπηρεσίες και τους εκάστοτε πληττόμενους φορείς. Η Εθνική Αρχή Κυβερνοασφάλειας αποτελεί το ενιαίο σημείο αναφοράς σχετικά με απειλές και συμβάντα στον κυβερνοχώρο, συλλέγοντας και διαμοιράζοντας πληροφορίες προς άλλους δημόσιους και ιδιωτικούς φορείς, σε συνεργασία με άλλες αρχές, σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, για την ανίχνευση, συγκέντρωση και ανάλυση δεδομένων που σχετίζονται με απειλές και περιστατικά στον κυβερνοχώρο. Η Ε.Α.Κ., προκειμένου να ενισχύσει την ικανότητα απόκρισης αλλά και τη συνεργασία μεταξύ των εμπλεκόμενων και των συναρμόδιων φορέων, καθώς και των ευαίσθητων υποδομών, συμμετέχει η ίδια και ενθαρρύνει τη συμμετοχή των αρμόδιων φορέων και ενδιαφερόμενων μερών στις πανευρωπαϊκές ασκήσεις κυβερνοασφάλειας του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), οι οποίες προσομοιώνουν συνθήκες πραγματικών κυβερνοεπιθέσεων, δοκιμάζουν τα υφιστάμενα σχέδια απόκρισης και επιτρέπουν την άντληση εξαιρετικά χρήσιμων συμπερασμάτων.

Περαιτέρω, η Εθνική Αρχή Κυβερνοασφάλειας, αναπτύσσει τεχνικές δυνατότητες και συνδράμει τις κρίσιμες υποδομές της χώρας, προβαίνοντας σε πλέγμα δράσεων για την πρόληψη κυβερνοεπιθέσεων ενώ χρησιμοποιεί πλατφόρμες, υπηρεσίες και εργαλεία, με στόχο, μεταξύ άλλων:

- Την προστασία Κυβερνητικών Ιστοτόπων από επιθέσεις DDOS
- Την αξιολόγηση Επιπέδου Κυβερνοασφάλειας Οργανισμών
- Την ανάλυση απειλών - CTI (Cybersecurity Threat Intelligence)
- Την αποστολή ενημερώσεων σε οργανισμούς για τις σημαντικότερες απειλές/ευπάθειες
- Τη διαχείριση/απόκριση & αναφορά Περιστατικών
- Την παρακολούθηση διαθεσιμότητας κεντρικών ιστοτόπων

5. Κυβερνοασφάλεια και Προστασία Προσωπικών Δεδομένων

Σημειώνεται ότι η κυβερνοασφάλεια, ως δημόσια πολιτική, στοχεύει πρωτίστως στην προστασία των πληροφοριακών συστημάτων από απειλές που αντιμετωπίζουν στον κυβερνοχώρο, τον μετριασμό των επιπτώσεών τους, την ταχεία ανάκαμψη από κυβερνοεπιθέσεις, καθώς και την αδιάλειπτη παροχή

κρίσιμων υπηρεσιών για την οικονομική και κοινωνική ζωή, οι οποίες εξαρτώνται από τη λειτουργία πληροφοριακών συστημάτων. Στο πλαίσιο αυτό, η εμπιστευτικότητα, η διαθεσιμότητα και η ακεραιότητα των συστημάτων και των δεδομένων, προσωπικού χαρακτήρα και μη, αποτελεί πρωτίστως προϋπόθεση για την εμπιστοσύνη των πολιτών και την υποστήριξη στην ψηφιακή μετάβαση, η οποία οφείλει να συντελείται με διαρκώς εντεινόμενους ρυθμούς. Η Εθνική Αρχή Κυβερνοασφάλειας, συνεργάζεται με το σύνολο των εθνικών αρχών, οι οποίες αποτελούν τους βασικούς «μετόχους» για την υλοποίηση της εθνικής στρατηγικής κυβερνοασφάλειας, όπως είναι και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Η ΑΠΔΠΧ, λειτουργώντας ως συνταγματικά κατοχυρωμένη ανεξάρτητη αρχή με βάση το ενωσιακό δίκαιο, καθώς και τις πρόνοιες του εθνικού συντακτικού και κοινού νομοθέτη, επιτελεί έναν εξαιρετικά σημαντικό ρόλο, καθώς η Πολιτεία την έχει εμπιστευτεί με την προστασία των δεδομένων προσωπικού χαρακτήρα και την παρακολούθηση της εφαρμογής των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ).

Τέλος, επισημαίνουμε ότι σε ένα ραγδαία μεταβαλλόμενο ευρωπαϊκό και περιφερειακό περιβάλλον ασφάλειας, η διαρκής ενίσχυση της κυβερνοασφάλειας αποτελεί μία πρόκληση παγκόσμια, όπως παγκόσμια είναι και η φύση του διαδικτύου, με τις τεχνολογικές εξελίξεις να μεταλλάσσουν δυναμικά τις μορφές εγκληματικότητας στο διαδίκτυο. Το Υπουργείο Ψηφιακής Διακυβέρνησης, ταυτόχρονα με την ψηφιοποίηση των υπηρεσιών και την αξιοποίηση όλων των ωφελημάτων των νέων τεχνολογιών προς όφελος του πολίτη, των επιχειρήσεων, της εθνικής οικονομίας και του κοινωνικού συνόλου εν γένει, προβαίνει σε όλες τις αναγκαίες ενέργειες για την προστασία των κρίσιμων πληροφοριακών συστημάτων από ένα πλέγμα απειλών στο διαδίκτυο και κυβερνοεπιθέσεων, οι οποίες πλήττουν όχι μόνο τη Χώρα μας, αλλά το σύνολο των δημοκρατιών του δυτικού κόσμου. Ήδη, για το έτος 2023 το παγκόσμιο κόστος του κυβερνοεγκλήματος υπολογίζεται σε 10 τρις και βαίνει διαρκώς αυξανόμενο. Απαιτείται συντονισμένη προσπάθεια τόσο σε επίπεδο διεθνές και περιφερειακό όσο και σε ευρωπαϊκό, καθώς και, προφανώς, εθνικό. Η Χώρα μας, συμμετέχοντας σε όλα τα διεθνή και ευρωπαϊκά φόρα για την κυβερνοασφάλεια καταβάλει κάθε προσπάθεια ώστε, από κοινού με τους εταίρους μας στην Ε.Ε. και τους στρατηγικούς μας συμμάχους, να εξασφαλίζει για τους Έλληνες πολίτες, την εθνική οικονομία και το κοινωνικό σύνολο το μέγιστο δυνατό επίπεδο ασφάλειας στον κυβερνοχώρο.

Ο Διοικητής
της Εθνικής Αρχής Κυβερνοασφάλειας

Μιχαήλ Μπλέτσας

Ακριβές Αντίγραφο

Σπ. Κουτσοδήμου



Εσωτερική διανομή:

- Γραφείο Διοικητή
- Γραφείο Προϊσταμένου Γενικής Διεύθυνσης Επιτελικού Σχεδιασμού
- Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας (3)