

Βρυξέλλες, 25.1.2017
COM(2017) 41 final

**ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ
ΕΥΡΩΠΑΪΚΟ ΣΥΜΒΟΥΛΙΟ ΚΑΙ ΤΟ ΣΥΜΒΟΥΛΙΟ**

Τέταρτη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας

Τέταρτη έκθεση προόδου προς μια αποτελεσματική και πραγματική Ένωση Ασφάλειας

I. ΕΙΣΑΓΩΓΗ

Η παρούσα είναι η τέταρτη μηνιαία έκθεση για τη σημειωθείσα πρόοδο προς την οικοδόμηση μιας αποτελεσματικής και πραγματικής Ένωσης Ασφάλειας, και καλύπτει τις εξελίξεις σε δύο βασικούς πυλώνες: *στην καταπολέμηση της τρομοκρατίας και του οργανωμένου εγκλήματος, καθώς και των μέσων που τα στηρίζουν· και στην ενίσχυση της άμυνάς μας και την οικοδόμηση ανθεκτικότητας έναντι αυτών των απειλών*. Η παρούσα έκθεση εστιάζει σε τέσσερις σημαντικούς τομείς: στα συστήματα πληροφοριών και τη διαλειτουργικότητα, την προστασία ευάλωτων στόχων, την απειλή στον κυβερνοχώρο και την προστασία των δεδομένων στο πλαίσιο των ποινικών ερευνών.

Η επίθεση τον Δεκέμβριο στη χριστουγεννιάτικη αγορά του Βερολίνου κατέδειξε εκ νέου σοβαρές αδυναμίες των συστημάτων μας πληροφοριών, οι οποίες πρέπει να αντιμετωπισθούν επείγοντως, ειδικότερα σε επίπεδο ΕΕ, για την παροχή συνδρομής στις επί τόπου εθνικές συνοριακές αρχές και αρχές επιβολής του νόμου ώστε να εκπληρώνουν πιο αποτελεσματικά τα απαιτητικά καθήκοντά τους. Η μη διασύνδεση των διαφορετικών συστημάτων πληροφοριών, γεγονός που επιτρέπει στους δράστες της επίθεσης να χρησιμοποιούν πολλαπλές ταυτότητες προκειμένου να κυκλοφορούν χωρίς να εντοπιστούν, μεταξύ άλλων και κατά τη διέλευση συνόρων, καθώς και η μη συστηματική ανάρτηση των εν λόγω πληροφοριών από τα κράτη μέλη στις σχετικές βάσεις δεδομένων της ΕΕ αποτελούν αδυναμίες στην πρακτική εφαρμογή που πρέπει να αποκατασταθούν επείγοντως. Επιπλέον, πρέπει να συνεχιστούν επίσης οι εργασίες σε ό, τι αφορά τα μέτρα επιβολής του νόμου σχετικά με τα σύνορα και την επιστροφή των αιτούντων άσυλο των οποίων η αίτηση απορρίφθηκε¹.

Όσον αφορά την προστασία ευάλωτων στόχων, η Επιτροπή θα επιταχύνει τις εργασίες της ώστε να φέρει σε επαφή εμπειρογνώμονες από τα κράτη μέλη για την ανταλλαγή βέλτιστων πρακτικών και την επίτευξη συμφωνίας σχετικά με τυποποιημένες κατευθυντήριες γραμμές.

Η απειλή στον κυβερνοχώρο που αντιμετωπίζει η ΕΕ λαμβάνει ευρεία κάλυψη από τα μέσα μαζικής επικοινωνίας και στην παρούσα έκθεση εξετάζονται οι διάφοροι άξονες εργασίας που έχουν ήδη αναπτυχθεί στον τομέα αυτό. Αυτοί οι άξονες καλύπτουν τόσο την πρόληψη — σε συνεργασία με τις επιχειρήσεις του κλάδου για την προώθηση της ασφάλειας βάσει σχεδιασμού και της εφαρμογής της οδηγίας για την ασφάλεια δικτύων και πληροφοριών — όσο και την προαγωγή της συνεργασίας μεταξύ κρατών μελών και με διεθνείς οργανισμούς και εταίρους για την αντιμετώπιση επιθέσεων στον κυβερνοχώρο καθώς αυτές συμβαίνουν. Κατά τους προσεχείς μήνες, η Επιτροπή και η Ύπατη Εκπρόσωπος της Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας θα καθορίσουν τις δράσεις που απαιτούνται για να δοθεί αποτελεσματική απάντηση σε επίπεδο ΕΕ έναντι των απειλών αυτών, με βάση τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο του 2013.

¹ Η Επιτροπή θα υποβάλει αναθεωρημένο σχέδιο δράσης για τις επιστροφές κατά τις προσεχείς εβδομάδες, βλ. Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το Συμβούλιο σχετικά με την έναρξη επιχειρησιακής λειτουργίας της Ευρωπαϊκής Συνοριοφυλακής και Ακτοφυλακής, COM(2017) 42.

Η προστασία της ιδιωτικής ζωής των φυσικών προσώπων και των δεδομένων προσωπικού χαρακτήρα αποτελεί θεμελιώδες δικαίωμα και, ως εκ τούτου, τον ακρογωνιαίο λίθο για οποιαδήποτε δράση προς μια πραγματική Ένωση Ασφάλειας. Η οδηγία για την προστασία των δεδομένων στον τομέα της αστυνομίας και της ποινικής δικαιοσύνης, που εκδόθηκε τον Απρίλιο του 2016, εξασφαλίζει κοινό υψηλό επίπεδο προστασίας των δεδομένων και θα διευκολύνει επομένως την ομαλή ανταλλαγή σχετικών δεδομένων μεταξύ των αρχών επιβολής του νόμου των κρατών μελών. Η Επιτροπή έχει επίσης δρομολογήσει αναθεώρηση της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες στο πλαίσιο της δέσμης μέτρων για τα δεδομένα ώστε να επεκτείνει την κάλυψη της οδηγίας σε όλους τους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών και να ευθυγραμμίσει τις διατάξεις της με τον γενικό κανονισμό για την προστασία δεδομένων. Η πρόταση έχει σχεδιαστεί κατά τρόπο που διασφαλίζει την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ενώ παράλληλα παραθέτει τους λόγους, βάσει των οποίων μπορεί να προβλέπονται περιορισμοί του πεδίου εφαρμογής του κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, μεταξύ άλλων για λόγους εθνικής ασφάλειας ή ποινικές έρευνες.

II. ΕΝΙΣΧΥΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΤΗΣ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ

Η ομιλία του Προέδρου Γιούνκερ για την κατάσταση της Ένωσης τον Σεπτέμβριο του 2016 και τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου του Δεκεμβρίου του 2016 αναφέρονται στη σημασία τού να αντιμετωπιστούν οι τρέχουσες ελλείψεις σε θέματα διαχείρισης πληροφοριών και βελτίωσης της **διαλειτουργικότητας και διασύνδεσης των υφιστάμενων συστημάτων πληροφοριών**. Τα πρόσφατα γεγονότα έχουν και πάλι καταδείξει την επείγουσα ανάγκη να συνδεθούν μεταξύ τους οι υφιστάμενες βάσεις δεδομένων της ΕΕ, αν μη τι άλλο για να δοθούν στις επί τόπου συνοριακές αρχές και αρχές επιβολής του νόμου τα εργαλεία που απαιτούνται για τον εντοπισμό της υποκλοπής ταυτότητας. Για παράδειγμα, ο δράστης της τρομοκρατικής επίθεσης του Δεκεμβρίου 2016 στο Βερολίνο χρησιμοποίησε τουλάχιστον 14 διαφορετικές ταυτότητες και κατάφερε να διέλθει από κράτη μέλη χωρίς να εντοπιστεί. Επομένως, υπάρχει σαφής ανάγκη να προβλέπεται η δυνατότητα ταυτόχρονης αναζήτησης με τη χρήση βιομετρικών αναγνωριστικών στοιχείων στα υφιστάμενα και μελλοντικά συστήματα πληροφοριών της ΕΕ ώστε οι τρομοκράτες και εγκληματίες να μην μπορούν πλέον να μετέρχονται παρόμοιων μέσων.

Στο πλαίσιο αυτό, η Επιτροπή ξεκίνησε εργασίες τον Απρίλιο του 2016 με την υποβολή προτάσεων για «πιο ισχυρά και έξυπνα συστήματα πληροφοριών για τα σύνορα και την ασφάλεια»². Εντοπίστηκαν ελλείψεις στις λειτουργίες των υφιστάμενων συστημάτων, κενά στην αρχιτεκτονική της ΕΕ για τη διαχείριση δεδομένων, προβλήματα με το πολύπλοκο τοπίο συστημάτων πληροφοριών των οποίων η διαχείριση γίνεται με διαφορετικούς τρόπους, καθώς και γενικός κατακερματισμός που οφείλεται στο γεγονός ότι τα υφιστάμενα συστήματα σχεδιάστηκαν για να λειτουργούν χωριστά και όχι από κοινού. Στο πλαίσιο της διαδικασίας αυτής, η Επιτροπή συγκρότησε την **ομάδα εμπειρογνομόνων υψηλού επιπέδου για τα συστήματα πληροφοριών και τη διαλειτουργικότητα** με οργανισμούς της ΕΕ, τα κράτη μέλη και σχετικούς

² Ανακοίνωση της Επιτροπής με θέμα «Πιο Ισχυρά και Έξυπνα Συστήματα Πληροφοριών για τα Σύνορα και την Ασφάλεια» COM(2016) 205 final.

ενδιαφερόμενους φορείς. Στις 21 Δεκεμβρίου 2016³, μια έκθεση του προέδρου της εν λόγω ομάδας παρουσίασε **τα ενδιάμεσα πορίσματα** της τα οποία περιλαμβάνουν την κατά προτεραιότητα επιλογή της δημιουργίας ενιαίας δικτυακής πύλης αναζήτησης που θα επιτρέπει στις εθνικές αρχές επιβολής του νόμου και τις συνοριακές αρχές την ταυτόχρονη αναζήτηση στις υφιστάμενες βάσεις δεδομένων και τα συστήματα πληροφοριών της ΕΕ. Η ενδιάμεση έκθεση υπογραμμίζει επίσης τη σημασία της ποιότητας των δεδομένων – δεδομένου ότι η αποτελεσματικότητα των συστημάτων πληροφοριών εξαρτάται από την ποιότητα και τη μορφή των δεδομένων που καταχωρίζονται σε αυτά – και διατυπώνει συστάσεις για τη βελτίωση της ποιότητας των δεδομένων στα συστήματα της ΕΕ μέσω αυτοματοποιημένου ελέγχου της ποιότητας των δεδομένων.

Η Επιτροπή θα δώσει γρήγορα συνέχεια στην επιλογή να δημιουργηθεί ενιαία πύλη αναζήτησης και, από κοινού με τον Οργανισμό της ΕΕ για τη λειτουργική διαχείριση συστημάτων ΤΠ μεγάλης κλίμακας, τον eu-LISA, θα αρχίσει τις εργασίες της όσον αφορά μια δικτυακή πύλη που θα επιτρέπει την παράλληλη αναζήτηση σε όλα τα συναφή υφιστάμενα συστήματα της ΕΕ. Η σχετική μελέτη θα πρέπει να είναι έτοιμη έως τον Ιούνιο και θα αποτελέσει τη βάση για το σχεδιασμό και τη δοκιμή πρωτότυπης πύλης πριν από το τέλος του έτους. Η Επιτροπή θεωρεί ότι η Ευρωπόλ θα πρέπει να συνεχίσει παράλληλα τις εργασίες της για ένα σύστημα διεπαφής που θα παρέχει τη δυνατότητα στους υπαλλήλους πρώτης γραμμής των κρατών μελών όταν αναζητούν πληροφορίες στα εθνικά τους συστήματα να αναζητούν αυτόματα πληροφορίες ταυτόχρονα στις βάσεις δεδομένων της Ευρωπόλ.

Οι εργασίες για την επίτευξη της διαλειτουργικότητας των συστημάτων πληροφοριών αποσκοπεί στην υπέρβαση του παρόντος κατακερματισμού στην αρχιτεκτονική της ΕΕ όσον αφορά τη διαχείριση των δεδομένων για τον έλεγχο των συνόρων και την ασφάλεια, καθώς και για τις συναφείς αδυναμίες. Όταν οι βάσεις δεδομένων χρησιμοποιούν κοινό αποθετήριο δεδομένων ταυτότητας — όπως προβλέπεται για το προτεινόμενο σύστημα εισόδου/εξόδου στην ΕΕ καθώς και το προτεινόμενο ευρωπαϊκό σύστημα πληροφοριών και άδειας ταξιδιού (ETIAS) — ένα πρόσωπο μπορεί να καταχωριστεί στις διάφορες βάσεις δεδομένων με μία μόνο ταυτότητα, γεγονός το οποίο εμποδίζει τη χρήση διαφόρων πλαστών ταυτοτήτων. Ως πρώτο βήμα, όπως προτείνεται στα ενδιάμεσα πορίσματα της ομάδας εμπειρογνομόνων υψηλού επιπέδου, η Επιτροπή ζήτησε από τον οργανισμό eu-LISA να αναλύσει τις τεχνικές και επιχειρησιακές πτυχές της εφαρμογής κοινής υπηρεσίας βιομετρικής αντιστοίχισης. Η εν λόγω υπηρεσία θα παρέχει τη δυνατότητα αναζήτησης σε διάφορες βάσεις δεδομένων με βιομετρικά δεδομένα, γεγονός που θα μπορούσε να αποκαλύψει τις πλαστές ταυτότητες που χρησιμοποιεί το εν λόγω πρόσωπο σε άλλο σύστημα. Πέραν αυτού, η ομάδα εμπειρογνομόνων υψηλού επιπέδου θα πρέπει τώρα να αξιολογήσει κατά πόσον είναι αναγκαία, τεχνικώς εφικτή και αναλογική η επέκταση του **κοινού αποθετηρίου δεδομένων ταυτότητας** που προβλέπεται για το σύστημα εισόδου/εξόδου και το ETIAS σε άλλα συστήματα. Εκτός από τα βιομετρικά δεδομένα που αποθηκεύονται στα υπηρεσία βιομετρικής αντιστοίχισης, ένα κοινό αποθετήριο δεδομένων ταυτότητας θα περιλάμβανε επίσης αλφαριθμητικά δεδομένα ταυτότητας. Η ομάδα θα πρέπει να υποβάλει τα πορίσματά της σχετικά με αυτό το θέμα στην τελική της έκθεση μέχρι τα τέλη Απριλίου 2017.

³ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1>

Τα πρόσφατα γεγονότα στον τομέα της ασφάλειας καταδεικνύουν την ανάγκη να επανεξεταστεί το θέμα της **υποχρεωτικής ανταλλαγής πληροφοριών** μεταξύ των κρατών μελών. Η πρόταση της Επιτροπής του Δεκεμβρίου 2016 για την ενίσχυση του **συστήματος πληροφοριών Σένγκεν** προβλέπει — για πρώτη φορά — υποχρέωση των κρατών μελών να εισάγουν καταχωρίσεις για πρόσωπα που σχετίζονται με τρομοκρατικά εγκλήματα. Είναι σημαντικό το γεγονός ότι οι συννομοθέτες εργάζονται τώρα για την ταχεία έγκριση των προτεινόμενων μέτρων. Η Επιτροπή είναι έτοιμη να εξετάσει εάν θα πρέπει να καθιερωθεί υποχρέωση ανταλλαγής πληροφοριών για άλλες βάσεις δεδομένων της ΕΕ.

III. ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΥΑΛΩΤΩΝ ΣΤΟΧΩΝ ΑΠΟ ΤΡΟΜΟΚΡΑΤΙΚΕΣ ΕΠΙΘΕΣΕΙΣ

Η επίθεση στο Βερολίνο ήταν η πλέον πρόσφατη επίθεση στην ΕΕ που στρεφόταν κατά των καλούμενων ευάλωτων στόχων, όπως είναι κατά κανόνα οι μη στρατιωτικές εγκαταστάσεις όπου συγκεντρώνεται μεγάλος αριθμός ατόμων (π.χ. δημόσιοι χώροι, νοσοκομεία, σχολεία, αθλητικοί χώροι, πολιτιστικά κέντρα, καφενεία και εστιατόρια, εμπορικά κέντρα και κόμβοι μεταφορών). Από τη φύση τους, τα εν λόγω σημεία είναι ευάλωτα και δύσκολα να προστατευθούν ενώ χαρακτηρίζονται επίσης από την μεγάλη πιθανότητα να υπάρξει σε περίπτωση επίθεσης μεγάλος αριθμός θυμάτων. Για όλους αυτούς τους λόγους προτιμούνται από τρομοκράτες. Η απειλή μελλοντικών επιθέσεων κατά ευάλωτων στόχων, συμπεριλαμβανομένων των μεταφορών, παραμένει υψηλή, όπως επιβεβαιώνεται από υπάρχουσες αξιολογήσεις, μεταξύ άλλων την έκθεση της Ευρωπόλ σχετικά με τις αλλαγές στον τρόπο λειτουργίας του Daesh⁴.

Το ευρωπαϊκό θεματολόγιο για την ασφάλεια του 2015 και η ανακοίνωση του 2016 σχετικά με την Ένωση Ασφάλειας τόνισαν την ανάγκη ενίσχυσης των προσπαθειών για τη βελτίωση της ασφάλειας και της χρήσης καινοτόμων εργαλείων και τεχνολογίας ανίχνευσης για την προστασία ευάλωτων στόχων. Η Επιτροπή καταβάλλει προσπάθειες για την υποστήριξη και την ενθάρρυνση της ανταλλαγής βέλτιστων πρακτικών μεταξύ των κρατών μελών, με σκοπό την ανάπτυξη βελτιωμένων εργαλείων για την πρόληψη των επιθέσεων κατά ευάλωτων στόχων και την αντιμετώπισή τους. Οι προσπάθειες αυτές οδήγησαν σε επιχειρησιακά εγχειρίδια και έγγραφα καθοδήγησης. Επί του παρόντος, η Επιτροπή αναπτύσσει, σε στενή συνεργασία με εμπειρογνώμονες των κρατών μελών, ένα περιεκτικό εγχειρίδιο σχετικά με τις διαδικασίες ασφαλείας και τα υποδείγματα που πρέπει να ισχύουν για διάφορους ευάλωτους στόχους (π.χ. εμπορικά κέντρα, νοσοκομεία, αθλητικές και πολιτιστικές εκδηλώσεις). Ο στόχος είναι η έκδοση εγγράφων καθοδήγησης για την προστασία ευάλωτων στόχων στα κράτη μέλη, στις αρχές του 2017, με βάση τις βέλτιστες πρακτικές που εφαρμόζονται στα κράτη μέλη.

Παράλληλα, η Επιτροπή θα οργανώσει τον Φεβρουάριο το πρώτο εργαστήριο με τις εθνικές αρχές σχετικά με την προστασία ευάλωτων στόχων, με σκοπό την ανταλλαγή πληροφοριών και την ανάπτυξη βέλτιστων πρακτικών σε ό, τι αφορά το πολύπλοκο θέμα της προστασίας ευάλωτων στόχων και τη δημόσια ασφάλεια και προστασία. Η Επιτροπή

⁴ Ευρωπόλ, *Changes in modus operandi of Islamic State (IS) revisited*, (Αλλαγές στον τρόπο λειτουργίας του ισλαμικού κράτους αναθεωρημένη έκθεση), Νοέμβριος 2016 – δημοσίευση της Ευρωπόλ που βρίσκεται στην ακόλουθη διεύθυνση: <https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited>

χρηματοδοτεί επίσης δοκιμαστικό σχέδιο από το Βέλγιο, τις Κάτω Χώρες και το Λουξεμβούργο, στο πλαίσιο του Ταμείου Εσωτερικής Ασφάλειας, για την δημιουργία ενός περιφερειακού κέντρου αριστείας για τις ειδικές παρεμβάσεις στον τομέα της επιβολής του νόμου, το οποίο θα παρέχει κατάρτιση για τους αστυνομικούς που είναι συχνά οι πρώτοι παρεμβαίνοντες σε περίπτωση επίθεσης.

Η αντιμετώπιση επιθέσεων κατά ευάλωτων στόχων αποτελεί βασικό στοιχείο των εργασιών της Επιτροπής για την πολιτική προστασία. Τον Δεκέμβριο, η Επιτροπή ανακοίνωσε τις δράσεις που προτίθεται να ακολουθήσει με τα κράτη μέλη για την προστασία των πολιτών της ΕΕ και για τη μείωση των τρωτών σημείων αμέσως μετά τις τρομοκρατικές επιθέσεις. Οι δράσεις αυτές θα ενισχύσουν τον συντονισμό μεταξύ όλων των παραγόντων που εμπλέκονται στη διαχείριση των συνεπειών των επιθέσεων και η Επιτροπή δεσμεύθηκε να στηρίζει τις προσπάθειες των κρατών μελών διευκολύνοντας κοινές δράσεις κατάρτισης και ασκήσεις, καθώς και εξασφαλίζοντας συνεχή διάλογο μέσω των υφιστάμενων σημείων επαφής και ομάδων εμπειρογνομόνων. Η Επιτροπή θα στηρίζει, επίσης, την ανάπτυξη εξειδικευμένων ενοτήτων για την αντιμετώπιση τρομοκρατικών επιθέσεων στο πλαίσιο του μηχανισμού πολιτικής προστασίας της Ένωσης, και πρωτοβουλιών για την ανταλλαγή των αντληθέντων διδαγμάτων και την ενίσχυση της ευαισθητοποίησης του κοινού.

Από κοινού με τα κράτη μέλη, η Επιτροπή θα εξετάσει επίσης το είδος της στήριξης της ΕΕ που θα μπορούσε να κινητοποιηθεί για να συμβάλει στην οικοδόμηση της ανθεκτικότητας και στην ενίσχυση της ασφάλειας γύρω από δυνητικούς ευάλωτους στόχους. Τα κράτη μέλη θα μπορούσαν επίσης να υποβάλουν αίτηση για χρηματοδότηση από την Ευρωπαϊκή Τράπεζα Επενδύσεων (ΕΤΕπ), (συμπεριλαμβανομένου του Ευρωπαϊκού Ταμείου Στρατηγικών Επενδύσεων), σύμφωνα με τις πολιτικές της ΕΕ και του ομίλου της ΕΤΕπ. Κάθε σχέδιο θα υπόκειται στις συνήθεις διαδικασίες λήψης αποφάσεων, όπως προβλέπεται στη νομοθεσία.

Όσον αφορά τους συγκεκριμένους ευάλωτους στόχους σε σχέση με τους δημόσιους χώρους μεταφορών, όπως τα δημόσια τμήματα των αερολιμένων ή σιδηροδρομικών σταθμών, στο ειδικό εργαστήριο της Επιτροπής του Νοεμβρίου 2016 στο οποίο συγκεντρώθηκε ευρύ φάσμα ενδιαφερομένων, τονίστηκε η ανάγκη να διατηρηθεί η ισορροπία ανάμεσα στις ανάγκες ασφάλειας, την εξυπηρέτηση του επιβάτη και τις δραστηριότητες μεταφοράς. Τα συμπεράσματα υπογραμμίζουν τη σημασία της οικοδόμησης μιας νοοτροπίας για την ασφάλεια, η οποία θα περιλαμβάνει όχι μόνο το προσωπικό αλλά και τους επιβάτες, τη σημασία των τοπικών αξιολογήσεων κινδύνου ως βάση για τον καθορισμό κατάλληλων αντιμέτρων, καθώς και την ανάγκη να ενισχυθεί η επικοινωνία μεταξύ όλων των εμπλεκόμενων μερών.

IV. ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΠΡΟΚΛΗΣΕΩΝ ΤΩΝ ΑΠΕΙΛΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Το έγκλημα στον κυβερνοχώρο και οι επιθέσεις στον κυβερνοχώρο αποτελούν τις βασικές προκλήσεις που αντιμετωπίζει η Ένωση, και η ανάληψη δράσης σε επίπεδο ΕΕ θα βοηθήσει στην ενίσχυση της συλλογικής μας ανθεκτικότητας. Κάθε ημέρα, τα συμβάντα ασφάλειας στον κυβερνοχώρο βλάπτουν σοβαρά τις ζωές των ανθρώπων και προκαλούν σημαντικές οικονομικές ζημιές στην ευρωπαϊκή οικονομία και τις επιχειρήσεις. Οι επιθέσεις στον κυβερνοχώρο αποτελούν βασική συνιστώσα των υβριδικών απειλών — εάν συνδυαστούν χρονικά με απειλές σωματικής βίας, για παράδειγμα στον τομέα της τρομοκρατίας, μπορούν να έχουν καταστροφικές συνέπειες.

Μπορούν επίσης να συμβάλουν στην αποσταθεροποίηση μιας χώρας ή την αμφισβήτηση των πολιτικών θεσμών της και των θεμελιωδών δημοκρατικών διαδικασιών. Όπως θα βασιζόμαστε όλο και περισσότερο στις ηλεκτρονικές τεχνολογίες, οι υποδομές ζωτικής σημασίας (από νοσοκομεία έως πυρηνικούς σταθμούς παραγωγής ηλεκτρικής ενέργειας) θα καθίστανται ολοένα και πιο ευάλωτα.

Η στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο του 2013 αποτελεί μέρος της βασικής πολιτικής αντιμετώπισης των προκλήσεων για την ασφάλεια στον κυβερνοχώρο. Η κεντρική δράση είναι η οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών (ΑΔΠ)⁵, που εκδόθηκε τον περασμένο Ιούλιο. Με αυτή τίθενται οι βάσεις για τη βελτίωση της συνεργασίας σε επίπεδο ΕΕ και της ανθεκτικότητας στον κυβερνοχώρο με την υποστήριξη της συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κρατών μελών και την προώθηση της επιχειρησιακής συνεργασίας σε συγκεκριμένα συμβάντα ασφάλειας στον κυβερνοχώρο και την ανταλλαγή πληροφοριών σχετικά με τους κινδύνους. Για να διασφαλιστεί η συνεπής εφαρμογή σε διάφορους τομείς και πέρα από σύνορα, η Επιτροπή θα πραγματοποιήσει την πρώτη συνεδρίαση της ομάδας συνεργασίας για την ασφάλεια δικτύων και πληροφοριών με τα κράτη μέλη τον Φεβρουάριο.

Τον Απρίλιο του 2016, η Επιτροπή και η Ύπατη Εκπρόσωπος της ΕΕ θέσπισαν ένα κοινό πλαίσιο για την αντιμετώπιση των υβριδικών απειλών⁶ στο οποίο προτείνονται 22 επιχειρησιακές δράσεις που αποσκοπούν στην αύξηση της ευαισθητοποίησης, την οικοδόμηση της ανθεκτικότητας, την καλύτερη ανταπόκριση στις κρίσεις, καθώς και την ενίσχυση της συνεργασίας μεταξύ της ΕΕ και του ΝΑΤΟ. Όπως ζητήθηκε από το Συμβούλιο, η Επιτροπή και η Ύπατη Εκπρόσωπος της ΕΕ θα υποβάλουν έκθεση το αργότερο έως τον Ιούλιο του 2017, προκειμένου να αξιολογήσουν την επιτευχθείσα πρόοδο.

Η Επιτροπή προωθεί και ενισχύει επίσης την τεχνολογική καινοτομία, μεταξύ άλλων μέσω της αξιοποίησης των κονδυλίων της ΕΕ για την έρευνα για την προώθηση νέων λύσεων και τη δημιουργία νέων τεχνολογιών που μπορούν να συμβάλουν στην ενίσχυση της ανθεκτικότητάς μας έναντι επιθέσεων στον κυβερνοχώρο (π.χ. έργα «ασφάλειας βάσει σχεδιασμού»). Το περασμένο καλοκαίρι, εγκαινιάσαμε σύμπραξη δημόσιου-ιδιωτικού τομέα σχετικά με την ασφάλεια στον κυβερνοχώρο με τις επιχειρήσεις του κλάδου, ύψους 1,8 δισ. EUR⁷.

Στον τομέα των μεταφορών, η ψηφιοποίηση μπορεί να αποτελέσει σημαντικό καταλύτη για την επίτευξη της απαραίτητης μετατροπής του σύγχρονου συστήματος μεταφορών. Ο ταχύς ρυθμός της ψηφιοποίησης έχει πολλά πλεονεκτήματα, αλλά καθιστά επίσης τις μεταφορές περισσότερο ευάλωτες στους κινδύνους για την ασφάλεια ή την προστασία στον κυβερνοχώρο. Πολλές δράσεις έχουν αναληφθεί για τον μετριασμό της απειλής σε διάφορα επίπεδα, ειδικά για την αεροπορία, αλλά και για τις θαλάσσιες, ποτάμιες, σιδηροδρομικές και οδικές μεταφορές⁸. Η πρόκληση που απομένει αφορά την περαιτέρω

⁵ Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

⁶ JOIN (2016)18.

⁷ Αναγγέλθηκε στην ανακοίνωση του 2016 για την κυβερνοανθεκτικότητα, COM(2016) 410 final.

⁸ Παραδείγματα είναι οι διεθνείς κατευθυντήριες γραμμές, όπως αυτές που εκπονήθηκαν από το Διεθνές Ναυτιλιακό Οργανισμό ή με μια πρόσφατα εγκριθείσα απόφαση του ΔΟΠΑ, κατόπιν κοινής

αποσαφήνιση, εναρμόνιση και συμπλήρωση των δραστηριοτήτων των διαφόρων εμπλεκόμενων φορέων για την ενίσχυση διαφόρων πτυχών της ανθεκτικότητας στον κυβερνοχώρο.

Σε ευρύτερη κλίμακα, και με δεδομένη την ταχέως εξελισσόμενη φύση των απειλών, κατά τους προσεχείς μήνες, η Επιτροπή και η Ύπατη Εκπρόσωπος της ΕΕ θα καθορίσουν τις δράσεις που απαιτούνται για να δοθεί αποτελεσματική απάντηση σε επίπεδο ΕΕ έναντι των απειλών αυτών, με βάση τη στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο του 2013.

V. ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΜΕ ΤΑΥΤΟΧΡΟΝΗ ΣΤΗΡΙΞΗ ΑΠΟΤΕΛΕΣΜΑΤΙΚΩΝ ΠΟΙΝΙΚΩΝ ΕΡΕΥΝΩΝ

Η οδηγία για την προστασία των δεδομένων στον τομέα της αστυνομίας και της ποινικής δικαιοσύνης⁹, αποτελεί συστατικό στοιχείο της καταπολέμησης της τρομοκρατίας και του σοβαρού εγκλήματος. Με βάση το κοινό πρότυπο προστασίας των δεδομένων που θεσπίζεται στην οδηγία, οι αρχές επιβολής του νόμου των κρατών μελών θα μπορούν να ανταλλάσσουν ομαλά τα σχετικά δεδομένα ενώ ταυτόχρονα τα δεδομένα των θυμάτων, των μαρτύρων καθώς και των υπόπτων για αξιόποινες πράξεις θα προστατεύονται δεόντως.

Επιπλέον, για να εξασφαλιστεί υψηλό επίπεδο προστασίας του απορρήτου των επικοινωνιών, τόσο για τα φυσικά πρόσωπα όσο και για τις επιχειρήσεις και ίσοι όροι ανταγωνισμού για όλους τους παράγοντες της αγοράς, όπως ορίζεται στη στρατηγική για την ψηφιακή ενιαία αγορά του Απριλίου 2015, η Επιτροπή ενέκρινε την πρόταση **κανονισμού για την προστασία της ιδιωτικής ζωής** (που αντικαθιστά την οδηγία 2002/58/ΕΚ) στις 11 Ιανουαρίου¹⁰. Όπως και στην ισχύουσα οδηγία, ο αναθεωρημένος κανονισμός για την προστασία της ιδιωτικής ζωής, συγκεκριμενοποιεί τον γενικό κανονισμό για την προστασία δεδομένων¹¹ και θεσπίζει ένα πλαίσιο σχετικά με την

πρωτοβουλίας της ΕΕ και των ΗΠΑ· η αναφορά συμβάντων στο πλαίσιο της οποίας αναπτύσσεται επί του παρόντος από τον Ευρωπαϊκό Οργανισμό Ασφάλειας της Αεροπορίας μια μέθοδος ταχύτερης αντίδρασης, και η ασφάλεια στον κυβερνοχώρο μέσω σχεδιασμού, που ισχύει για τα υπό εκπόνηση νέα συστήματα, όπως το γενικό πρόγραμμα διαχείρισης της εναέριας κυκλοφορίας από την κοινή επιχείρηση SESAR.

⁹ Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Η οδηγία, που άρχισε να ισχύει από την 5η Μαΐου 2016, πρέπει να μεταφερθεί από τα κράτη μέλη έως τις 6 Μαΐου 2018. Η Επιτροπή έχει συστήσει ομάδα εμπειρογνομόνων με τα κράτη μέλη, για την ανταλλαγή απόψεων σχετικά με τη μεταφορά της οδηγίας για την αστυνομία.

¹⁰ Κανονισμός για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, COM(2017) 10.

¹¹ Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) που θα αρχίσει να εφαρμόζεται στις 25 Μαΐου 2018.

προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

Με την εν λόγω αναθεώρηση, όλα τα δεδομένα των ηλεκτρονικών επικοινωνιών, ακόμη και όταν η επικοινωνία είναι παρεπόμενη, θεωρούνται απόρρητα/περιορισμένης πρόσβασης — είτε αυτή γίνεται μέσω των παραδοσιακών υπηρεσιών τηλεπικοινωνιών είτε μέσω των καλούμενων επιφυών (over the top - OTT) υπηρεσιών που είναι ισοδύναμες από λειτουργική άποψη (π.χ. Skype, Whatsapp), και συχνά, για πολλούς χρήστες μπορούν να υποκαταστήσουν τους συνήθεις παρόχους τηλεπικοινωνιών¹². Οι υποχρεώσεις που επιβάλλονται στους παρόχους υπηρεσιών — εκτός από το σεβασμό των επιλογών σχετικά με την ιδιωτική ζωή των πελατών τους όσον αφορά τη χρήση, την αποθήκευση και την επεξεργασία των δεδομένων τους — περιλαμβάνουν επίσης την υποχρέωση των παρόχων υπηρεσιών που είναι εγκατεστημένοι εκτός της ΕΕ να ορίσουν αντιπρόσωπο σε κράτος μέλος. Αυτή η υποχρέωση θα δώσει στα κράτη μέλη τη δυνατότητα να διευκολύνουν τη συνεργασία των αρχών επιβολής του νόμου και των δικαστικών αρχών με τους παρόχους υπηρεσιών για να έχουν πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία (βλ. κατωτέρω).

Βάσει των ισχυόντων κανόνων για την προστασία της ιδιωτικής ζωής, η πρόσβαση των αρχών επιβολής του νόμου και των δικαστικών αρχών σε συναφείς ηλεκτρονικές πληροφορίες που είναι αναγκαίες για τη διερεύνηση του εγκλήματος θα διέπεται από την εξαίρεση που προβλέπεται στο άρθρο 11 του προτεινόμενου κανονισμού για την προστασία της ιδιωτικής ζωής¹³. Η διάταξη αυτή παρέχει τη δυνατότητα στην ενωσιακή ή εθνική νομοθεσία, να περιορίζει το απόρρητο της επικοινωνίας, όπου είναι αναγκαίο και αναλογικό, για τη διαφύλαξη της εθνικής ασφάλειας, της άμυνας, της δημόσιας ασφάλειας και της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων. Η διάταξη αυτή έχει ιδιαίτερη σημασία για τους εθνικούς κανόνες σχετικά με τη **διατήρηση των δεδομένων**, δηλαδή για να υποχρεώνει τους παρόχους υπηρεσιών τηλεπικοινωνιών να διατηρούν τα δεδομένα των επικοινωνιών για συγκεκριμένο χρονικό διάστημα για την ενδεχόμενη πρόσβαση για σκοπούς επιβολής του νόμου, μετά την ακύρωση το 2014 της οδηγίας για τη διατήρηση δεδομένων από το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ)¹⁴. Έκτοτε, δεν θεσπίστηκε πράξη της ΕΕ για τη διατήρηση των δεδομένων, και ορισμένα κράτη μέλη θέσπισαν τους δικούς τους εθνικούς νόμους για τη διατήρηση δεδομένων. Ασκήθηκαν προσφυγές κατά των νόμων για τη διατήρηση δεδομένων της Σουηδίας και του Ηνωμένου Βασιλείου ενώπιον του ΔΕΕ που εξέδωσε την απόφασή του στην υπόθεση *Tele2* στις 21 Δεκεμβρίου¹⁵. Το ΔΕΕ έκρινε ως ασύμβατη με το δίκαιο της Ένωσης εθνική ρύθμιση η οποία, για τον σκοπό καταπολέμησης του εγκλήματος,

¹² Αυτό ακολουθεί την προσέγγιση που υιοθετήθηκε στην προτεινόμενη οδηγία για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών, η οποία υποβλήθηκε από την Επιτροπή στις 14 Σεπτεμβρίου 2016 (δέσημη μέτρων για τις τηλεπικοινωνίες), COM(2016) 590 final.

¹³ Βλ. άρθρο 11 παράγραφος 1, «ρήτρα για τη διατήρηση των δεδομένων», η οποία παραμένει αμετάβλητη σε σχέση με το άρθρο 15 της οδηγίας για την προστασία της ιδιωτικής ζωής και ευθυγραμμίζεται με τις απαιτήσεις του γενικού κανονισμού για την προστασία δεδομένων. Οι εν λόγω περιορισμοί πρέπει να σέβονται την ουσία των θεμελιωδών δικαιωμάτων και να είναι απαραίτητοι, κατάλληλοι και αναλογικοί.

¹⁴ Απόφαση του ΔΕΕ στις συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12 *Digital Rights Ireland* της 8ης Απριλίου 2014.

¹⁵ Απόφαση του ΔΕΕ στις συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15 *Tele2* της 21ης Δεκεμβρίου 2016.

προβλέπει γενική και χωρίς διάκριση διατήρηση του συνόλου των δεδομένων κίνησης και των δεδομένων θέσεως όλων των συνδρομητών και των χρηστών αφορώσα όλα τα μέσα ηλεκτρονικής επικοινωνίας. Οι συνέπειες της απόφασης τελούν υπό εξέταση και η Επιτροπή θα επεξεργασθεί κατευθυντήριες γραμμές σχετικά με τον τρόπο με τον οποίο μπορούν να συντάσσονται εθνικοί νόμοι για τη διατήρηση δεδομένων που να συνάδουν με την απόφαση.

Το έγκλημα αφήνει ψηφιακά ίχνη που μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε δικαστικές διαδικασίες· οι ηλεκτρονικές επικοινωνίες μεταξύ των υπόπτων συχνά αποτελούν το μοναδικό στοιχείο που μπορούν να συγκεντρώσουν οι αρχές επιβολής του νόμου και οι εισαγγελικές αρχές. Ωστόσο, η πρόσβαση σε **ηλεκτρονικά αποδεικτικά στοιχεία**, – ιδίως αν είναι αποθηκευμένα στο εξωτερικό ή σε υπολογιστικό νέφος — μπορεί να είναι πολύπλοκη τόσο από τεχνική όσο και από νομική σκοπιά και συχνά επαχθής από διαδικαστική σκοπιά, γεγονός που εμποδίζει την ανάγκη των ανακριτών να κινηθούν γρήγορα. Για την αντιμετώπιση αυτών των προκλήσεων, η Επιτροπή αξιολογεί επί του παρόντος λύσεις που να επιτρέπουν στους ανακριτές τη συγκέντρωση διασυνοριακών ηλεκτρονικών αποδεικτικών στοιχείων, μεταξύ άλλων, με την επίτευξη μεγαλύτερης αποτελεσματικότητας όσον αφορά τη διασυνοριακή αμοιβαία νομική βοήθεια, με την εξεύρεση τρόπων για άμεση συνεργασία με τους παρόχους υπηρεσιών διαδικτύου, και την πρόταση κριτηρίων για τον προσδιορισμό και την επιβολή της δικαιοδοσίας στον κυβερνοχώρο, σε πλήρη συμμόρφωση με τους ισχύοντες κανόνες περί προστασίας των δεδομένων¹⁶. Η Επιτροπή υπέβαλε έκθεση στο Συμβούλιο Δικαιοσύνης και Εσωτερικών Υποθέσεων της 9ης Δεκεμβρίου 2016 σχετικά με την επιτευχθείσα πρόοδο¹⁷.

Μια περιεκτική (και ακόμη εν εξελίξει) διαδικασία διαβούλευσης με τους εμπειρογνώμονες επέτρεψε στην Επιτροπή να καταγράψει τα διάφορα και συχνά πολύπλοκα προβλήματα που δημιουργούνται από την πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία, να κατανοήσει καλύτερα τους ισχύοντες κανόνες και πρακτικές στα κράτη μέλη, καθώς και να εντοπίσει πιθανές επιλογές πολιτικής. Η έκθεση προόδου παρέχει επισκόπηση των ιδεών που έχουν προκύψει μέχρι σήμερα κατά τη διάρκεια της συγκέντρωσης πληροφοριών και της διαδικασίας της διαβούλευσης με τους εμπειρογνώμονες· η Επιτροπή, κατόπιν διαβουλεύσεων με τους ενδιαφερόμενους φορείς, θα την εξετάσει περαιτέρω κατά τους προσεχείς μήνες. Όπως ανακοινώθηκε στο πρόγραμμα εργασίας της Επιτροπής, η Επιτροπή θα παρουσιάσει μια πρωτοβουλία το 2017.

VI. ΣΥΜΠΕΡΑΣΜΑ

Η επόμενη έκθεση που αναμένεται την 1η Μαρτίου θα αποτελέσει ευκαιρία για την επανεξέταση της προόδου σχετικά με την εφαρμογή αυτών και άλλων βασικών πτυχών των εργασιών.

¹⁶ Όπως αποφασίστηκε στο Ευρωπαϊκό θεματολόγιο για την ασφάλεια, COM(2015) 185 final, και στην ανακοίνωση της Επιτροπής σχετικά με την υλοποίηση του Ευρωπαϊκού Θεματολογίου για την Ασφάλεια για την καταπολέμηση της τρομοκρατίας και την οικοδόμηση μιας αποτελεσματικής και πραγματικής Ένωσης Ασφάλειας, COM(2016) 230 final.

¹⁷ Στα συμπεράσματά του σχετικά με τη βελτίωση της ποινικής δικαιοσύνης στον κυβερνοχώρο, της 9ης Ιουνίου 2016, το Συμβούλιο κάλεσε την Επιτροπή να λάβει συγκεκριμένα μέτρα, να αναπτύξει κοινή ενωσιακή προσέγγιση και να υποβάλει παραδοτέα έως τα τέλη Ιουνίου 2017.