Γνωμοδότηση της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής με θέμα «Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA, τον "οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο", και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών ("πράξη για την ασφάλεια στον κυβερνοχώρο")»

[COM(2017) 477 final/2 2017/0225 (COD)]

(2018/C 227/13)

Εισηγητής: ο κ. **Alberto MAZZOLA**

Συνεισηγητής: ο κ. **Antonio LONGO**

Αίτηση γνωμοδότησης	Ευρωπαϊκό Κοινοβούλιο, 23.10.2017
	Συμβούλιο της Ευρωπαϊκής Ένωσης, 25.10.2017
Νομική βάση:	Άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης
Αρμόδιο τμήμα	Μεταφορές, ενέργεια, υποδομές, κοινωνία των πληροφοριών
Υιοθετήθηκε από το τμήμα	5.2.2018
Υιοθετήθηκε από την ολομέλεια	14.2.2018
Σύνοδος ολομέλειας αριθ.	532
Αποτέλεσμα της ψηφοφορίας	206/1/2
(υπέρ/κατά/αποχές)	

1. **Συμπεράσματα και συστάσεις**

1.1. Η ΕΟΚΕ θεωρεί ότι η νέα μόνιμη εντολή του ENISA, όπως προτείνεται από την Επιτροπή, θα συμβάλει σημαντικά στην ενίσχυση της ανθεκτικότητας των ευρωπαϊκών συστημάτων. Ωστόσο, ο συνοδευτικός προσωρινός προϋπολογισμός και οι πόροι που διατίθενται στον ENISA δεν θα επαρκούν για την εκπλήρωση της εντολής του.

1.2. Η ΕΟΚΕ συνιστά σε όλα τα κράτη μέλη να θεσπίσουν έναν σαφή και ισοδύναμο οργανισμό, ομόλογο του ENISA, καθώς τα περισσότερα δεν το έχουν πράξει ακόμη.

1.3. Η ΕΟΚΕ θεωρεί επίσης ότι, όσον αφορά τη δημιουργία ικανοτήτων, ο ENISA θα πρέπει να δώσει προτεραιότητα σε δράσεις υποστήριξης της ηλεκτρονικής διακυβέρνησης ([1]). Η ψηφιακή ταυτότητα σε ευρωπαϊκό/παγκόσμιο επίπεδο για πρόσωπα, οργανισμούς και αντικείμενα είναι καθοριστικής σημασίας, η δε πρόληψη και καταπολέμηση της κλοπής ταυτότητας και της ηλεκτρονικής απάτης θα πρέπει να αποτελούν προτεραιότητα.

1.4. Η ΕΟΚΕ συνιστά ο ENISA να υποβάλλει τακτικές εκθέσεις σχετικά με την ετοιμότητα των κρατών μελών στον κυβερνοχώρο, εστιάζοντας κυρίως στους τομείς που προσδιορίζονται στο παράρτημα ΙΙ της οδηγίας ΑΔΠ. Ετήσια ευρωπαϊκή άσκηση στον κυβερνοχώρο θα πρέπει να αξιολογεί την ετοιμότητα των κρατών μελών και την αποτελεσματικότητα του ευρωπαϊκού μηχανισμού αντιμετώπισης κρίσεων στον κυβερνοχώρο και να υποβάλλει συστάσεις.

1.5. Η ΕΟΚΕ υποστηρίζει την πρόταση να δημιουργηθεί δίκτυο ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο. Αυτό το δίκτυο θα συντηρείται από ένα Κέντρο Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο (CRCC). Το εν λόγω δίκτυο θα μπορούσε να στηρίξει την ευρωπαϊκή ψηφιακή κυριαρχία αναπτύσσοντας μια ανταγωνιστική ευρωπαϊκή βιομηχανική βάση για τις σημαντικές τεχνολογικές δυνατότητες με βάση το έργο της συμβατικού τύπου σύμπραξης δημόσιου και ιδιωτικού τομέα (ΣΔΙΤ), η οποία θα πρέπει να εξελιχθεί σε τριμερή κοινή επιχείρηση.

1.6. Ο ανθρώπινος παράγοντας αποτελεί μία από τις σημαντικότερες αιτίες ατυχημάτων στον κυβερνοχώρο. Σύμφωνα με την ΕΟΚΕ, είναι αναγκαίο να αναπτυχθεί ισχυρή βάση δεξιοτήτων στον κυβερνοχώρο και να βελτιωθεί η κυβερνοϋγιεινή, μεταξύ άλλων μέσω εκστρατειών ευαισθητοποίησης με αποδέκτες ιδιώτες και επιχειρήσεις. Η ΕΟΚΕ υποστηρίζει τη δημιουργία προγράμματος σπουδών πιστοποιημένου από την ΕΕ για τα σχολεία και τους επαγγελματίες.

([1]) Ψηφιακή ενιαία αγορά: ενδιάμεση αξιολόγηση.

1.7. Η ΕΟΚΕ πιστεύει, αφενός, ότι η ευρωπαϊκή ψηφιακή ενιαία αγορά χρειάζεται επίσης ομοιογενή ερμηνεία των κανόνων για την ασφάλεια στον κυβερνοχώρο, συμπεριλαμβανομένης αμοιβαίας αναγνώρισης μεταξύ των κρατών μελών και, αφετέρου, ότι ένα πλαίσιο πιστοποίησης με συστήματα πιστοποίησης για τους διάφορους τομείς θα μπορούσε να παράσχει μια κοινή βάση. Ωστόσο, πρέπει να προβλεφθούν διαφορετικές προσεγγίσεις για τους διάφορους τομείς, λόγω του τρόπου λειτουργίας τους. Ως εκ τούτου, η ΕΟΚΕ πιστεύει ότι στη διαδικασία θα πρέπει να συμμετέχουν τομεακοί φορείς της ΕΕ (ΕΟΑΑ, ERA, ΕΜΑ κ.λπ.) και, σε ορισμένες περιπτώσεις, με τη σύμφωνη γνώμη του ENISA για τη διασφάλιση της συνέπειας, να τους ανατίθεται η εκπόνηση συστημάτων ασφάλειας στον κυβερνοχώρο. Πρέπει να υιοθετηθούν ελάχιστα ευρωπαϊκά πρότυπα για την ασφάλεια στον τομέα της ΤΠ σε συνεργασία με τη CEN, τη Cenelec και το ETSI.

1.8. Η προβλεπόμενη ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο υπό την υποστήριξη του ENISA θα πρέπει να αποτελείται από εθνικά εποπτικά όργανα πιστοποίησης, ενδιαφερόμενους φορείς του ιδιωτικού τομέα, συμπεριλαμβανομένων παραγόντων από διάφορες εφαρμογές, και επιστημονικούς φορείς και φορείς της κοινωνίας των πολιτών.

1.9. Η ΕΟΚΕ θεωρεί ότι ο οργανισμός θα πρέπει να παρακολουθεί τις επιδόσεις και τη λήψη αποφάσεων των εθνικών εποπτικών αρχών πιστοποίησης μέσω ελέγχων και επιθεωρήσεων εξ ονόματος της Επιτροπής και ότι ο κανονισμός θα πρέπει να ορίζει τις αρμοδιότητες και τις κυρώσεις για τη μη τήρηση των προδιαγραφών.

1.10. Η ΕΟΚΕ πιστεύει ότι από τις δραστηριότητες πιστοποίησης δεν μπορεί να αποκλείεται ένα κατάλληλο σύστημα επισήμανσης, το οποίο θα εφαρμόζεται και στα εισαγόμενα προϊόντα προς ενίσχυση της εμπιστοσύνης των καταναλωτών.

1.11. Η Ευρώπη θα πρέπει να αυξήσει τις επενδύσεις με τη σύγκλιση διαφόρων κονδυλίων της ΕΕ, εθνικών κεφαλαίων και επενδύσεων του ιδιωτικού τομέα προς την κατεύθυνση στρατηγικών στόχων με ισχυρή συνεργασία δημόσιου-ιδιωτικού τομέα, καθώς και μέσω της δημιουργίας ενωσιακού Ταμείου Κυβερνοασφάλειας για την καινοτομία και την Ε&Α στο τρέχον και στο μελλοντικό πρόγραμμα-πλαίσιο για την έρευνα. Επιπλέον, η Ευρώπη θα πρέπει να δημιουργήσει ένα ταμείο για την ανάπτυξη της κυβερνοασφάλειας, προσθέτοντας μια νέα πτυχή στον τρέχοντα και στο μελλοντικό μηχανισμό «Συνδέοντας την Ευρώπη» καθώς και στο επόμενο ΕΤΣΕ 3.0.

1.12. Η ΕΟΚΕ πιστεύει ότι απαιτείται ένα ελάχιστο επίπεδο ασφάλειας για τις «συνήθεις» συσκευές του «διαδικτύου των προσώπων» (IoP). Στην περίπτωση αυτή, η πιστοποίηση αποτελεί βασική μέθοδο παροχής υψηλότερου επιπέδου ασφάλειας. Η ασφάλεια του διαδικτύου των πραγμάτων (IoT) πρέπει να αποτελεί προτεραιότητα.

2. **Το υφιστάμενο πλαίσιο πιστοποίησης της ασφάλειας στον κυβερνοχώρο**

2.1. Η ασφάλεια στον κυβερνοχώρο είναι κρίσιμης σημασίας για την ευημερία και την εθνική ασφάλεια, καθώς και για την ίδια τη λειτουργία των δημοκρατιών μας, των ελευθεριών και των αξιών μας. «Η ασφάλεια στον κυβερνοχώρο είναι ένα οικοσύστημα όπου οι νόμοι, οι οργανώσεις, οι δεξιότητες, η συνεργασία και η τεχνική εφαρμογή πρέπει να συνδυάζονται αρμονικά για να είναι πιο αποτελεσματικά», αναφέρει ο Παγκόσμιος δείκτης ασφάλειας στον κυβερνοχώρο των Ηνωμένων Εθνών, προσθέτοντας ότι η ασφάλεια στον κυβερνοχώρο «καταλαμβάνει ολοένα και σημαντικότερη θέση στο σκεπτικό των υπεύθυνων λήψης αποφάσεων των χωρών».

2.2. Η ανάγκη για ένα ασφαλές οικοσύστημα καθίσταται ζωτικής σημασίας λόγω της επανάστασης του διαδικτύου. Η επανάσταση αυτή δεν έχει μόνο επαναπροσδιορίσει τις βιομηχανίες συναλλαγών επιχειρήσεων-καταναλωτών (B2C), όπως τα μέσα μαζικής ενημέρωσης, οι λιανικές και οι χρηματοπιστωτικές υπηρεσίες, αλλά και αναδιαρθρώνει τη μεταποίηση, την ενέργεια, τη γεωργία, τις μεταφορές και άλλους βιομηχανικούς τομείς της οικονομίας που μαζί αντιπροσωπεύουν τα δύο τρίτα σχεδόν του παγκόσμιου ακαθάριστου εγχώριου προϊόντος, καθώς και τις υποδομές των επιχειρήσεων κοινής ωφελείας και τις αλληλεπιδράσεις των ανθρώπων με τη δημόσια διοίκηση.

2.3. Η στρατηγική για την ψηφιακή ενιαία αγορά βασίζεται στη βελτίωση της πρόσβασης σε αγαθά, υπηρεσίες και περιεχόμενο, δημιουργώντας το κατάλληλο νομικό πλαίσιο για τα ψηφιακά δίκτυα και υπηρεσίες και αξιοποιώντας τα οφέλη μιας οικονομίας με βάση τα δεδομένα. Εκτιμάται ότι η στρατηγική θα μπορούσε να συνεισφέρει 415 δισεκατομμύρια ευρώ ετησίως στην οικονομία της ΕΕ. Το χάσμα δεξιοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο για τους επαγγελματίες του ιδιωτικού τομέα στην Ευρώπη προβλέπεται να ανέρθει στα 350.000 άτομα έως το 2022 ([2]).

([2]) OJ JOIN/2017/0450 final.

2.4. Σύμφωνα με εκτιμήσεις μελέτης του 2014, ο οικονομικός αντίκτυπος της εγκληματικότητας στον κυβερνοχώρο στην Ένωση ανερχόταν στο 0,41 % του ΑΕγχΠ της ΕΕ (δηλαδή περίπου 55 δισεκατ. ευρώ) το 2013 ([3]).

2.5. Σύμφωνα με την ειδική έκδοση του Ευρωβαρομέτρου 464α σχετικά με τη στάση των Ευρωπαίων απέναντι στην ασφάλεια στον κυβερνοχώρο, το 73 % των χρηστών του διαδικτύου εκφράζει την ανησυχία ότι οι ηλεκτρονικές προσωπικές τους πληροφορίες ενδέχεται να μην φυλάσσονται κατά τρόπο ασφαλή από τους ιστοτόπους και το 65 % ότι ενδέχεται να μην φυλάσσονται κατά τρόπο ασφαλή από τις δημόσιες αρχές. Οι περισσότεροι ερωτηθέντες ανησυχούν για το ενδεχόμενο να πέσουν θύματα διάφορων μορφών εγκληματικότητας στον κυβερνοχώρο, και ειδικότερα για το κακόβουλο λογισμικό στις συσκευές τους (69 %), την κλοπή ταυτότητας (69 %) και την απάτη μέσω τραπεζικών καρτών και ηλεκτρονικών τραπεζικών συναλλαγών (66 %) ([4]).

2.6. Μέχρι στιγμής, κανένα νομικό πλαίσιο δεν μπόρεσε να αντεπεξέλθει στον ρυθμό της ψηφιακής καινοτομίας, ορισμένα δε νομικά κείμενα συνεισφέρουν ανά αντικείμενο στη δημιουργία του κατάλληλου πλαισίου: η αναθεώρηση του κώδικα για τις τηλεπικοινωνίες, ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ), η οδηγία για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (οδηγία ΑΔΠ), ο κανονισμός σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (κανονισμός e-IDAS), η ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ–ΗΠΑ, η οδηγία σχετικά με τις απάτες πληρωμών πλην των μετρητών και ούτω καθεξής.

2.7. Υπάρχουν πολλοί διαφορετικοί οργανισμοί πέρα από τον ENISA, του «ενωσιακού οργανισμού για την ασφάλεια στον κυβερνοχώρο» που ασχολούνται με θέματα ασφάλειας στον κυβερνοχώρο: η Ευρωπόλ, η Cert-EU (Ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική της Ευρωπαϊκής Ένωσης), το Κέντρο ανάλυσης πληροφοριών της ΕΕ (EU INTCEN), ο Ευρωπαϊκός Οργανισμός για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης (eu-LISA), τα κέντρα κοινοχρησίας και ανάλυσης πληροφοριών (ISAC), ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια στον Κυβερνοχώρο (ECSO), ο Ευρωπαϊκός Οργανισμός Άμυνας (ΕΟΑ), το Συνεργατικό Κέντρο Αριστείας για την Άμυνα στον Κυβερνοχώρο του ΝΑΤΟ και η GGE των Ηνωμένων Εθνών (Ομάδα κυβερνητικών εμπειρογνωμόνων των Ηνωμένων Εθνών για τις εξελίξεις στον τομέα των πληροφοριών και των τηλεπικοινωνιών στο πλαίσιο της διεθνούς ασφάλειας).

2.8. Η ασφάλεια εκ σχεδιασμού είναι κομβικής σημασίας για την παροχή αγαθών και υπηρεσιών υψηλής ποιότητας: οι έξυπνες συσκευές δεν είναι και τόσο έξυπνες εάν δεν είναι ασφαλείς, και το ίδιο ισχύει για τα έξυπνα αυτοκίνητα, τις έξυπνες πόλεις και τα έξυπνα νοσοκομεία — όλα απαιτούν ενσωματωμένη ασφάλεια για τις συσκευές, τα συστήματα, τις αρχιτεκτονικές και τις υπηρεσίες.

2.9. Στις 19-20 Οκτωβρίου 2017, το Ευρωπαϊκό Συμβούλιο ζήτησε την υιοθέτηση κοινής προσέγγισης για την ασφάλεια στον κυβερνοχώρο της ΕΕ μετά την προτεινόμενη μεταρρυθμιστική δέσμη ζητώντας «κοινή προσέγγιση για την ασφάλεια στον κυβερνοχώρο: ο ψηφιακός κόσμος απαιτεί εμπιστοσύνη και η εμπιστοσύνη μπορεί να επιτευχθεί μόνον αν εξασφαλίσουμε πιο προορατική ασφάλεια βάσει σχεδιασμού σε όλες τις ψηφιακές πολιτικές, αν παράσχουμε επαρκή πιστοποίηση της ασφάλειας των προϊόντων και υπηρεσιών και αν αυξήσουμε την ικανότητά μας πρόληψης, αποτροπής, εντοπισμού και αντιμετώπισης των επιθέσεων στον κυβερνοχώρο» ([5]).

2.10. Στο ψήφισμά του της 17ης Μαΐου 2017, το Ευρωπαϊκό Κοινοβούλιο «τονίζει την ανάγκη να υπάρχει ασφάλεια από άκρο σε άκρο σε ολόκληρη την αλυσίδα αξίας των χρηματοπιστωτικών υπηρεσιών· επισημαίνει τους μεγάλους και ποικίλους κινδύνους των επιθέσεων στον κυβερνοχώρο, που έχουν ως στόχο τις υποδομές των χρηματοπιστωτικών αγορών μας, το Διαδίκτυο των Πραγμάτων, τα νομίσματα και τα δεδομένα μας· […] καλεί τις ΕΕΑ να επανεξετάζουν τακτικά τα επιχειρησιακά πρότυπα που καλύπτουν τους κινδύνους ΤΠΕ στα χρηματοπιστωτικά ιδρύματα· ζητεί, επιπλέον, να καταρτιστούν κατευθυντήριες γραμμές από τις ΕΕΑ σχετικά με την εποπτεία των κινδύνων των κρατών μελών στον κυβερνοχώρο· τονίζει τη σημασία της τεχνολογικής τεχνογνωσίας στις ΕΕΑ» ([6]).

2.11. Η ΕΟΚΕ είχε αρκετές ευκαιρίες στο παρελθόν να εξετάσει το θέμα ([7]), συμπεριλαμβανομένου του συνεδρίου για τη μελλοντική ανάπτυξη της ηλεκτρονικής διακυβέρνησης ([8]) κατά τη διάρκεια της διάσκεψης κορυφής του Ταλίν, δημιούργησε δε μόνιμη ομάδα μελέτης για το ψηφιακό θεματολόγιο.

([3]) Έγγραφο εργασίας των υπηρεσιών της Επιτροπής — Εκτίμηση των επιπτώσεων που συνοδεύει την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, Μέρος 1/6, σ. 21, Βρυξέλλες, 13/9/17.

([4]) Ειδική έκδοση του Ευρωβαρομέτρου 464α — Κύμα EB87.4 — Στάση των Ευρωπαίων απέναντι στην ασφάλεια στον κυβερνοχώρο, Σεπτέμβριος 2017.

([5]) Συμπεράσματα του Ευρωπαϊκού Συμβουλίου της 19ης Οκτωβρίου 2017.

([6]) Ψήφισμα του ΕΚ της 17.5.2017 — A8-0176/2017.

([7]) Ψηφιακή ενιαία αγορά: ενδιάμεση αξιολόγηση.ΕΕ C 75, 10.3.2017, σ. 124, ΕΕ C 246, 28.7.2017, σ. 8, ΕΕ C 345, 13.10.2017, σ. 52, ΕΕ C 288, 31.8.2017, σ. 62, ΕΕ C 271, 19.9.2013, σ. 133.

([8]) Ανακοίνωση τύπου της ΕΟΚΕ αριθ. ° 31/2017: Η κοινωνία των πολιτών εξετάζει την ηλεκτρονική διακυβέρνηση και την κυβερνοασφάλεια με την επερχόμενη Εσθονική Προεδρία: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incoming-estonian-presidency

3. **Οι προτάσεις της Επιτροπής**

3.1. Η δέσμη μέτρων για την ασφάλεια στον κυβερνοχώρο περιλαμβάνει μια κοινή ανακοίνωση που επανεξετάζει την προηγούμενη ευρωπαϊκή στρατηγική στον τομέα της ασφάλειας στον κυβερνοχώρο (2013), καθώς και έναν νόμο περί ασφάλειας στον κυβερνοχώρο με επίκεντρο τη νέα εντολή του ENISA και το προτεινόμενο πλαίσιο πιστοποίησης.

3.2. Η στρατηγική διαρθρώνεται γύρω από τρία βασικά τμήματα: την ανθεκτικότητα, την αποτροπή και τη διεθνή συνεργασία. Το τμήμα περί αποτροπής επικεντρώνεται κυρίως στα ζητήματα της εγκληματικής δραστηριότητας στον κυβερνοχώρο, συμπεριλαμβανομένης της σύμβασης της Βουδαπέστης, ενώ το τμήμα περί διεθνούς συνεργασίας εξετάζει την άμυνα στον κυβερνοχώρο, τη διπλωματία στον κυβερνοχώρο και τη συνεργασία με το ΝΑΤΟ.

3.3. Η πρόταση περιέχει σειρά νέων πρωτοβουλιών όπως:

— δημιουργία ισχυρότερου ενωσιακού οργανισμού για την ασφάλεια στον κυβερνοχώρο,

— θέσπιση ενωσιακού συστήματος πιστοποίησης της ασφάλειας στον κυβερνοχώρο,

— ταχεία εφαρμογή της οδηγίας ΑΔΠ

3.4. Το τμήμα περί ανθεκτικότητας προτείνει δράσεις σχετικές με την ασφάλεια στον κυβερνοχώρο, οι οποίες αφορούν ειδικότερα: ζητήματα αγοράς, την οδηγία ΑΔΠ, την ταχεία αντιμετώπιση καταστάσεων έκτακτης ανάγκης, την ανάπτυξη ικανοτήτων της ΕΕ, την εκπαίδευση, την κατάρτιση -στις δεξιότητες στον κυβερνοχώρο και την υγιεινή στον κυβερνοχώρο- και την ευαισθητοποίηση.

3.5. Παράλληλα, ο νόμος περί ασφάλειας στον κυβερνοχώρο προτείνει τη δημιουργία ενωσιακού πλαισίου πιστοποίησης για την ασφάλεια στον κυβερνοχώρο για τα προϊόντα και τις υπηρεσίες ΤΠΕ.

3.6. Ο νόμος περί ασφάλειας στον κυβερνοχώρο προτείνει επίσης την ενίσχυση του ρόλου του ENISA ως οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο, παρέχοντας στον εν λόγω φορέα μόνιμη εντολή. Εκτός από τις τρέχουσες αρμοδιότητές του, ο ENISA αναμένεται να καλύψει και νέα καθήκοντα υποστήριξης και συντονισμού σχετικά με τη στήριξη της εφαρμογής της οδηγίας ΑΔΠ, τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο, το προσχέδιο, την ανάπτυξη ικανοτήτων, τις γνώσεις και τις πληροφορίες, την ευαισθητοποίηση, καθήκοντα σχετικά με την αγορά όπως η υποστήριξη της τυποποίησης και της πιστοποίησης, η έρευνα και καινοτομία, οι πανευρωπαϊκές ασκήσεις ασφάλειας στον κυβερνοχώρο και η γραμματειακή υποστήριξη του δικτύου των ομάδων αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (CSIRT).

4. **Γενικές παρατηρήσεις — Επισκόπηση**

4.1. ***Πλαίσιο: Ανθεκτικότητα***

4.1.1. *Ενιαία αγορά ασφάλειας στον κυβερνοχώρο*

Καθήκον επιμέλειας: Η ανάπτυξη της προτεινόμενης αρχής του «καθήκοντος επιμέλειας» που αναφέρεται στην κοινή ανακοίνωση για τη χρήση ασφαλών διαδικασιών κύκλου ζωής ανάπτυξης αποτελεί ενδιαφέρουσα ιδέα που πρέπει να αναπτυχθεί στη βιομηχανία της ΕΕ, γεγονός το οποίο θα μπορούσε να οδηγήσει σε συνολική προσέγγιση για τη συμμόρφωση με την κοινοτική νομοθεσία. Εξ ορισμού, η ασφάλεια πρέπει να συνεξετάζεται στις μελλοντικές εξελίξεις.

Ευθύνη: Η πιστοποίηση θα διευκολύνει την απόδοση ευθύνης σε περίπτωση διαφωνίας.

4.1.2. Οδηγία ΑΔΠ: ενέργεια, μεταφορές, τραπεζικές/χρηματοοικονομικές υπηρεσίες, υγεία, νερό, ψηφιακή υποδομή, ηλεκτρονικό εμπόριο.

Κατά την ΕΟΚΕ, η πλήρης και αποτελεσματική εφαρμογή της οδηγίας ΑΔΠ είναι απαραίτητη προκειμένου να διασφαλιστεί η ανθεκτικότητα των εθνικών κρίσιμων τομέων.

Η ΕΟΚΕ πιστεύει ότι πρέπει να ενισχυθεί η ανταλλαγή πληροφοριών μεταξύ δημόσιων και ιδιωτικών φορέων μέσω των τομεακών κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC). Θα πρέπει να αναπτυχθεί ο κατάλληλος μηχανισμός για την ασφαλή ανταλλαγή εμπιστευτικών πληροφοριών εντός ενός ISAC, αλλά και μεταξύ CSIRT και ISAC, βάσει αξιολόγησης/ανάλυσης του μηχανισμού που χρησιμοποιείται σήμερα.

4.1.3. *Ταχεία αντιμετώπιση καταστάσεων έκτακτης ανάγκης*

Το «πρότυπο» προσέγγισης μπορεί να παράσχει μια αποτελεσματική διαδικασία στο πλαίσιο της επιχειρησιακής αντιμετώπισης περιστατικών μεγάλης κλίμακας, τόσο σε ενωσιακό επίπεδο όσο και σε επίπεδο κρατών μελών. Η ΕΟΚΕ υπογραμμίζει την ανάγκη συμμετοχής του ιδιωτικού τομέα. Πρέπει επίσης να λαμβάνονται υπόψη οι φορείς παροχής βασικών υπηρεσιών στο μηχανισμό επιχειρησιακής αντιμετώπισης, καθώς θα μπορούσαν να παρέχουν πολύτιμες πληροφορίες σχετικά με τις απειλές ή/και να στηρίζουν την ανίχνευση και την αντιμετώπιση απειλών και κρίσεων μεγάλης κλίμακας.

Η κοινή ανακοίνωση προτείνει την ενσωμάτωση των περιστατικών στον κυβερνοχώρο στους μηχανισμούς διαχείρισης κρίσεων της ΕΕ. Αν και η ΕΟΚΕ αντιλαμβάνεται την ανάγκη συλλογικής αντίδρασης και αλληλεγγύης σε περίπτωση επίθεσης, απαιτείται καλύτερη κατανόηση του τρόπου με τον οποίο θα μπορούσε να εφαρμοστεί αυτό, καθώς οι απειλές στον κυβερνοχώρο συνήθως διαδίδονται μεταξύ των χωρών. Τα εργαλεία που χρησιμοποιούνται σε εθνικές καταστάσεις έκτακτης ανάγκης μπορούν να χρησιμοποιηθούν μερικώς μόνο σε περίπτωση τοπικής ανάγκης.

4.1.4. *Ανάπτυξη ικανοτήτων της ΕΕ*

Προκειμένου η ΕΕ να είναι πραγματικά ανταγωνιστική σε παγκόσμιο επίπεδο και να οικοδομήσει στιβαρή τεχνολογική βάση, είναι ουσιαστικής σημασίας η θέσπιση συνεπούς, μακροπρόθεσμου πλαισίου που θα καλύπτει όλα τα στάδια της αξιακής αλυσίδας της ασφάλειας στον κυβερνοχώρο. Προς τούτο, η προώθηση της συνεργασίας μεταξύ των ευρωπαϊκών περιφερειακών οικοσυστημάτων είναι κομβικής σημασίας για την ανάπτυξη ευρωπαϊκής αλυσίδας αξίας για την ασφάλεια στον κυβερνοχώρο. Η ΕΟΚΕ εκφράζει την ικανοποίησή της για την πρόταση να δημιουργηθεί δίκτυο ικανοτήτων στον τομέα της ασφάλειας στον κυβερνοχώρο.

Το εν λόγω δίκτυο θα μπορούσε να στηρίξει την ευρωπαϊκή ψηφιακή κυριαρχία αναπτύσσοντας μια ανταγωνιστική ευρωπαϊκή βιομηχανική βάση και, μειώνοντας την εξάρτηση από την τεχνογνωσία που αναπτύσσεται εκτός της ΕΕ για τις σημαντικές τεχνολογικές δυνατότητες, να παράσχει τεχνικές ασκήσεις, εργαστήρια και ακόμη και βασική κατάρτιση για την κυβερνοϋγιεινή για επαγγελματίες και μη επαγγελματίες, καθώς και να ενθαρρύνει -με βάση το έργο της ΣΔΙΤ- την ανάπτυξη ενός δικτύου εθνικών οργανισμών δημόσιου-ιδιωτικού τομέα για τη στήριξη της ανάπτυξης αγοράς στην Ευρώπη. «Η προώθηση της ΣΔΙΤ θα πρέπει να οδηγήσει στη βελτιστοποίηση, προσαρμογή ή επέκτασή του» (EE-BG-AT Trio Presidency Cybersecurity Work Programme) μέσω της θέσπισης τριμερούς κοινής επιχείρησης (της Επιτροπής, των κρατών μελών και των επιχειρήσεων).

Για να είναι αποτελεσματικό και να επιτύχει τους προτεινόμενους στόχους του σε ευρωπαϊκό επίπεδο, το δίκτυο πρέπει να βασίζεται σε ένα σαφώς καθορισμένο σύστημα διακυβέρνησης.

Το δίκτυο θα υποστηρίζεται από ένα Κέντρο Έρευνας και Ικανοτήτων Ασφάλειας στον Κυβερνοχώρο (CRCC) σε ευρωπαϊκό επίπεδο, το οποίο θα συνδέει τα υφιστάμενα εθνικά κέντρα ικανοτήτων σε ολόκληρη την ΕΕ. Το CRCC όχι μόνο θα συντονίζει και θα διαχειρίζεται την έρευνα όπως και σε άλλες κοινές επιχειρήσεις, αλλά και θα επιτρέπει την αποτελεσματική ανάπτυξη ενός ευρωπαϊκού οικοσυστήματος ασφάλειας του κυβερνοχώρου που θα υποστηρίζει την υλοποίηση και ανάπτυξη της ενωσιακής καινοτομίας.

4.2. ***Πλαίσιο: Αποτροπή***

4.2.1. Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο αποτελεί ύψιστη προτεραιότητα σε εθνικό και ευρωπαϊκό επίπεδο, η οποία απαιτεί ισχυρή πολιτική δέσμευση. Οι δραστηριότητες αποτροπής θα πρέπει να διεξάγονται βάσει ισχυρής εταιρικής σχέσης μεταξύ του δημόσιου και του ιδιωτικού τομέα, με την καθιέρωση αποτελεσματικής ανταλλαγής πληροφοριών και εμπειρογνωμοσύνης τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο. Θα μπορούσε να προβλεφθεί η δυνατότητα επέκτασης των δραστηριοτήτων της Ευρωπόλ στον τομέα της εγκληματολογίας στον κυβερνοχώρο και της παρακολούθησης.

4.3. ***Πλαίσιο: Διεθνής συνεργασία***

4.3.1. Η ανάπτυξη και η διατήρηση αξιόπιστης συνεργασίας με τρίτες χώρες μέσω της διπλωματίας στον κυβερνοχώρο και των εταιρικών σχέσεων είναι αποφασιστικής σημασίας για την ενίσχυση της ικανότητας της Ευρώπης να προλαμβάνει, να αποτρέπει και να ανταποκρίνεται σε επιθέσεις μεγάλης κλίμακας στον κυβερνοχώρο. Η Ευρώπη θα πρέπει να προωθήσει τη συνεργασία της με τις ΗΠΑ, την Κίνα, το Ισραήλ, την Ινδία και την Ιαπωνία. Ο εκσυγχρονισμός των ελέγχων των εξαγωγών της ΕΕ θα πρέπει να αποτρέπει τις παραβιάσεις των ανθρωπίνων δικαιωμάτων ή τη χρήση των τεχνολογιών σε βάρος της ίδιας της ασφάλειας της ΕΕ, αλλά και να διασφαλίζει ότι η βιομηχανία της ΕΕ δεν τιμωρείται σε σχέση με τις προσφορές τρίτων χωρών. Θα πρέπει να προβλεφθεί ειδική στρατηγική για τις υποψήφιες προς ένταξη χώρες με σκοπό την προετοιμασία της ανταλλαγής ευαίσθητων διασυνοριακών δεδομένων, συμπεριλαμβανομένης της δυνατότητας συμμετοχής, ως παρατηρητών, σε ορισμένες δραστηριότητες των χωρών του ENISA — πρέπει δε αυτές να ταξινομούνται ανάλογα με την αποφασιστικότητα με την οποία καταπολεμούν το έγκλημα στον κυβερνοχώρο, ενώ θα μπορούσε να δημιουργηθεί και «μαύρη λίστα».

4.3.2. Η ΕΟΚΕ εκφράζει την ικανοποίησή της για τη θέσπιση αμυντικής πολιτικής στον κυβερνοχώρο στην προβλεπόμενη δεύτερη φάση ενός πιθανού μελλοντικού κέντρου ικανοτήτων της ΕΕ στον τομέα της ασφάλειας στον κυβερνοχώρο. Για τον λόγο αυτό, εν τω μεταξύ, η Ευρώπη θα μπορούσε να εξετάσει την ανάπτυξη ικανοτήτων διπλής χρήσης, συμπεριλαμβανομένης της αξιοποίησης του Ευρωπαϊκού Ταμείου Άμυνας και της προγραμματισμένης δημιουργίας, μέχρι το 2018, μιας πλατφόρμας κατάρτισης και εκπαίδευσης στον τομέα της άμυνας στον κυβερνοχώρο. Δεδομένων του αμοιβαία αναγνωρισμένου δυναμικού και των απειλών, η ΕΟΚΕ κρίνει αναγκαία την ανάπτυξη της συνεργασίας ΕΕ-ΝΑΤΟ, ενώ η ευρωπαϊκή βιομηχανία πρέπει επίσης να παρακολουθεί στενά τις εξελίξεις στη συνεργασία ΕΕ-ΝΑΤΟ σχετικά με την ενίσχυση της διαλειτουργικότητας των προτύπων ασφάλειας στον κυβερνοχώρο και άλλες μορφές συνεργασίας στο πλαίσιο της προσέγγισης της ΕΕ όσον αφορά την άμυνα στον κυβερνοχώρο.

4.4. ***Πλαίσιο πιστοποίησης της ΕΕ***

4.4.1. Η ΕΟΚΕ πιστεύει ότι η Ευρώπη πρέπει να αντιμετωπίσει την πρόκληση του κατακερματισμού της ασφάλειας στον κυβερνοχώρο με μια ομοιογενή ερμηνεία των κανόνων, συμπεριλαμβανομένης αμοιβαίας αναγνώρισης μεταξύ των κρατών μελών στο πλαίσιο μιας ενιαίας διαδικασίας ώστε να διευκολύνεται η προστασία της ψηφιακής ενιαίας αγοράς. Ένα πλαίσιο πιστοποίησης θα μπορούσε να παράσχει μια κοινή βάση (με ειδικές ρυθμίσεις σε υψηλότερα επίπεδα, όπου απαιτείται), διασφαλίζοντας συνέργειες σε κάθετους τομείς και μειώνοντας τον σημερινό κατακερματισμό.

4.4.2. Η ΕΟΚΕ εκφράζει την ικανοποίησή της για τη δημιουργία ευρωπαϊκού πλαισίου πιστοποίησης για την ασφάλεια στον κυβερνοχώρο και συστημάτων πιστοποίησης για τους διάφορους τομείς βάσει επαρκών απαιτήσεων και σε συνεργασία με τους κύριους ενδιαφερόμενους. Ωστόσο, ο χρόνος που απαιτείται για την είσοδο στην αγορά και το κόστος πιστοποίησης, καθώς και η ποιότητα και η ασφάλεια, είναι βασικά στοιχεία που πρέπει να λαμβάνονται υπόψη. Θα θεσπιστούν συστήματα πιστοποίησης για την ενίσχυση της ασφάλειας σύμφωνα με τις υφιστάμενες ανάγκες και τη γνώση σχετικά με τις απειλές: η ευελιξία και η ικανότητα εξέλιξης αυτών των συστημάτων πρέπει να συνεξεταστούν προκειμένου να επιτραπούν οι απαραίτητες επικαιροποιήσεις. Πρέπει να προβλεφθούν διαφορετικές προσεγγίσεις για τους διάφορους τομείς, λόγω του τρόπου λειτουργίας τους. Ως εκ τούτου, η ΕΟΚΕ πιστεύει ότι στη διαδικασία θα πρέπει να συμμετέχουν τομεακοί φορείς της ΕΕ (ΕΟΑΑ, ΕΑΤ, ERA, ΕΜΑ κ.λπ.) και, σε ορισμένες περιπτώσεις, με τη σύμφωνη γνώμη του ENISA, να τους ανατίθεται να εκπονούν συστήματα ασφάλειας στον κυβερνοχώρο, προς αποφυγή αλληλοεπικαλύψεων και εξασφάλιση συνέπειας.

4.4.3. Σύμφωνα με την ΕΟΚΕ, είναι σημαντικό το πλαίσιο πιστοποίησης να βασίζεται σε κοινά καθορισμένα ευρωπαϊκά πρότυπα στον τομέα της ασφάλειας στον κυβερνοχώρο και των ΤΠΕ που θα είναι στο μέτρο του δυνατού, διεθνώς αναγνωρισμένα. Λαμβάνοντας υπόψη το χρονοδιάγραμμα και τα εθνικά προνόμια, θα πρέπει να υιοθετηθούν ελάχιστα ευρωπαϊκά πρότυπα για την ασφάλεια στον τομέα της ΤΠ σε συνεργασία με τη CEN, τη Cenelec και το ETSI. Τα επαγγελματικά πρότυπα θα πρέπει να θεωρούνται θετικό στοιχείο, δεν θα πρέπει όμως να είναι νομικά δεσμευτικά ή να παρεμποδίζουν τον ανταγωνισμό.

4.4.4. Υπάρχει σαφής ανάγκη να συσχετιστούν οι ευθύνες με τα διαφορετικά επίπεδα διασφάλισης βάσει του αντικτύπου των απειλών. Η έναρξη διαλόγου με τις ασφαλιστικές εταιρείες θα μπορούσε να ωφελήσει τη θέσπιση αποτελεσματικών απαιτήσεων στον τομέα της ασφάλειας στον κυβερνοχώρο, ανάλογα με τον τομέα εφαρμογής. Κατά την άποψη της ΕΟΚΕ, θα πρέπει να υποστηριχθούν και να ενθαρρυνθούν οι εταιρείες που αναζητούν «υψηλό επίπεδο διασφάλισης», ιδίως για συσκευές και συστήματα ζωτικής σημασίας.

4.4.5. Δεδομένου του χρόνου που μεσολάβησε από την υιοθέτηση της Οδηγίας 85/374/ΕΟΚ ([9]), και υπό το φως των τρεχουσών τεχνολογικών εξελίξεων, η ΕΟΚΕ καλεί την Επιτροπή να εξετάσει κατά πόσον είναι σκόπιμο να συμπεριληφθούν στο πεδίο εφαρμογής της οδηγίας ορισμένα από τα σενάρια που παρατίθενται στην πρόταση κανονισμού, προκειμένου να βελτιωθεί η ασφάλεια και το επίπεδο προστασίας των προϊόντων.

4.4.6. Η ΕΟΚΕ εκτιμά ότι η προβλεπόμενη ευρωπαϊκή ομάδα πιστοποίησης της ασφάλειας στον κυβερνοχώρο υπό την υποστήριξη του ENISA θα πρέπει να αποτελείται από εθνικά εποπτικά όργανα πιστοποίησης, ενδιαφερόμενους φορείς του ιδιωτικού τομέα και παράγοντες από διάφορα πεδία εφαρμογών, ώστε να διασφαλίζεται η ανάπτυξη ολοκληρωμένων συστημάτων πιστοποίησης. Επιπλέον, θα πρέπει να προβλέπεται συνεργασία μεταξύ της εν λόγω ομάδας και αντιπροσωπευτικών φορέων των κλάδων της ΕΕ/του ΕΟΧ (π.χ. ΣΔΙΤ, τράπεζες, μεταφορές, ενέργεια, ομοσπονδίες κ.λπ.) μέσω του διορισμού εμπειρογνωμόνων. Η ομάδα αυτή θα πρέπει να μπορεί να εξετάζει τα ευρωπαϊκά επιτεύγματα όσον αφορά την πιστοποίηση (βασισμένη κυρίως στη Συμφωνία Αμοιβαίας Αναγνώρισης (ΣΑΑ) SO-GIS, στα εθνικά συστήματα και τα ιδιοκτησιακά καθεστώτα) και να αποσκοπεί στη διατήρηση των ευρωπαϊκών ανταγωνιστικών πλεονεκτημάτων.

([9]) ΕΕ L 210 της 7.8. 1985, σ. 29.

4.4.7. Η ΕΟΚΕ προτείνει να ανατεθεί σε αυτήν την ομάδα ενδιαφερομένων η ευθύνη για την από κοινού προετοιμασία συστημάτων πιστοποίησης, σε συνεργασία με την Ευρωπαϊκή Επιτροπή. Θα πρέπει επίσης να καθοριστούν τομεακές απαιτήσεις με συναινετική συμφωνία μεταξύ δημόσιων και ιδιωτικών ενδιαφερόμενων φορέων (χρηστών και προμηθευτών).

4.4.8. Επιπλέον, η ομάδα θα πρέπει να επανεξετάζει τακτικά τα συστήματα πιστοποίησης λαμβάνοντας υπόψη τις απαιτήσεις κάθε τομέα και να προσαρμόζει τα συστήματα όταν είναι απαραίτητο.

4.4.9. Η ΕΟΚΕ υποστηρίζει τη σταδιακή κατάργηση των εθνικών συστημάτων πιστοποίησης μετά την εισαγωγή του ευρωπαϊκού συστήματος, όπως προτείνεται στο άρθρο 49 του κανονισμού. Η ενιαία αγορά δεν μπορεί να λειτουργεί με διαφορετικούς και ανταγωνιστικούς εθνικούς κανόνες. Για τον σκοπό αυτό, η ΕΟΚΕ προτείνει να γίνει απογραφή όλων των εθνικών συστημάτων.

4.4.10. Η ΕΟΚΕ συνιστά στην Επιτροπή να δρομολογήσει δράση για την προώθηση της πιστοποίησης και των πιστοποιητικών ασφάλειας στον κυβερνοχώρο στην ΕΕ και τη στήριξη της αναγνώρισής τους σε όλες τις διεθνείς εμπορικές συμφωνίες.

4.5. ***ENISA***

4.5.1. Η ΕΟΚΕ θεωρεί ότι η νέα μόνιμη εντολή του ENISA, όπως προτείνεται από την Επιτροπή, θα συμβάλει σημαντικά στην ενίσχυση της ανθεκτικότητας των ευρωπαϊκών συστημάτων. Ωστόσο, ο συνοδευτικός προσωρινός προϋπολογισμός και οι πόροι που διατίθενται στον μεταρρυθμισμένο ENISA ενδέχεται να μην επαρκούν για την εκπλήρωση της εντολής του.

4.5.2. Η ΕΟΚΕ ενθαρρύνει όλα τα κράτη μέλη να θεσπίσουν έναν σαφή και παρεμφερή οργανισμό, ομόλογο του ENISA, καθώς τα περισσότερα δεν το έχουν πράξει ακόμη. Πρέπει να προωθηθεί διαρθρωμένο πρόγραμμα για την απόσπαση εθνικών εμπειρογνωμόνων στον ENISA ώστε να υποστηριχθεί η ανταλλαγή βέλτιστων πρακτικών και να ενισχυθεί η εμπιστοσύνη. Η ΕΟΚΕ συνιστά επίσης στην Επιτροπή να εξασφαλίσει τη συλλογή και το διαμοιρασμό των υφιστάμενων ορθών πρακτικών και αποτελεσματικών μέτρων των κρατών μελών.

4.5.3. Η ΕΟΚΕ θεωρεί επίσης ότι, όσον αφορά τη δημιουργία ικανοτήτων, ο ENISA θα πρέπει να δώσει προτεραιότητα σε δράσεις υποστήριξης της ηλεκτρονικής διακυβέρνησης ([10]). Η ψηφιακή ταυτότητα σε ευρωπαϊκό/παγκόσμιο επίπεδο για πρόσωπα, οργανισμούς, εταιρείες και αντικείμενα είναι καθοριστικής σημασίας, η δε πρόληψη και καταπολέμηση της κλοπής της ταυτότητας και της ηλεκτρονικής απάτης, καθώς και η καταπολέμηση της κλοπής βιομηχανικής διανοητικής ιδιοκτησίας, θα πρέπει να αποτελούν προτεραιότητα.

4.5.4. Ο ENISA θα πρέπει επίσης να υποβάλλει τακτικές εκθέσεις σχετικά με την ετοιμότητα των κρατών μελών στον κυβερνοχώρο, εστιάζοντας κυρίως στους τομείς που προσδιορίζονται στο παράρτημα ΙΙ της οδηγίας ΑΔΠ. Ετήσια ευρωπαϊκή άσκηση στον κυβερνοχώρο θα πρέπει να αξιολογεί την ετοιμότητα των κρατών μελών και την αποτελεσματικότητα του ευρωπαϊκού μηχανισμού αντιμετώπισης κρίσεων στον κυβερνοχώρο και να υποβάλλει συστάσεις.

4.5.5. Η ΕΟΚΕ εκφράζει την ανησυχία ότι οι πόροι είναι εξαιρετικά περιορισμένοι όσον αφορά την επιχειρησιακή συνεργασία, συμπεριλαμβανομένου του δικτύου των CSIRT.

4.5.6. Όσον αφορά τα καθήκοντα που σχετίζονται με την αγορά, η ΕΟΚΕ θεωρεί ότι η ενίσχυση της συνεργασίας με τα κράτη μέλη και η δημιουργία επίσημου δικτύου φορέων στον τομέα της ασφάλειας στον κυβερνοχώρο θα συμβάλουν στη στήριξη της συνεργασίας μεταξύ των ενδιαφερομένων ([11]). Ο χρόνος που απαιτείται για την είσοδο στην αγορά είναι πολύ μικρός, είναι δε αποφασιστικής σημασίας για τις επιχειρήσεις της ΕΕ να είναι σε θέση να ανταγωνίζονται στον τομέα αυτό, και ο ENISA θα πρέπει να είναι σε θέση να αντιδρά ανταποκρινόμενος ανάλογα. Η ΕΟΚΕ θεωρεί ότι, όπως και άλλοι οργανισμοί της ΕΕ, ο ENISA θα μπορούσε στο μέλλον να εφαρμόσει ένα σύστημα τελών και δικαιωμάτων. Η ΕΟΚΕ εκφράζει την ανησυχία της για το γεγονός ότι ο ανταγωνισμός σε θέματα αρμοδιοτήτων μεταξύ της ΕΕ και των εθνικών οργανισμών θα μπορούσε, όπως και σε άλλους τομείς, να καθυστερήσει την ορθή θέσπιση του ρυθμιστικού πλαισίου της ΕΕ και να ζημιώσει την ενιαία αγορά της ΕΕ.

4.5.7. Η ΕΟΚΕ σημειώνει ότι τα καθήκοντα που σχετίζονται με την Ε&Κ και τη διεθνή συνεργασία είναι επί του παρόντος ελάχιστα.

([10]) Ψηφιακή ενιαία αγορά: ενδιάμεση αξιολόγηση.
([11]) ΕΕ C 75 της 10.03. 2017, σ. 124.

4.5.8. Η ΕΟΚΕ θεωρεί ότι η ασφάλεια στον κυβερνοχώρο πρέπει να αποτελεί σταθερό σημείο συζήτησης κατά τις τακτικές κοινές συνεδριάσεις των υπηρεσιών Δικαιοσύνης και Εσωτερικών Υποθέσεων (ΔΕΥ), ενώ ο ENISA και η Ευρωπόλ πρέπει να συνεργάζονται τακτικά.

4.5.9. Με δεδομένο ότι ο κυβερνοχώρος είναι πολύ καινοτόμος, πρέπει να εξεταστεί προσεκτικά η θέσπιση προτύπων ώστε να αποφευχθεί η παρακώλυση της καινοτομίας, κάτι το οποίο απαιτεί ένα δυναμικό πλαίσιο. Θα πρέπει να διασφαλιστεί κατά το δυνατόν περισσότερο η αμφίδρομη συμβατότητα, προκειμένου να προστατευθούν και οι πολίτες, αλλά και οι επενδύσεις των εταιρειών.

4.5.10. Λόγω της σημασίας των εθνικών εποπτικών αρχών πιστοποίησης, η ΕΟΚΕ προτείνει ο παρών κανονισμός να θεσπίσει ήδη ένα επίσημο δίκτυο αρχών που θα είναι αρμόδιο να επιλύει διασυνοριακά ζητήματα με την υποστήριξη του ENISA. Το δίκτυο θα μπορούσε αργότερα να εξελιχθεί σε ενιαία υπηρεσία.

4.5.11. Η εμπιστοσύνη είναι θεμελιώδους σημασίας, όμως ο ENISA δεν μπορεί να εκδίδει αποφάσεις ούτε να ελέγχει εκθέσεις. Η ΕΟΚΕ θεωρεί ότι ο οργανισμός θα πρέπει να παρακολουθεί τις επιδόσεις και τη λήψη αποφάσεων των εθνικών εποπτικών αρχών πιστοποίησης μέσω ελέγχων και επιθεωρήσεων εξ ονόματος της Επιτροπής.

4.5.12. Η συμμετοχή στο διοικητικό συμβούλιο του ENISA πρέπει να επεκταθεί, με καθεστώς παρατηρητή, στη βιομηχανία και τις ενώσεις καταναλωτών.

4.6. ***Βιομηχανία, ΜΜΕ, χρηματοδότηση/επενδύσεις και καινοτόμα επιχειρηματικά μοντέλα***

4.6.1. *Βιομηχανία και επενδύσεις*

Για να αυξηθεί η παγκόσμια ανταγωνιστικότητα των επιχειρήσεων της ΕΕ που δραστηριοποιούνται στον τομέα των ΤΠΕ, οι δράσεις πρέπει να προσανατολίζονται προς τη βελτίωση της στήριξης της ανάπτυξης και της ανταγωνιστικότητας της βιομηχανίας ΤΠΕ, συμπεριλαμβανομένων των ΜΜΕ.

Η Ευρώπη θα πρέπει να αυξήσει τις επενδύσεις με τη σύγκλιση διαφόρων κονδυλίων της ΕΕ, εθνικών κεφαλαίων και επενδύσεων του ιδιωτικού τομέα προς την κατεύθυνση στρατηγικών στόχων με ισχυρή συνεργασία δημόσιου-ιδιωτικού τομέα. Το επίπεδο των επενδύσεων σε ζωτικούς τομείς θα πρέπει να αυξηθεί και να συνοδευτεί από τη δημιουργία ενός Ταμείου Κυβερνοασφάλειας της ΕΕ για την καινοτομία και την Ε&Α στο τρέχον και το μελλοντικό πρόγραμμα-πλαίσιο για την έρευνα. Επιπλέον, η Ευρώπη θα πρέπει να δημιουργήσει ένα ταμείο για την ανάπτυξη της κυβερνοασφάλειας, προσθέτοντας μια νέα πτυχή στον τρέχοντα και στο μελλοντικό μηχανισμό «Συνδέοντας την Ευρώπη» καθώς και στο επόμενο ΕΤΣΕ 3.0.

Θα πρέπει να δημιουργηθούν κίνητρα για τα κράτη μέλη της ΕΕ ώστε να αγοράζουν ευρωπαϊκές λύσεις όταν είναι δυνατόν και να επιλέγουν ευρωπαίους προμηθευτές, εφόσον υπάρχουν, ιδίως για ευαίσθητες εφαρμογές. Η Ευρώπη πρέπει να στηρίξει την ανάπτυξη ευρωπαίων πρωτοπόρων στον κυβερνοχώρο οι οποίοι θα μπορούν να ανταγωνιστούν σε μια παγκόσμια αγορά.

4.6.2. *ΜΜΕ*

Λόγω του κατακερματισμού της αγοράς, υπάρχει ανάγκη μεγαλύτερης σαφήνειας όσον αφορά τη ζήτηση των πελατών, προκειμένου να αντιμετωπιστεί καλύτερα η αγορά. Χωρίς δομημένη ζήτηση, οι ΜΜΕ και οι νεοσύστατες επιχειρήσεις δεν μπορούν να αναπτυχθούν με ταχείς ρυθμούς. Σε αυτό το πλαίσιο, η θέσπιση ενός ευρωπαϊκού κόμβου ασφάλειας στον κυβερνοχώρο για τις ΜΜΕ θα ήταν θετική.

Η τεχνολογία στον τομέα της ασφάλειας στον κυβερνοχώρο μεταβάλλεται ταχύτατα και οι ΜΜΕ, χάρη στην ευελιξία τους, μπορούν να παράσχουν τις λύσεις αιχμής που απαιτούνται για να παραμείνουν ανταγωνιστικές. Σε σύγκριση με τις τρίτες χώρες, η ΕΕ εξακολουθεί να αναζητά κατάλληλο επιχειρηματικό μοντέλο για τις ΜΜΕ.

Πρέπει να αναπτυχθούν προγράμματα για τις νεοφυείς επιχειρήσεις και τις ΜΜΕ ώστε να στηριχθεί το κόστος της πιστοποίησης και να αντισταθμιστεί η μεγάλη δυσκολία χρηματοδότησης της τεχνολογικής και εμπορικής τους ανάπτυξης.

4.7. ***Ο ανθρώπινος παράγοντας: εκπαίδευση και προστασία***

4.7.1. Η ΕΟΚΕ διαπιστώνει ότι η πρόταση της Επιτροπής δεν λαμβάνει προσηκόντως υπόψη τον άνθρωπο ως κινητήριο υποκείμενο των ψηφιακών διαδικασιών, τόσο ως αποδέκτη αυτών όσο και ως υπαίτιο των σημαντικότερων συμβάντων στον κυβερνοχώρο.

4.7.2. Είναι αναγκαίο να αναπτυχθεί μια ισχυρή βάση δεξιοτήτων στον κυβερνοχώρο και να βελτιωθεί η κυβερνοϋγιεινή και η ευαισθητοποίηση μεταξύ ατόμων και επιχειρήσεων. Για να επιτευχθεί το αποτέλεσμα αυτό, θα πρέπει να εξεταστούν ζητήματα όπως ειδικές επενδύσεις, ο χρόνος κατάρτισης εκπαιδευτών υψηλού επιπέδου και αποτελεσματικές εκστρατείες ευαισθητοποίησης. Η εφαρμογή αυτών των τριών γραμμών δράσης απαιτεί τη συμμετοχή των εθνικών και περιφερειακών αρχών (υπεύθυνων για την υλοποίηση και την επένδυση σε αποτελεσματικά εκπαιδευτικά προγράμματα), αλλά και των επιχειρήσεων και των ΜΜΕ σε μια συλλογική προσέγγιση.

4.7.3. Θα πρέπει να εξεταστεί το ενδεχόμενο δημιουργίας προγράμματος σπουδών πιθανώς πιστοποιημένου από την ΕΕ για τα σχολεία και τους επαγγελματίες, με την ενεργό συμμετοχή του ENISA και των εθνικών ομολόγων του. Επιπλέον, πρέπει να εξετάζεται η ισότητα των φύλων κατά την ανάπτυξη εκπαιδευτικών προγραμμάτων προς βελτίωση των επιπέδων απασχόλησης στον τομέα της ασφάλειας στον κυβερνοχώρο.

4.7.4. Η ΕΟΚΕ θεωρεί ότι η δραστηριότητα πιστοποίησης πρέπει να περιλαμβάνει ένα επαρκές σύστημα επισήμανσης τόσο για το υλισμικό όσο και για το λογισμικό, όπως ισχύει για πολλά άλλα προϊόντα (π.χ. ενεργειακά προϊόντα). Το μέσο αυτό θα παρέχει το τριπλό πλεονέκτημα να μειώνει το κόστος για τις επιχειρήσεις, να καταργεί τον υφιστάμενο κατακερματισμό στην αγορά εξαιτίας των διαφορετικών συστημάτων πιστοποίησης που εφαρμόζονται ήδη σε εθνική κλίμακα και να απλοποιεί την κατανόηση εκ μέρους των καταναλωτών όσον αφορά την ποιότητα και τα χαρακτηριστικά του αντικειμένου που αγοράζουν. Για τον σκοπό αυτό, είναι σημαντικό να υπόκεινται στους ίδιους μηχανισμούς πιστοποίησης και επισήμανσης και τα προϊόντα που εισάγονται από τρίτες χώρες. Τέλος, η ΕΟΚΕ θεωρεί ότι η δημιουργία ενός ειδικού λογοτύπου θα μπορούσε να συμβάλλει ώστε οι καταναλωτές και οι χρήστες να αντιλαμβάνονται άμεσα την αξιοπιστία των προϊόντων που αγοράζουν ή των ιστοσελίδων από τις οποίες πραγματοποιούν συναλλαγές αγοραπωλησίας ή προβλέπουν την υποβολή ευαίσθητων δεδομένων.

4.7.5. Ο ENISA θα μπορούσε να αναλάβει μια σημαντική δραστηριότητα πληροφόρησης και ενημέρωσης έτσι ώστε να ενισχυθούν τόσο η αντίληψη σχετικά με τις «ασφαλείς» ψηφιακές συμπεριφορές όσο και η εμπιστοσύνη των χρηστών στο Διαδίκτυο. Για το σκοπό αυτό, θα πρέπει να υπάρξει συμμετοχή των ενώσεων των επιχειρήσεων, των καταναλωτών και άλλων οργανισμών που δραστηριοποιούνται στις ψηφιακές υπηρεσίες.

4.7.6. Όπως έχει ήδη προταθεί στη γνωμοδότηση INT/828, συμπληρωματικά ως προς την «Πράξη για την ασφάλεια στον κυβερνοχώρο» (Cybersecurity Act), η ΕΟΚΕ θεωρεί απολύτως αναγκαίο να δρομολογηθεί το ταχύτερο δυνατόν ένα ευρύ ευρωπαϊκό πρόγραμμα για την ψηφιακή εκπαίδευση και κατάρτιση, προκειμένου να παρασχεθούν σε όλους τους πολίτες τα απαιτούμενα μέσα για να ανταποκριθούν με τον καλύτερο δυνατό τρόπο στη μετάβαση. Ειδικότερα, μολονότι έχει επίγνωση των ειδικών εθνικών αρμοδιοτήτων στον τομέα, η ΕΟΚΕ ελπίζει ότι το πρόγραμμα αυτό θα ξεκινά από τα σχολεία, ενισχύοντας τις γνώσεις του διδακτικού προσωπικού, προσαρμόζοντας τα προγράμματα σπουδών και τη διδασκαλία στις ψηφιακές τεχνολογίες (συμπεριλαμβανομένης της ηλεκτρονικής μάθησης) και παρέχοντας σε όλους τους μαθητές εκπαίδευση υψηλής ποιότητας. Είναι αυτονόητο ότι το πρόγραμμα αυτό θα περιλαμβάνει τη διά βίου μάθηση, με σκοπό την προσαρμογή ή την επικαιροποίηση των δεξιοτήτων όλων των εργαζομένων ([12]).

5. **Ειδικές παρατηρήσεις**

5.1. ***Αναδυόμενες τεχνολογίες και λύσεις: η περίπτωση του διαδικτύου των πραγμάτων (IoT)***

Ο αριθμός των συνδεδεμένων συσκευών αυξάνεται συνεχώς και αναμένεται να φτάσει σε πολλαπλάσιο αριθμό σε σχέση με τους κατοίκους του πλανήτη, λόγω της ψηφιοποίησης συστατικών στοιχείων, συστημάτων και λύσεων και της ενίσχυσης της συνδεσιμότητας. Η τάση αυτή δημιουργεί νέες ευκαιρίες για τους παραβάτες του κυβερνοχώρου, ειδικά επειδή οι συσκευές του διαδικτύου των πραγμάτων συχνά δεν προστατεύονται τόσο καλά όσο οι παραδοσιακές συσκευές.

Τα ευρωπαϊκά πρότυπα ασφαλείας σε διαφορετικά κατακόρυφα τμήματα που χρησιμοποιούν συσκευές του διαδικτύου των πραγμάτων μπορούν να μειώσουν την αναπτυξιακή προσπάθεια, τον χρόνο και τον προϋπολογισμό για όλους τους ασχολούμενους στη βιομηχανία που συμμετέχουν στην αξιακή αλυσίδα των συνδεδεμένων προϊόντων.

Είναι πιθανόν να απαιτείται κάποια μορφή ελάχιστου επιπέδου ασφαλείας μέσω IDAM (Διαχείριση Ταυτότητας και Πρόσβασης), βελτιώσεων και διαχείρισης συσκευών για τις «συνήθεις» συσκευές του «διαδικτύου των προσώπων» (IoP). Καθώς η πιστοποίηση αποτελεί βασική μέθοδο παροχής υψηλότερου επιπέδου ασφάλειας, θα πρέπει να δοθεί μεγαλύτερη έμφαση στην ασφάλεια του διαδικτύου των πραγμάτων (IoT) κατά τη νέα προσέγγιση πιστοποίησης της ΕΕ.

Βρυξέλλες, 14 Φεβρουαρίου 2018.

Ο Πρόεδρος
της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής
Γιώργος ΝΤΑΣΗΣ

([12]) Ψηφιακή ενιαία αγορά: ενδιάμεση αξιολόγηση.