DELPHI ECONOMIC FORUM

CENTER FOR CYBER RESILIENCE

ΣΕ ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΤΟ ΕΛΙΑΜΕΠ ELIAMEP

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

ΠΩΣ ΘΩΡΑΚΙΖΟΥΜΕ ΤΟ ΨΗΦΙΑΚΟ ΜΕΛΛΟΝ ΤΗΣ ΧΩΡΑΣ;

EXECUTIVE SUMMARY ΤΟΥ POLICY PAPER ΤΟΥ ΚΕΝΤΡΟΥ ΚΥΒΕΡΝΟ-ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΤΟΥ ΟΙΚΟΝΟΜΙΚΟΥ ΦΟΡΟΥΜ ΤΩΝ ΔΕΛΦΩΝ

POWERED BY vodafone

FOREWORD

Το Οικονομικό Φόρουμ των Δελφών, επιθυμώντας να συνεχίσει να αποτελεί μία σταθερά εμπλουτισμού του δημοσίου διαλόγου με επιστημονική γνώση και ολοκληρωμένες προτάσεις πολιτικής σε ζητήματα αιχμής, δημιούργησε το 2024 το Κέντρο Κυβερνο-Ανθεκτικότητας (Center for Cyber Resilience).

Τον περασμένο Μάρτιο, το Κέντρο διοργάνωσε, με την υποστήριξη της Vodafone Ελλάδας, μια εξαιρετικά πλούσια σε περιεχόμενο συζήτηση στρογγυλής τραπέζης, με θέμα τους κινδύνους και τις κυβερνο-απειλές που επηρεάζουν την ψηφιακή οικονομία, αλλά και την ίδια μας τη ζωή. Πέρα από τις επίκαιρες τοποθετήσεις των αρμόδιων υπουργών, κορυφαίων ακαδημαϊκών και παραγόντων της αγοράς, τη συζήτηση τροφοδότησε και μία έρευνα κοινής γνώμης της Metron Analysis, σε συνεργασία με το ΕΛΙΑΜΕΠ, σχετικά με τη χρήση του διαδικτύου στις επιχειρήσεις και στον δημόσιο τομέα. Από την έρευνα είναι ξεκάθαρο το εξής: όσο περισσότερο το διαδίκτυο γίνεται αναπόσπαστο κομμάτι της ζωής μας, τόσο περισσότερες είναι οι πιθανότητες να έρθουμε αντιμέτωποι με το κυβερνο-έγκλημα και τόσο μεγαλύτερος ο αντίκτυπος αυτού του νέου τύπου εγκλήματος στη ζωή πολιτών και επιχειρήσεων.

Το policy paper που κρατάτε στα χέρια σας αποτελεί μια προσπάθεια εξειδίκευσης και εμβάθυνσης στα θέματα της σημαντικής συζήτησης που ξεκίνησε εκείνο το απόγευμα, στις 1 Μαρτίου 2024. Με τη βοήθεια του ΕΛΙΑΜΕΠ, και ιδιαίτερα του Δρος Τριαντάφυλλου Καρατράντου και της εξαιρετικής ομάδας του, έχουμε την ευκαιρία να αποκτήσουμε μία σαφή εικόνα για την εξέλιξη του φαινομένου τις τελευταίες δεκαετίες, όσο και για τη θεσμική και νομική απάντηση σε αυτό, που έχει επιχειρήσει να προσφέρει τόσο η Ευρωπαϊκή Ένωση όσο και το ελληνικό κράτος.

Λέμε συχνά πως η τεχνολογία μοιραία βρίσκεται κάποια βήματα μπροστά ακόμα και από τις πλέον αποτελεσματικές κρατικές υπηρεσίες ασφάλειας, και η θεσμική και νομική θωράκιση των δημοκρατιών μας, αποτέλεσμα διαβούλευσης και συμβιβασμών, συνήθως έρχεται κατόπιν εορτής. Για τον λόγο αυτό, το policy paper περιέχει και μία σειρά από συγκεκριμένες προτάσεις πολιτικής, που θα μπορούσαν να αξιοποιηθούν, από την πολιτική και επιχειρηματική ηγεσία, την ακαδημαϊκή κοινότητα, αλλά και κάθε ενδιαφερόμενο, ώστε αυτή η «διαφορά φάσης», μεταξύ τεχνολογικού εγκλήματος και νομικού και επιχειρησιακού πλαισίου, να αμβλυνθεί όσο είναι εφικτό.

Είναι αυτού του τύπου η ολοκληρωμένη παρέμβαση στα δημόσια πράγματα που φιλοδοξεί να πετύχει το Οικονομικό Φόρουμ των Δελφών, μέσω της δραστηριότητας των –τριών πλέον– κέντρων πολιτικής που έχει δημιουργήσει τα τελευταία χρόνια: του Κέντρου για το Μέλλον της Εργασίας, του Κέντρου για το Μέλλον της Υγείας, και πλέον του Κέντρου Κυβερνο-Ανθεκτικότητας. Αποτελεί δέσμευσή μας να συνεχίσουμε σε αυτόν τον δρόμο και τα επόμενα χρόνια.

Καλή ανάγνωση

ΓΙΑΝΝΗΣ ΘΩΜΑΤΟΣ,
Αντιπρόεδρος του Οικονομικού Φόρουμ των Δελφών

FOREWORD

Η κυβερνοασφάλεια αποτελεί έναν από τους πιο κρίσιμους τομείς της σύγχρονης ψηφιακής εποχής, καθώς οι τεχνολογικές εξελίξεις και η αυξανόμενη συνδεσιμότητα δημιουργούν νέες προκλήσεις και κινδύνους. Σε μία εποχή που οι κυβερνοαπειλές γίνονται όλο και πιο περίπλοκες και επικίνδυνες, η Vodafone αναγνωρίζει τη σημασία της προστασίας των δεδομένων και των πληροφοριών τόσο για τις επιχειρήσεις όσο και για τους πολίτες. Η στρατηγική μας λοιπόν, επικεντρώνεται στην ενίσχυση των αμυντικών μηχανισμών μας, στην προληπτική ανάλυση κινδύνων, στην εκπαιδευτική ενδυνάμωση των χρηστών, αλλά και στην ευρύτερη ευαισθητοποίηση της κοινωνίας στο κορυφαίο ζήτημα της κυβερνοασφάλειας.

Στο πλαίσιο αυτό, και ειδικά στο τελευταίο σημείο, είμαστε εξαιρετικά ικανοποιημένοι για το γεγονός ότι είχαμε την είχαμε την ευκαιρία να συνεργαστούμε εκ νέου με το Center for Cyber Resilience του Οικονομικού Φόρουμ των Δελφών και το ΕΛΙΑΜΕΠ, με αποτέλεσμα το policy paper που διαβάζετε.

Σε αυτή την έκθεση, εξετάζονται οι κυριότερες προκλήσεις που αφορούν τον τομέα της κυβερνοασφάλειας, το πώς φτάσαμε στο υπάρχον θεσμικό πλαίσιο προστασίας τόσο στην Ευρωπαϊκή Ένωση όσο και στην Ελλάδα, ενώ ιδιαίτερη σημασία έχουν τα εξαιρετικά ενδιαφέροντα ευρήματα της έρευνας κοινής γνώμης που εκπόνησε η Metron Analysis ειδικά για αυτό το θέμα, και που αναδεικνύουν ανάγλυφα τη σημασία του για τις ελληνικές επιχειρήσεις αλλά και τους πολίτες. Αξίζει, τέλος, να διαβάσει κανείς με προσοχή τα συμπεράσματα και τις προτεινόμενες πολιτικές για την ενίσχυση της κυβερνοασφάλειας, που, αν εισακουστούν, μπορούν να επιτρέψουν στη χώρα μας να συμμετάσχει απρόσκοπτα στην ψηφιακή επανάσταση του μέλλοντος.

ΧΑΡΗΣ ΜΠΡΟΥΜΙΔΗΣ,
Προέδρος και διευθύνων σύμβουλος της Vodafone Ελλάδας

ΕΙΣΑΓΩΓΗ

Η ραγδαία ανάπτυξη της τεχνολογίας, στην εποχή της 4ης Βιομηχανικής Επανάστασης, της τεχνητής νοημοσύνης και του «διαδικτύου των πραγμάτων» (Internet of Things), έχει μεταβάλει εκ βάθρων τη λειτουργία των κρατών, τις υποδομές και, κυρίως, την καθημερινότητα των πολιτών. Πράγματι, η ανάπτυξη μιας τεχνολογίας μπορεί να βελτιώνει την ποιότητα της ζωής μας αλλά, παράλληλα, διευρύνει και την τρωτότητά μας. Αυτός είναι και ο βασικός λόγος που οι νέες τεχνολογίες είναι πλέον στενά συνδεδεμένες με τις πολιτικές ασφάλειας.

Όπως είναι φυσικό, αυτός ο θαυμαστός καινούριος κόσμος αντιμετωπίζεται από πολλούς με σκεπτικισμό. Κατά κάποιο τρόπο βλέπουμε μία νέα τοποθέτηση του απλουστευτικού, εν πολλοίς, διλήμματος «ασφάλεια ή ελευθερία» στον τομέα των τεχνολογιών. Είναι αναμενόμενο, ειδικότερα αν λάβουμε υπόψη μας πως, από τη μία πλευρά, η τεχνολογία τρέχει ταχύτερα από τις ρυθμιστικές πρωτοβουλίες των κρατών, και, από την άλλη, σε χώρες όπως η Ελλάδα, υπάρχει ένας σημαντικός αριθμός πολιτών που δεν είναι πλήρως εξοικειωμένος με τις δυνατότητες και τη σωστή χρήση των νέων τεχνολογιών.

Κρίσιμη παράμετρος σε όλη αυτή τη διαδικασία αποτελεί η συνεργασία του δημοσίου και του ιδιωτικού τομέα, όπως των παρόχων επικοινωνίας και δικτύων. Σε αυτή την κατεύθυνση άλλωστε κινείται και η ΕΕ με τη δημιουργία του EU Internet Forum, αλλά και με την ενθάρρυνση της ενισχυμένης αλληλεπίδρασης δημοσίου και ιδιωτικού τομέα.

Η χρήση νέων τεχνολογιών, τόσο από τις κρατικές υπηρεσίες, όσο και από τον ιδιωτικό τομέα, πρέπει να γίνεται κατόπιν μίας διαδικασίας ορθής αξιοποίησης, που θα προστατεύει τα ανθρώπινα δικαιώματα και τις ελευθερίες. Αυτός είναι και ο λόγος που η ΕΕ δίνει ιδιαίτερη έμφαση στο ζήτημα της προστασίας της ιδιωτικότητας, και έχει θεσπίσει ένα αρκετά αυστηρό πλαίσιο προστασίας των προσωπικών δεδομένων, το οποίο αποτελεί και τη βάση για τις πολιτικές προστασίας δεδομένων τόσο των δημοσίων φορέων, όσο και των ιδιωτικών εταιρειών.

Στο πλαίσιο αυτό κινείται και η συγκεκριμένη μελέτη, αποτέλεσμα της συνεργασίας του Center for Cyber Resilience του Οικονομικού Φόρουμ των Δελφών με την Vodafone Ελλάδας, το ΕΛΙΑΜΕΠ και τη Metron Analysis, για μια πρώτη, αλλά συστηματική αποτύπωση της κατάστασης, των τάσεων, αλλά και της οπτικής των πολιτών για την κυβερνοασφάλεια στην Ελλάδα. Η μελέτη έχει τέσσερις βασικούς άξονες: α) τις νέες τάσεις για τις νέες τεχνολογίες και την κυβερνοασφάλεια, β) το πλαίσιο και τις πολιτικές της ΕΕ, γ) την αρχιτεκτονική και το πλαίσιο της κυβερνοασφάλειας στην Ελλάδα και δ) την οπτική των πολιτών και των επιχειρήσεων. Η τελευταία ενότητα περιλαμβάνει τα συμπεράσματα και μια σειρά προτάσεων πολιτικής για τον δημόσιο και τον ιδιωτικό τομέα.

> «Βλέπουμε μία νέα τοποθέτηση του απλουστευτικού, εν πολλοίς, διλήμματος «ασφάλεια ή ελευθερία» στον τομέα των τεχνολογιών. Η χρήση νέων τεχνολογιών, τόσο από τις κρατικές υπηρεσίες, όσο και από τον ιδιωτικό τομέα, πρέπει να γίνεται κατόπιν μίας διαδικασίας ορθής αξιοποίησης, που θα προστατεύει τα ανθρώπινα δικαιώματα και τις ελευθερίες».

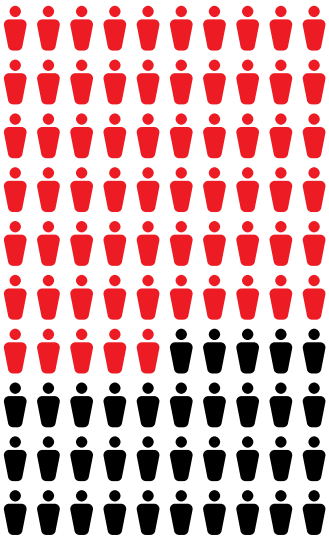
Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΟΝ 21ο ΑΙΩΝΑ: ΤΑΣΕΙΣ ΚΑΙ ΑΠΕΙΛΕΣ

Η ψηφιακή επανάσταση και η ψηφιοποίηση της κοινωνίας προκαλούν τη δημιουργία ενός μεταβαλλόμενου πεδίου ασφάλειας, επηρεάζοντας σχεδόν κάθε κοινωνική, οικονομική και πολιτική πτυχή, καθώς εγείρουν σημαντικές προκλήσεις, που αφορούν την ανάπτυξη κακόβουλων δραστηριοτήτων. Η ανάδυση νέων ασύμμετρων απειλών αποκτά διεθνή χαρακτήρα, καθώς ο κυβερνοχώρος δεν γνωρίζει γεωγραφικά όρια. Οι επιτιθέμενοι είναι ικανοί με τις κακόβουλες ενέργειές τους να επηρεάσουν τρία βασικά συστατικά της ασφάλειας: την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των δεδομένων.

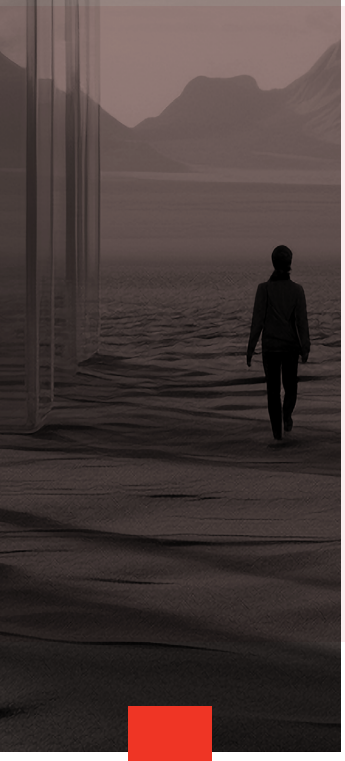
Όροι όπως κυβερνοασφάλεια (cybersecurity), κυβερνοάμυνα (cyberdefence), κυβερνοεπίθεση (cyberattack), κυβερνοτρομοκρατία (cyberterrorism), κυβερνοπόλεμος (cyberwar), κυβερνοκατασκοπεία (cyberespionage), παραπληροφόρηση (disinformation) και κυβερνοέγκλημα (cybercrime) αναλύονται όλο και περισσότερο από τις επιστήμες που ασχολούνται άμεσα με αυτές.

Ειδική αναφορά πρέπει να γίνει στο πώς λειτουργούν τα Μέσα Κοινωνικής Δικτύωσης. Η στροφή από τα παραδοσιακά κανάλια επικοινωνίας προς τα ΜΚΔ δεν βελτίωσε απαραίτητα την ποιότητα του πολιτικού λόγου. Αντίθετα, τα ΜΚΔ είναι γνωστό ότι λειτουργούν ως echo chamber της πόλωσης και προωθούν τη ρητορική «εμείς εναντίον των άλλων». Αυτοί οι παράγοντες συσχετίζονται με τον διαδικτυακό εκφοβισμό, την παρενόχληση και, ειδικότερα, τη ρητορική μίσους.

64,6%



Οι χρήστες του κυβερνοχώρου υπολογίζεται ότι είναι πάνω από **5,18 δισ.** ανά τον κόσμο, δηλαδή αποτελούν το **64,6%** του παγκόσμιου πληθυσμού.



6,5 ΩΡΕΣ

Οι χρήστες είναι «ενεργοί» για τουλάχιστον **6,5 ώρες** σε καθημερινή βάση.

4,8 δισ.

Υπολογίζεται ότι **4,8 δισ. άνθρωποι** (δηλαδή το 59% του παγκόσμιου πληθυσμού) έχουν δημιουργήσει λογαριασμό κοινωνικής δικτύωσης[1].

1. Statista Research Department. (22 Μαΐου 2023). Αριθμός χρηστών διαδικτύου και μέσων κοινωνικής δικτύωσης έως τον Απρίλιο του 2023. https://www.statista.com/statistics/617136/digital-population-worldwide/

Η ΚΑΤΑΣΤΑΣΗ ΣΤΗΝ ΕΛΛΑΔΑ

Με όρους εκτίμησης επικινδυνότητας, οι σημαντικότερες απειλές στον κυβερνοχώρο για την Ελλάδα σχετίζονται με τις οικονομικές απάτες, τη σεξουαλική εκμετάλλευση ανηλίκων, τα εξαρτώμενα από το διαδίκτυο εγκλήματα, τη διακίνηση ψευδών ειδήσεων, και τις «κυβερνοεπιθέσεις» με τη χρήση κακόβουλου λογισμικού κατά κρίσιμων υποδομών, στρατηγικών δικτύων και κυβερνητικών υπηρεσιών.

Σημαντικός είναι ακόμα ο κίνδυνος από τις δραστηριότητες των δικτύων του οργανωμένου εγκλήματος και της τρομοκρατίας στο «σκοτεινό διαδίκτυο» (dark web), όπως το εμπόριο όπλων και ναρκωτικών, η προπαγάνδα, η ριζοσπαστικοποίηση, η στρατολόγηση μαχητών, η χρηματοδότηση τρομοκρατικών επιθέσεων κ.ά. Εξίσου βαρύνουσα είναι η απειλή από κυβερνοεπιθέσεις, όπως αυτή κατά των ΕΛΤΑ τον Δεκέμβριο του 2022, με κύρια μορφή τους το Ransomware, δηλαδή επίθεση με κακόβουλο λογισμικό με σκοπό τα λύτρα από τον κάτοχο της συσκευής του δικτύου της υπηρεσίας.

Οι συγκεκριμένες επιθέσεις δεν πραγματοποιούνται ωστόσο μόνο εναντίον δημόσιων υπηρεσιών αλλά και κατά εταιρειών, ακόμα και ιδιωτών. Μια επίθεση DDoS μπορεί να στοχεύσει από το online τραπεζικό σύστημα μέχρι μια ηλεκτρονική πλατφόρμα παραγγελίας φαγητού, αλλά και ένα μέσο κοινωνικής δικτύωσης, ενώ η πιο απλή μορφή επίθεσης Ransomware γίνεται κατά ιδιώτη, όπου με κλείδωμα του υπολογιστή τού ζητούν ένα συγκεκριμένο χρηματικό ποσό ως αντάλλαγμα.

Ο ανθρώπινος παράγοντας παραμένει μια κρίσιμη τρωτότητα τόσο για τις επιχειρήσεις όσο και για τα άτομα. Το 82% των παραβιάσεων κατά των επιχειρήσεων αφορούσε τον ανθρώπινο παράγοντα, μέσω ζητημάτων όπως το σφάλμα και η κοινωνική μηχανική (social engineering).

ΠΟΛΙΤΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΕ

Η ΕΕ ξεκίνησε τις δράσεις της στον τομέα της κυβερνοασφάλειας από το 2004, με τη δημιουργία του ENISA, και του πρωταρχικού σχεδίου ευρωπαϊκής οδηγίας για την ασφάλεια των υποδομών που χρονολογείται από το 2008.

Ο ENISA, ως οργανισμός της ΕΕ για την κυβερνοασφάλεια, αναφέρεται στην κρισιμότητα του ζητήματος της υιοθέτησης μιας εθνικής στρατηγικής για την κυβερνοασφάλεια, η οποία πρέπει να αποσκοπεί σε μια σειρά από εθνικούς στόχους και προτεραιότητες που πρέπει να επιτευχθούν σε συγκεκριμένο χρονικό πλαίσιο.

Κάθε κράτος-μέλος της ΕΕ είναι υποχρεωμένο να χαράξει μια εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύων και πληροφοριών, και να είναι αποτελεσματικό στην προστασία βασικών υπηρεσιών (ζωτικής ή κρίσιμης σημασίας υποδομές, όπως ενέργεια, μεταφορές, τραπεζική/χρηματοπιστωτική αγορά, τομέας υγείας, παροχή/διανομή νερού, ψηφιακές υποδομές), αλλά και υπηρεσιών που σχετίζονται με την ηλεκτρονική αγορά, τη μηχανή αναζήτησης και τη νεφοϋπολογιστική (Cloud computing).

> «Κάθε κράτος-μέλος της ΕΕ είναι υποχρεωμένο να χαράξει μια εθνική στρατηγική για την ασφάλεια των συστημάτων δικτύων και πληροφοριών».

ΧΡΟΝΟΛΟΓΙΕΣ–ΣΤΑΘΜΟΙ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΠΟΛΙΤΙΚΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

2011: Δημιουργείται η μόνιμη CERT–EU (Computer Emergency Response Team – CERT) και φιλοξενείται διοικητικά από τη Γενική Διεύθυνση Πληροφορικής της Ευρωπαϊκής Επιτροπής.

2013: Υιοθετείται η «Στρατηγική κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης, για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο», το πρώτο συνεκτικό κείμενο στρατηγικής της ΕΕ για θέματα ασφάλειας στο κυβερνοχώρο.

2013: Ιδρύεται το Ευρωπαϊκό Κέντρο για Εγκλήματα στον Κυβερνοχώρο (European Cybercrime Centre – EC3) και υπάγεται στη Europol.

2014: Εγκρίνεται από την ΕΥΕΔ (Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης – European External Action Service) το «Πλαίσιο πολιτικής για την κυβερνοάμυνα», στο οποίο αναφέρονται οι βασικοί πυλώνες αντιμετώπισης των κυβερνο–απειλών.

2016: Ψηφίζεται ο Γενικός Κανονισμός για την Προστασία Δεδομένων(General Data Protection Regulatory – GDPR), ο οποίος ορίζει τις υποχρεώσεις στις οποίες πρέπει να προσαρμόζονται οι οργανισμοί και οι εταιρείες κατά την επεξεργασία των προσωπικών δεδομένων των χρηστών σε ευρωπαϊκό όσο και μη περιβάλλον.

2016: Εγκρίνεται από το Ευρωπαϊκό Κοινοβούλιο η «Οδηγία για την ασφάλεια των δικτύων και πληροφοριών» (NIS – Directive on Security of Network and Information Systems), ο πρώτος ευρωπαϊκός νόμος για την ασφάλεια στον κυβερνοχώρο. Αποτελεί τον ακρογωνιαίο λίθο για την ενίσχυση και βελτίωση των εθνικών δυνατοτήτων ασφάλειας των κρατών-μελών[2].

2017: Η ΕΕ προχωράει στην αναθεώρηση της στρατηγικής της κυβερνοασφάλειας. Η στρατηγική ονομάστηκε «Ανθεκτικότητα, αποτροπή και άμυνα: οικοδόμηση ισχυρής κυβερνοασφάλειας για την ΕΕ» (Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU) και αναφέρεται σε απειλές στον οικονομικό, πολιτικό και στρατιωτικό τομέα.

2017: Η Ευρωπαϊκή Επιτροπή παρουσιάζει το «Blueprint for a Coordinated Response to Large Scale Cybersecurity Incidents and Crises» (Πρόγραμμα δράσης για μια συντονισμένη απόκριση σε μεγάλη κλίμακας περιστατικά και κρίσεις κυβερνοασφάλειας).

2019: Υιοθετείται το European Cybersecurity Act [Regulation (EU) 2019/881], που αφορά την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών. Ο ENISA εξελίσσεται σε κεντρικό, καθοριστικό παράγοντα στο (ψηφιακό) «οικοσύστημα της ασφάλειας».

2022: Τίθεται σε ισχύ η Πράξη για τις Ψηφιακές Υπηρεσίες (Digital Services Act– DSA), που αφορά τις μεγαλύτερες εταιρείες ψηφιακής τεχνολογίας και όλους τους διαδικτυακούς μεσάζοντες που προσφέρουν τις υπηρεσίες τους στην ενιαία αγορά της ΕΕ, ανεξάρτητα από το αν είναι εγκατεστημένοι στην ΕΕ ή εκτός.

2. Η αναθεώρηση της Οδηγίας, πέντε χρόνια μετά την υιοθέτησή της, είναι ενδεικτική της ταχείας εξέλιξης της τεχνολογίας και των απειλών. Η νέα Οδηγία «NIS2» τέθηκε σε εφαρμογή στις 16 Ιανουαρίου 2023 και πρέπει να υιοθετηθεί από όλα τα κράτη-μέλη μέχρι τις 17 Οκτώβρη 2024.

2022: Η Ευρωπαϊκή Επιτροπή παρουσιάζει τον Νόμο για την Ανθεκτικότητα στον Κυβερνοχώρο (Cyber Resilience Act –CRA), που έρχεται να συμπληρώσει την Πράξη περί Τεχνητής Νοημοσύνης (AI Act), τον Νόμο της ΕΕ για την Κυβερνοασφάλεια (EU Cybersecurity Act) και την Οδηγία NIS·2.

2022: Η Ευρωπαϊκή Επιτροπή ανακοινώνει το πλαίσιο πολιτικής της ΕΕ για την Κυβερνοάμυνα (European Cyber–defence policy). Η νέα πολιτική απαιτεί επενδύσεις στην άμυνα στον κυβερνοχώρο, για να ενισχύσει τον συντονισμό και τη συνεργασία μεταξύ των στρατιωτικών και πολιτικών κοινοτήτων.

2023: Η Ευρωπαϊκή Ένωση θεωρεί τον κυβερνοχώρο ως πεδίο στρατηγικού ανταγωνισμού, από τον οποίο απορρέουν κίνδυνοι που αφορούν την ασφάλεια και την άμυνα της ΕΕ. Οι κίνδυνοι αυτοί έχουν μια αυξητική τάση, λόγω των διαρκών γεωπολιτικών εντάσεων και της αυξανόμενης εξάρτησης από τις ψηφιακές τεχνολογίες. Η αυξανόμενη τρωτότητα έναντι απειλών και συμβάντων στον κυβερνοχώρο απαιτεί αποτελεσματική ρύθμιση. Ωστόσο, το παρόν πλαίσιο έναντι τέτοιων απειλών μέχρι σήμερα έχει κριθεί ανεπαρκές. Σε απάντηση, στις 18 Απριλίου 2023, η Ευρωπαϊκή Επιτροπή κατέθεσε σχέδιο νόμου με κύριο στόχο την ενίσχυση της εναρμόνισης, προκειμένου να μετριαστεί η αυξανόμενη ευπάθεια με τον εντοπισμό, την προετοιμασία και την αντιμετώπιση απειλών και περιστατικών κυβερνοασφάλειας εντός της ΕΕ. Ο Νόμος για την Αλληλεγγύη στον Κυβερνοχώρο (Cyber Solidarity Act) είναι μια πρόταση που επιδιώκει να εφαρμόσει μέτρα από τις υπάρχουσες στρατηγικές.

ΤΟ ΕΘΝΙΚΟ ΣΥΣΤΗΜΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Η Ελλάδα λειτουργεί εντός του στρατηγικού και θεσμικού πλαισίου της ΕΕ που παρουσιάστηκε αναλυτικά. Στο εθνικό σύστημα κυβερνοασφάλειας τον κύριο συντονιστικό ρόλο έχει το Υπουργείο Ψηφιακής Διακυβέρνησης. Στο πλαίσιο αυτό, το 2018, το τότε Υπουργείο Ψηφιακής Πολιτικής, δημοσίευσε την «Εθνική Στρατηγική Κυβερνοασφάλειας», η οποία καθόριζε τον κεντρικό σχεδιασμό του κράτους για την ασφάλεια στον κυβερνοχώρο. Επίσης, από το 2017, η Γενική Διεύθυνση Κυβερνοασφάλειας ορίστηκε ως Εθνική Αρχή Κυβερνοασφάλειας, με αρμοδιότητα την υλοποίηση και επικαιροποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Τον Δεκέμβριο του 2020, η Εθνική Αρχή Κυβερνοασφάλειας εξέδωσε τη νέα «Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025». Κεντρικός στόχος της εν λόγω στρατηγικής είναι «ένα σύγχρονο και ασφαλές ψηφιακό περιβάλλον πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών προς όφελος της οικονομικής και κοινωνικής ευημερίας, με την εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων των πολιτών, την ανάπτυξη κουλτούρας ασφαλούς χρήσης των ψηφιακών υπηρεσιών και εφαρμογών, και την επαύξηση της εμπιστοσύνης των πολιτών και των επιχειρήσεων στις ψηφιακές τεχνολογίες».

Το εθνικό σύστημα κυβερνοασφάλειας έχει τρεις βασικούς επιχειρησιακούς βραχίονες: α) την Εθνική Υπηρεσία Πληροφοριών – Εθνικό CERT, β) τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας και γ) τη Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας – αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT).

Το 38% του γενικού πληθυσμού δηλώνει όχι τόσο (25%) και καθόλου (13%) ενημερωμένο για τους κινδύνους ασφάλειας στο διαδίκτυο.

Σημαντικές αλλαγές στον τομέα της κυβερνοασφάλειας προέκυψαν και από τον Νόμο 5002/2022 – Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών. Ειδικότερα, συστάθηκε η Επιτροπή Συντονισμού για Θέματα Κυβερνοασφάλειας με αποστολή τον προγραμματισμό, την παρακολούθηση, τον συντονισμό ενεργειών, τις παρεμβάσεις σε ζητήματα που άπτονται της κυβερνοασφάλειας από το αρχικό στάδιο της πρόληψης μέχρι το στάδιο της αποτελεσματικής αντιμετώπισης περιστατικών κυβερνοεπιθέσεων, και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο.

Στις αρμοδιότητες της επιτροπής περιλαμβάνονται μεταξύ άλλων: α) η παροχή κατευθύνσεων σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο, β) ο συντονισμός, η παρακολούθηση και η αξιολόγηση της υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας, γ) η έγκριση του Εθνικού Σχεδίου Έκτακτης Ανάγκης, και δ) η εισήγηση προς το Κυβερνητικό Συμβούλιο Εθνικής Ασφάλειας οποιουδήποτε θέματος άπτεται της κυβερνοασφάλειας. Η δεύτερη σημαντική πρόβλεψη του νόμου είναι το Εθνικό Σχέδιο Αποτίμησης Επικινδυνότητας Συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών (ΤΠΕ).

Η πλέον πρόσφατη θεσμική εξέλιξη στον τομέα της κυβερνοασφάλειας είναι η σύσταση, με τον Νόμο 5086/2024, της Εθνικής Αρχής Κυβερνοασφάλειας. Σκοπός της αρχής είναι η οργάνωση, ο συντονισμός, η εφαρμογή και ο έλεγχος ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, σε επίπεδο πρόληψης, προστασίας, αποτροπής, εντοπισμού, αντιμετώπισης, αποκατάστασης και ανάκαμψης από κυβερνοεπιθέσεις.

Η ΓΝΩΜΗ ΤΩΝ ΠΟΛΙΤΩΝ ΚΑΙ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

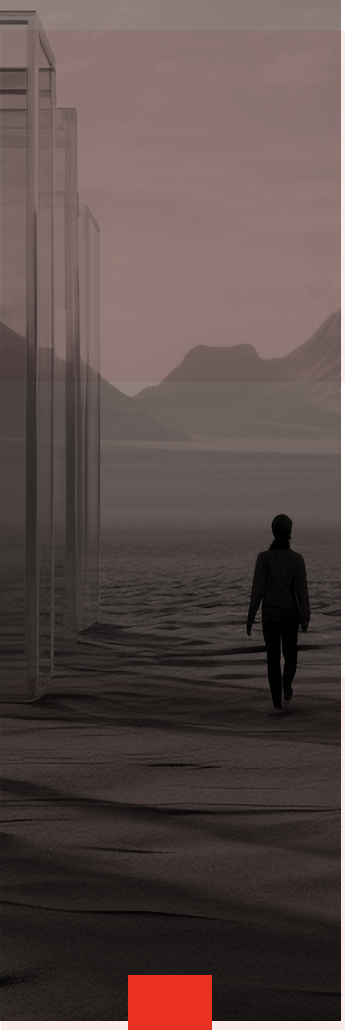
Μέσα σε αυτό το πλαίσιο, πώς κινείται η κοινή γνώμη στην Ελλάδα; Με άλλα λόγια, τι πιστεύουν οι Έλληνες, αλλά και οι επιχειρήσεις για την ασφάλεια στο διαδίκτυο; Αυτό ήταν το αντικείμενο των δύο ειδικών ερευνών που διεξήγαγε η Metron Analysis, τα βασικά στοιχεία των οποίων παρουσιάζονται σε αυτή την ενότητα.

Η κατανόηση της απειλής από τους πολίτες είναι εξαιρετικά κρίσιμη για τα ζητήματα κυβερνοασφάλειας. Γι' αυτό έχει ενδιαφέρον να αναφερθούμε στο πώς αντιλαμβάνονται οι Έλληνες τις απειλές στο διαδίκτυο. Σύμφωνα με την έρευνα της Metron Analysis, παρότι το 84% δηλώνει πως αντιμετωπίζει κινδύνους στο διαδίκτυο, το 67% είναι αυτό που λαμβάνει μέτρα προστασίας κατά τη διάρκεια της περιήγησής του. Σε αυτά συμπεριλαμβάνονται: α) η επίσκεψη μόνο σε ιστοσελίδες που γνωρίζουν και εμπιστεύονται, β) το μη άνοιγμα μηνυμάτων ηλεκτρονικού ταχυδρομείου από αποστολείς που δεν γνωρίζουν, γ) η αποκλειστική χρήση του προσωπικού υπολογιστή και δ) η εγκατάσταση λογισμικού antivirus.

Προκαλεί προβληματισμό πως το 38% του γενικού πληθυσμού δηλώνει όχι τόσο (25%) και καθόλου (13%) ενημερωμένο για τους κινδύνους ασφάλειας στο διαδίκτυο. Οι περιστασιακοί χρήστες και οι μεγαλύτερες ηλικίες είναι λιγότερο ενημερωμένοι για τους κινδύνους, ενώ οι περισσότερο ευαισθητοποιημένοι είναι οι νεότεροι ηλικιακά (83% των Millennials), οι υψηλότερης κοινωνικής τάξης και μορφωτικού επιπέδου (78%), και οι φοιτητές (89%).

Οι Έλληνες αισθάνονται ανασφάλεια και για τα προσωπικά τους δεδομένα στο διαδίκτυο. Σε σύγκριση με πέντε χρόνια πριν, ένας στους δύο (51%) δηλώνει ότι αισθάνεται λιγότερη ασφάλεια ως προς τα προσωπικά του δεδομένα και τις πληροφορίες. Πρέπει να τονίσουμε πως δεν πρόκειται για έναν ελληνικό εξαιρετισμό, καθώς αντίστοιχες μετρήσεις σε άλλες χώρες της ΕΕ, αλλά και στις ΗΠΑ, δείχνουν αντίστοιχη τάση.

Έχει αυξηθεί σημαντικά το ποσοστό των Ελλήνων που χρησιμοποιεί καθημερινά το διαδίκτυο – στις νεότερες γενιές (Millennials και Gen Z) φτάνει το **100%**.



ΟΣΟ ΠΕΡΙΣΣΟΤΕΡΟ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΤΟ ΔΙΑΔΙΚΤΥΟ, ΤΟΣΟ ΠΕΡΙΣΣΟΤΕΡΟ ΘΕΩΡΟΥΝ ΠΩΣ ΑΝΤΙΜΕΤΩΠΙΖΟΥΝ ΚΙΝΔΥΝΟΥΣ **(84%)**. ΟΙ ΜΕΓΑΛΥΤΕΡΟΙ ΚΙΝΔΥΝΟΙ ΕΙΝΑΙ ΟΙ ΑΠΑΤΕΣ, Η ΚΑΤΑΧΡΗΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ Η ΣΕΞΟΥΑΛΙΚΗ ΚΑΚΟΠΟΙΗΣΗ ΚΑΙ ΕΚΜΕΤΑΛΛΕΥΣΗ ΑΝΗΛΙΚΩΝ.

Το **11%** του συνόλου δηλώνει πως έχει πέσει θύμα εγκληματικής δραστηριότητας, κάτι που, ωστόσο, αλλάζει ριζικά στους εντατικούς χρήστες, με το **60%** να έχει εντοπίσει κακόβουλο λογισμικό ή παραπλανητικό email.

ΟΛΟΙ ΓΝΩΡΙΖΟΥΝ ΤΗ ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ, ΑΛΛΑ ΜΟΝΟ ΕΝΑΣ ΣΤΟΥΣ ΤΡΕΙΣ ΑΠΟ ΟΣΟΥΣ ΔΗΛΩΝΟΥΝ ΠΩΣ ΕΧΟΥΝ ΠΕΣΕΙ ΘΥΜΑ ΑΠΑΤΗΣ ΑΠΕΥΘΥΝΟΝΤΑΙ ΣΕ ΑΥΤΗ, ΕΝΩ ΤΟ **25%** ΤΩΝ ΘΥΜΑΤΩΝ ΑΠΕΥΘΥΝΟΝΤΑΙ ΣΕ ΣΥΓΓΕΝΕΙΣ ΚΑΙ ΦΙΛΟΥΣ. ΠΕΡΙΣΣΟΤΕΡΕΣ ΑΠΟ **1 ΣΤΙΣ 5 ΕΤΑΙΡΕΙΕΣ (21%)** ΕΧΟΥΝ ΑΠΕΥΘΥΝΘΕΙ ΣΤΗ ΔΙΩΞΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΓΙΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.

Το ένα τρίτο των ελληνικών εταιρειών αναφέρει περιστατικά κυβερνοεπίθεσης ή κυβερνοεγκλήματος που αφορούν, κατά κύριο λόγο, παραπλανητικά emails και δευτερευόντως κακόβουλο λογισμικό ή χακάρισμα κοινωνικών δικτύων και emails, ενώ ελάχιστα σχετίζονται με παραβίαση προσωπικών δεδομένων πελατών.

Παρά την κλιμάκωση των κινδύνων, οι ελληνικές επιχειρήσεις, και ειδικά οι μεγαλύτερες σε μέγεθος, δηλώνουν σήμερα πιο ασφαλείς και θωρακισμένες συγκριτικά με πέντε χρόνια νωρίτερα, με το **41%** να θεωρεί ότι τα προσωπικά δεδομένα είναι πλέον πιο ασφαλή.

ΣΤΗ ΜΕΓΑΛΗ ΤΟΥΣ ΠΛΕΙΟΝΟΤΗΤΑ **(85%)**, ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΔΗΛΩΝΟΥΝ ΟΤΙ ΠΑΙΡΝΟΥΝ ΜΕΤΡΑ ΔΙΑΦΥΛΑΞΗΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΓΟΡΕΣ/ ΣΥΝΑΛΛΑΓΕΣ. Η ΤΑΣΗ ΑΥΤΗ ΕΙΝΑΙ ΕΝΤΟΝΟΤΕΡΗ ΜΕΤΑΞΥ ΤΩΝ ΜΕΓΑΛΥΤΕΡΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ **(94%)**.

Σημαντικά μικρότερο είναι το ποσοστό των επιχειρήσεων που δηλώνει ότι διαθέτει σχέδιο πρόληψης/αντιμετώπισης κυβερνοεπιθέσεων: **σχεδόν 6 στις 10 εταιρείες στην Ελλάδα (57%)** απαντούν ότι διαθέτουν σχέδιο πρόληψης των περιστατικών κυβερνοασφάλειας, ποσοστό που στις μεγαλύτερες εταιρείες φθάνει το **85%**.

ΜΟΝΟ ΤΟ **19%** ΤΩΝ ΕΤΑΙΡΕΙΩΝ ΤΟΥ ΔΕΙΓΜΑΤΟΣ ΤΗΣ ΕΡΕΥΝΑΣ ΕΧΕΙ ΑΞΙΟΠΟΙΗΣΕΙ, ΜΕΧΡΙ ΣΗΜΕΡΑ, ΕΘΝΙΚΗ Ή ΕΥΡΩΠΑΪΚΗ ΧΡΗΜΑΤΟΔΟΤΗΣΗ ΓΙΑ ΤΗΝ ΑΝΑΒΑΘΜΙΣΗ ΣΤΟ ΠΕΔΙΟ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ.

Αν και η εκπαίδευση θεωρείται κομβικό σημείο, πρακτικά, μόνο **3 στις 10 επιχειρήσεις** παρείχαν τον τελευταίο χρόνο εκπαίδευση στο προσωπικό τους σε θέματα ασφάλειας.

ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ ΠΟΛΙΤΙΚΗΣ

Ο τομέας των αναδυόμενων τεχνολογιών είναι αυτή τη στιγμή το σημαντικότερο ζήτημα, με όρους στρατηγικής πρόκλησης, που αντιμετωπίζουν οι αρμόδιοι για τη χάραξη πολιτικής για την ασφάλεια σε διεθνές αλλά και εθνικό επίπεδο.

Υπάρχουν τρεις δομικές παθογένειες για την κυβερνοασφάλεια στην Ελλάδα:

α) Ο κατακερματισμός της πολιτικής εσωτερικής ασφάλειας, μιας και σε αυτή ως υποσύνολο εντάσσεται η κυβερνοασφάλεια, μεταξύ διαφορετικών υπουργείων και υπηρεσιών. Αξίζει αναφοράς πως μόνο σε επίπεδο βασικών παρόχων ασφάλειας εμπλέκονται τέσσερα διαφορετικά υπουργεία (Προστασίας του Πολίτη, Πολιτικής Προστασίας και Κλιματικής Κρίσης, Ψηφιακής Διακυβέρνησης, Ναυτιλίας και Νησιωτικής Πολιτικής), καθώς και το Υπουργείο Εθνικής Άμυνας και η Ε.Υ.Π.

β) Η προβληματική συνεργασία μεταξύ δημοσίου και ιδιωτικού τομέα. Τις περισσότερες κρίσιμες υποδομές, για παράδειγμα, τις διαχειρίζονται ιδιωτικές εταιρείες, οι οποίες έχουν τον δικό τους σχεδιασμό ασφάλειας. Το πρόβλημα ξεκινά από το γεγονός ότι το δημόσιο δεν έχει ένα ολοκληρωμένο πλαίσιο και συγκεκριμένα standards, τα οποία θα πρέπει να ακολουθεί ο διαχειριστής της υποδομής, είτε είναι δημόσιος, είτε ιδιωτικός.

γ) Απουσία κουλτούρας ασφάλειας από το ανθρώπινο δυναμικό που «τρέχει» στην καθημερινότητα τις κρίσιμες υποδομές. Πρέπει εδώ να προσθέσουμε και δύο δομικά προβλήματα του σχεδιασμού. Το πρώτο είναι η μη αξιοποίηση των μελλοντικών τάσεων – ο σχεδιασμός ασφάλειας δεν μπορεί να ακολουθεί τις απειλές και τους κινδύνους, αλλά να προσπαθεί να τους προβλέψει ώστε να κινηθεί εμπροσθοβαρώς (Foresight Led Planning). Το δεύτερο είναι η μη επένδυση στην ανάδειξη των τρωτοτήτων. Επιτυχής σχεδιασμός σημαίνει εντοπισμός τρωτοτήτων και θωράκισή τους.

ΠΡΟΤΕΙΝΟΜΕΝΕΣ ΑΛΛΑΓΕΣ ΠΟΛΙΤΙΚΗΣ

Οι βασικοί πυλώνες αλλαγών είναι οι ακόλουθοι:

Οι προτεινόμενες κατευθύνσεις αλλαγών και μεταρρυθμίσεων αφορούν:

(α) **τη δημιουργία δυνατοτήτων** με στόχο την έγκαιρη ανίχνευση, πρόληψη και ταχεία αντίδραση στις απειλές, αλλά και στις προκύπτουσες κρίσεις ασφάλειας, μέσω ολοκληρωμένης και συντονισμένης προσέγγισης,

(β) **την αλλαγή του υφιστάμενου νομοθετικού πλαισίου** για την προστασία και την ενίσχυση της «ανθεκτικότητας» των κρίσιμων υποδομών, προκειμένου να συμβαδίζει με τους εξελισσόμενους κινδύνους,

(γ) **την ανάπτυξη συνεργειών** μεταξύ των φορέων του δημοσίου και ιδιωτικού τομέα, σε κοινή κατεύθυνση όσον αφορά στην ανταλλαγή πληροφοριών σχετικά με την ασφάλεια και εντατικότερη συνεργασία με άλλα κράτη, καθώς και με τα θεσμικά όργανα και τους οργανισμούς της ΕΕ,

(δ) **την προσαρμογή των επαγγελματιών** στους τομείς της επιβολής του νόμου και απονομής της δικαιοσύνης στις σύγχρονες μεθόδους επιβολής του νόμου και στη νέα και καινοτόμο τεχνολογία,

(ε) **την «ευαισθητοποίηση»** της ελληνικής κοινωνίας σε θέματα ασφάλειας και την απόκτηση των δεξιοτήτων για τη βελτίωση της ετοιμότητάς της στην αντιμετώπιση πιθανών απειλών.

Καταληκτικά, παρατίθενται ορισμένες προτάσεις πολιτικής:

ΑΣΦΑΛΕΙΑ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

1. **Εκπόνηση** εθνικής στρατηγικής για την κυβερνοασφάλεια και την προστασία των κρίσιμων οντοτήτων, η οποία θα συμβαδίζει με τις τελικές προβλέψεις της Οδηγίας CER για την ανθεκτικότητα αυτών.
2. **Καθορισμός** των εθνικών κρίσιμων υποδομών ανά τομέα ακολουθώντας τη λογική της Οδηγίας CER.
3. **Καθορισμός** ενός φορέα που θα έχει την ευθύνη παρακολούθησης και ελέγχου της πολιτικής προστασίας των κρίσιμων υποδομών.
4. **Δημιουργία** ψηφιακής εθνικής βάσης κρίσιμων υποδομών.
5. **Έλεγχος** των σχεδίων και των διαδικασιών ασφάλειας των κρίσιμων υποδομών.
6. **Συχνές εκπαιδεύσεις** του προσωπικού που απασχολείται σε κρίσιμες υποδομές.
7. **Αναζήτηση και υιοθέτηση** βέλτιστων πρακτικών για την ασφάλεια των κρίσιμων υποδομών.
8. **Καθορισμός** εθνικών standards ασφάλειας υποδομών και διαδικασιών ελέγχου, και πιστοποίησης της εφαρμογής τους.
9. **Καθορισμός** προδιαγραφών ασφάλειας σε όλες τις κρίσιμες υποδομές και έλεγχος εφαρμογής τους.

ΜΕΛΛΟΝΤΙΚΕΣ ΤΑΣΕΙΣ ΚΑΙ ΕΓΚΑΙΡΗ ΠΡΟΕΙΔΟΠΟΙΗΣΗ

10. **Συνέργειες** με την ακαδημαϊκή και την ερευνητική κοινότητα, τόσο για την ανάδειξη μελλοντικών τάσεων, όσο και για τον καλύτερο σχεδιασμό ασφάλειας.
11. **Αξιοποίηση μεθοδολογιών** foresight για μελέτες επικινδυνότητας.
12. **Χρήση** νέων τεχνολογικών εργαλείων και συστημάτων έγκαιρης προειδοποίησης για την ενίσχυση της ασφάλειας και την αποτροπή των κινδύνων.
13. **Ενδυνάμωση** των διαδικασιών διαλειτουργικότητας και συνδεσιμότητας των κέντρων ελέγχου και των επιχειρήσεων των κρίσιμων υποδομών με τα συντονιστικά κέντρα επιχειρήσεων της Ελληνικής Αστυνομίας και της Γενικής Γραμματείας Πολιτικής Προστασίας.
14. **Ενίσχυση** των συνεργειών δημοσίου και ιδιωτικού τομέα, με έμφαση στην ανταλλαγή πληροφοριών και βέλτιστων πρακτικών.

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΚΑΙ ΔΡΑΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ

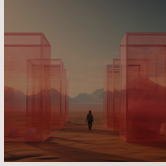
15. **Σχεδιασμός** και υλοποίηση μιας επικοινωνιακής εκστρατείας ενημέρωσης και ευαισθητοποίησης τόσο από το κράτος, όσο και από τις ιδιωτικές εταιρείες, για τις νομοθετικές δικλείδες, τις πολιτικές προστασίας και τα δικαιώματα των πολιτών.
16. **Δράσεις** για τη διαμόρφωση μίας ατομικής και συλλογικής κουλτούρας ασφάλειας στο διαδίκτυο, που να δίνει έμφαση στη λήψη μέτρων προστασίας, αλλά και για την ενημέρωση των αρμοδίων δημοσίων φορέων σε περιπτώσεις κινδύνου.
17. **Σχεδιασμός και διεξαγωγή** ασκήσεων και stress tests.
18. **Σχεδιασμός και υλοποίηση** προγραμμάτων εκπαίδευσης για την ενίσχυση των δεξιοτήτων κυβερνοασφάλειας των πολιτών.
19. **Δημιουργία** εκπαιδευτικών δομών που θα παρέχουν τόσο γενικές, όσο και στοχευμένες εκπαιδεύσεις για τους πολίτες, αλλά και για τις διάφορες κατηγορίες επαγγελματιών και επιχειρήσεων.

ΕΝΙΣΧΥΣΗ ΤΗΣ ΕΡΕΥΝΑΣ ΚΑΙ ΔΗΜΙΟΥΡΓΙΑ ΓΝΩΣΗΣ

20. **Διεξαγωγή** τακτικών ποιοτικών και ποσοτικών ερευνών για τη χαρτογράφηση των προτιμήσεων, αλλά και των απειλών που θεωρούν πως αντιμετωπίζουν οι Έλληνες στο διαδίκτυο, οι οποίες πρέπει να συνδυαστούν με τον σχεδιασμό και την αξιοποίηση σύγχρονων εργαλείων για την ασφαλή πλοήγηση και την προστασία των προσωπικών δεδομένων.
21. **Περαιτέρω ανάπτυξη** του επιστημονικού και ερευνητικού τομέα για την κυβερνοασφάλεια, με στόχο και την δημιουργία περισσότερων ειδικών στον τομέα, που θα καλύψουν και τις ανάγκες που έχει η αγορά.

ΕΝΙΣΧΥΣΗ ΤΩΝ ΣΥΝΕΡΓΕΙΩΝ ΜΕ ΤΟΝ ΙΔΙΩΤΙΚΟ ΤΟΜΕΑ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

22. **Υποστήριξη** των επιχειρήσεων, κυρίως των μικρών, για την αξιοποίηση εθνικών και ευρωπαϊκών χρηματοδοτήσεων για θέματα κυβερνοασφάλειας.
23. **Απλοποίηση και κωδικοποίηση** της νομοθεσίας γύρω από θέματα κυβερνοασφάλειας.
24. **Δημιουργία** Εθνικού PPP (Public– Private Platform) για θέματα κυβερνοασφάλειας.



ΤΑΥΤΟΤΗΤΑ POLICY PAPER

Το policy paper **«Κυβερνοασφάλεια: Πώς θωρακίζουμε το ψηφιακό μέλλον της χώρας;»** συνοψίζει και εμβαθύνει στα βασικά συμπεράσματα της συζήτησης στρογγυλής τραπέζης που είχε διοργανώσει τον Μάρτιο του 2024 το Center for Cyber Resilience του Οικονομικού Φόρουμ των Δελφών, σε συνεργασία με τον ΕΛΙΑΜΕΠ και με την υποστήριξη της Vodafone Ελλάδας.

Στη συζήτηση στρογγυλής τραπέζης συμμετείχαν οι: Μιχάλης Χρυσοχοΐδης – υπουργός Προστασίας του Πολίτη, Δημήτριος Παπαστεργίου – υπουργός Ψηφιακής Διακυβέρνησης, Δημοσθένης Αναγνωστόπουλος – γενικός γραμματέας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης, Θεμιστοκλής Δεμίρης – διοικητής Εθνικής Υπηρεσίας Πληροφοριών, Βασίλειος Παπακώστας – διευθυντής Δίωξης Ηλεκτρονικού Εγκλήματος, Θωμάς Δομπρίδης – προϊστάμενος της Γενικής Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης, Ιωάννης Πανολίας – διευθυντής Στρατηγικού Σχεδιασμού / Εθνική Αρχή Κυβερνοασφάλειας, Θάνος Ντόκος – σύμβουλος Εθνικής Ασφάλειας του πρωθυπουργού, Σπύρος Παπαγεωργίου – διευθυντής Κυβερνοάμυνας (ΔΙΚΥΒ/ΓΕΕΘΑ) / Υπουργείο Εθνικής Άμυνας, Παρασκευή Δραμαλιώτη – γενική Γραμματέας Συντονισμού, Δημοσθένης Οικονόμου – επικεφαλής Τμ. Ασφάλειας Πληροφοριών και Προστασίας Δεδομένων (ENISA), Στέλλα Τσίτσουλα – πρόεδρος Ελληνικού Ινστιτούτου Κυβερνοασφάλειας, Φαίη Μακαντάση – διευθύντρια Ερευνών / διαΝΕΟσις, Στέφανος Ζήσης – ICT Risk & Cybersecurity Audit and Supervision / Τράπεζα της Ελλάδος, Παναγιώτης Παπαγιαννακόπουλος – εταίρος, αναπληρωτής επικεφαλής υπηρεσιών κυβερνοασφάλειας της EY στην περιοχή της Κεντρικής, Ανατολικής, Νοτιοανατολικής Ευρώπης και Κεντρικής Ασίας (CESA), Χρήστος Βιδάκης – εταίρος, cyber leader / Deloitte, Νίκος Δημάκος – εταίρος & head of Consulting / KPMG, Βασίλειος Κουτεντάκης – ανώτερος γενικός διευθυντής / Τράπεζα Πειραιώς, Νίκος Γιαννακάκης – γενικός διευθυντής Πληροφορικής Motor Oil, Γεωργία Αναστασίου – Cyber & Information Security director / ΟΠΑΠ, Καρώνης Άγγελος – Information Security Senior manager / Kaizen Gaming (Stoiximan/Betano), Δημήτριος Γιάντσης – γενικός διευθυντής Έργων / Κ.Τ.Π.Μ.Α.Ε., Μιχάλης Κασιμιώτης – διευθύνων σύμβουλος / Hewlett Packard Enterprise Ελλάδος και Κύπρου, Δημήτριος Πατσός – Senior Cuber Security specialist / Microsoft, Χρήστος Κοντέλλης – γενικός διευθυντής Ιδιωτικού Τομέα / Netcompany-Intrasoft, Αντώνης Τζωρτζακάκης – διευθύνων σύμβουλος / 5G Συμμετοχές Α.Ε. και επενδυτικού ταμείου Φαιστός, Ευγενία Μπόζου – επικεφαλής Κυβερνητικών Υποθέσεων και Δημόσιας Πολιτικής Google Ελλάδας, Κύπρου, Μάλτας, Δημήτριος Γκρίτζαλης – καθηγητής Κυβερνοασφάλειας στο Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου Αθηνών, Στέφανος Γκρίτζαλης – καθηγητής Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, διευθυντής του Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο και Τεχνολογίες, Πληροφορικής και Επικοινωνιών» (MSc in Law and ICT), Λίλιαν Μήτρου – πρόεδρος Ινστιτούτου για το Δίκαιο Προστασίας της Ιδιωτικότητας, των Προσωπικών Δεδομένων και την Τεχνολογία & καθηγήτρια στο Πανεπιστήμιο Αιγαίου, Κώστας Πατσάκης – αναπληρωτής καθηγητής, Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς, Γιάννης Θωμάτος – διευθύνων σύμβουλος στην Εταιρεία Δημοσίων Σχέσεων και Επικοινωνίας Tsomokos, Χάρης Μπρουμίδης – πρόεδρος και διευθύνων σύμβουλος Vodafone Ελλάδας, Στράτος Φαναράς – πρόεδρος και διευθύνων σύμβουλος της Metron Analysis S.A., Τριαντάφυλλος Καρατράντος – κύριος ερευνητής του ΕΛΙΑΜΕΠ (θεματικές: ριζοσπαστικοποίηση, τρομοκρατία, μοντέλα αστυνόμευσης, ασφάλεια και εξωτερική πολιτική), Απόστολος Μαγγηριάδης – παρουσιαστής ειδήσεων, δημοσιογράφος, Μαρία Σκάγκου – διευθύντρια Νομικών και Κανονιστικών Θεμάτων, Εταιρικής Ασφάλειας & Εταιρικών Σχέσεων Vodafone Ελλάδας.

Το policy paper επιμελήθηκε ο Δρ Τριαντάφυλλος Καρατράντος, κύριος ερευνητής του ΕΛΙΑΜΕΠ, και υποστηρίχθηκε από Ομάδα Έργου αποτελούμενη από τη Δρ Ελένη Καψοκόλη, υποψήφια μεταδιδάκτωρ του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς, και την Ξένια Σταμάτη.

ΟΜΑΔΑ ΕΡΓΟΥ ΕΛΙΑΜΕΠ

Δρ ΤΡΙΑΝΤΑΦΥΛΛΟΣ ΚΑΡΑΤΡΑΝΤΟΣ, συντονιστής Ομάδας Έργου

Είναι διδάκτωρ Ευρωπαϊκής Ασφάλειας και Νέων Απειλών του Πανεπιστημίου Αιγαίου. Είναι κύριος ερευνητής σε ζητήματα ριζοσπαστικοποίησης, τρομοκρατίας, μοντέλων αστυνόμευσης, ασφάλειας και εξωτερικής πολιτικής στο Ελληνικό Ίδρυμα Ευρωπαϊκής και Εξωτερικής Πολιτικής (ΕΛΙΑΜΕΠ). Τον Σεπτέμβριο του 2021, με απόφαση της Ευρωπαϊκής Επιτροπής, ορίστηκε μέλος της Συμβουλευτικής Ομάδας Ερευνητών Υψηλού Επιπέδου (Advisory Board of Researchers) για την έρευνα και την εξέλιξη της πολιτικής ως προς την πρόληψη της ριζοσπαστικοποίησης και την αντιμετώπιση του βίαιου εξτρεμισμού. Από τον Σεπτέμβριο του 2023 έχει οριστεί εθνικός εκπρόσωπος στο High Level Risk Forum του ΟΟΣΑ. Τον Ιούλιο του 2019 μέχρι τον Αύγουστο του 2021 διετέλεσε σύμβουλος Πολιτικής Ασφάλειας του Υπουργού Προστασίας του Πολίτη, ενώ από τον Σεπτέμβριο του 2021 είναι σύμβουλος Πολιτικών Ασφάλειας του υπουργού Επικρατείας.

Δρ ΕΛΕΝΗ ΚΑΨΟΚΟΛΗ, μέλος Ομάδας Έργου

Η Ελένη Καψοκόλη είναι υποψήφια μεταδιδάκτωρ του Τμήματος Διεθνών και Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς. Το 2022 ολοκλήρωσε τη διδακτορική της διατριβή σχετικά με την ισλαμική τρομοκρατία στον κυβερνοχώρο από το ίδιο τμήμα. Είναι πτυχιούχος Πολιτικών Επιστημών και Δημόσιας Διοίκησης από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, και κάτοχος μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις και Στρατηγικές Σπουδές από το Πάντειο Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών. Είναι απόφοιτη της Διδακτορικής Σχολής του Ευρωπαϊκού Κολλεγίου Ασφάλειας και Άμυνας και ερευνήτρια στο Εργαστήριο Πληροφόρησης και Κυβερνοασφάλειας του Τμήματος Διεθνών & Ευρωπαϊκών Σπουδών του Πανεπιστημίου Πειραιώς.

ΞΕΝΙΑ ΣΤΑΜΑΤΗ, μέλος Ομάδας Έργου

Η Ξένια Σταμάτη είναι πτυχιούχος Διεθνών, Ευρωπαϊκών και Περιφερειακών Σπουδών, του Παντείου Πανεπιστημίου, και κάτοχος μεταπτυχιακού διπλώματος στη Διεθνή και Ευρωπαϊκή Διακυβέρνηση και Πολιτική από το Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών. Εργάζεται στον ιδιωτικό τομέα με εξειδίκευση στη διαχείριση έργων, χρησιμοποιώντας εργαλεία όπως το Jira και το Confluence. Τον τελευταίο χρόνο εργάζεται στην Alpha Bank, ως Project & Facilities Manager των 4.500 ακινήτων της. Έχει άριστες γνώσεις αγγλικών και γαλλικών, αλλά και γνώσεις ισπανικών και κινεζικών.