ΣΥΣΤΑΣΕΙΣ

ΣΥΣΤΑΣΗ (ΕΕ) 2019/534 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 26ης Μαρτίου 2019

Κυβερνοασφάλεια δικτύων 5G

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 292,

Εκτιμώντας τα ακόλουθα:

(1) Η Επιτροπή έχει αναγνωρίσει ότι η εγκατάσταση των τεχνολογιών δικτύου 5ης γενιάς (5G) αποτελεί σημαντικό παράγοντα διευκόλυνσης των μελλοντικών ψηφιακών υπηρεσιών και προτεραιότητα της στρατηγικής για την ψηφιακή ενιαία αγορά. Η Επιτροπή ενέκρινε το σχέδιο δράσης 5G, για να διασφαλίσει ότι η Ένωση θα διαθέτει τις απαραίτητες υποδομές συνδεσιμότητας για τον ψηφιακό μετασχηματισμό της από το 2020 και μετά ([1]).

(2) Τα δίκτυα 5G θα βασιστούν στην τρέχουσα 4η γενιά (4G) τεχνολογιών δικτύου, αλλά θα παρέχουν νέες δυνατότητες υπηρεσιών και θα καταστούν κεντρική υποδομή και παράγοντας διευκόλυνσης για μεγάλα τμήματα της οικονομίας της Ένωσης. Μετά την εισαγωγή τους, τα δίκτυα 5G θα αποτελέσουν τον κορμό ενός ευρέος φάσματος υπηρεσιών, απαραίτητων για τη λειτουργία της εσωτερικής αγοράς και για τη διατήρηση και την εκτέλεση ζωτικών κοινωνικών και οικονομικών λειτουργιών — όπως η ενέργεια, οι μεταφορές, ο τραπεζικός τομέας, η υγεία και τα βιομηχανικά συστήματα ελέγχου. Η οργάνωση των δημοκρατικών διαδικασιών, όπως οι εκλογές, θα βασίζεται επίσης όλο και περισσότερο στις ψηφιακές υποδομές και στα δίκτυα 5G.

(3) Η εξάρτηση πολλών υπηρεσιών ζωτικής σημασίας από τα δίκτυα 5G συνεπάγεται σοβαρότατες συνέπειες σε περίπτωση συστημικής και εκτεταμένης διαταραχής. Ως εκ τούτου, η κατοχύρωση της κυβερνοασφάλειας των δικτύων 5G αποτελεί ζήτημα στρατηγικής σημασίας για την Ένωση, σε μια περίοδο κατά την οποία οι κυβερνοεπιθέσεις αυξάνονται συνεχώς και χρησιμοποιούν πιο σύνθετες μεθόδους από ποτέ.

(4) Λόγω του διασυνδεμένου και διακρατικού χαρακτήρα των υποδομών στις οποίες βασίζεται το ψηφιακό οικοσύστημα, καθώς και του διασυνοριακού χαρακτήρα των σχετικών απειλών, τα τυχόν σημαντικά τρωτά σημεία και/ή περιστατικά κυβερνοασφάλειας που αφορούν δίκτυα 5G και εκδηλώνονται σε ένα κράτος μέλος θα μπορούσαν να επηρεάσουν την Ένωση στο σύνολό της. Για τον λόγο αυτό, θα πρέπει να ληφθούν μέτρα για τη στήριξη ενός υψηλού κοινού επιπέδου κυβερνοασφάλειας των δικτύων 5G.

(5) Η ανάγκη δράσης σε ενωσιακό επίπεδο επιβεβαιώθηκε από τα κράτη μέλη. Σύμφωνα με τα συμπεράσματά του της 21ης Μαρτίου 2019, το Ευρωπαϊκό Συμβούλιο προσβλέπει στη σύσταση της Επιτροπής για μια εναρμονισμένη προσέγγιση όσον αφορά την ασφάλεια των δικτύων 5G ([2]).

(6) Η διασφάλιση της ευρωπαϊκής κυριαρχίας θα πρέπει να αποτελεί μείζονα στόχο, με πλήρη σεβασμό των ευρωπαϊκών αξιών της ανοιχτότητας και της ανεκτικότητας ([3]). Οι ξένες επενδύσεις σε στρατηγικούς τομείς, η απόκτηση κρίσιμων περιουσιακών στοιχείων, τεχνολογιών και υποδομών στην Ένωση και η προμήθεια εξοπλισμού κρίσιμης σημασίας ενδέχεται επίσης να ενέχουν κινδύνους για την ασφάλεια της Ένωσης.

(7) Η κυβερνοασφάλεια των δικτύων 5G είναι καίριας σημασίας για τη διασφάλιση της στρατηγικής αυτονομίας της Ένωσης, όπως αναγνωρίζεται στην κοινή ανακοίνωση «ΕΕ-Κίνα — Στρατηγική προοπτική» ([4]).

(8) Στο ψήφισμα του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις απειλές κατά της ασφάλειας που συνδέονται με την αυξανόμενη τεχνολογική παρουσία της Κίνας στην ΕΕ, η Επιτροπή και τα κράτη μέλη καλούνται επίσης να αναλάβουν δράση σε ενωσιακό επίπεδο ([5]).

(9) Στην παρούσα σύσταση εξετάζονται οι κίνδυνοι κυβερνοασφάλειας στα δίκτυα 5G με τον καθορισμό κατευθυντήριων γραμμών για την κατάλληλη ανάλυση των κινδύνων και τα μέτρα διαχείρισης της επικινδυνότητας σε εθνικό επίπεδο, για την ανάπτυξη μιας συντονισμένης ευρωπαϊκής εκτίμησης της επικινδυνότητας και για την καθιέρωση διαδικασίας για την ανάπτυξη κοινής εργαλειοθήκης με τα βέλτιστα μέτρα διαχείρισης της επικινδυνότητας.

(10) Υπάρχει ένα ισχυρό ενωσιακό νομοθετικό πλαίσιο για την προστασία των δικτύων ηλεκτρονικών επικοινωνιών.

([1]) COM(2016) 588 final.
([2]) Συμπεράσματα του Ευρωπαϊκού Συμβουλίου της 21ης και της 22ας Μαρτίου 2019.
([3]) Η Κατάσταση της Ένωσης το 2018 — Η ώρα της ευρωπαϊκής κυριαρχίας, 12 Σεπτεμβρίου 2018.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//EN.

(11) Το πλαίσιο της Ένωσης στον τομέα των ηλεκτρονικών επικοινωνιών ([6]) προάγει τον ανταγωνισμό, την εσωτερική αγορά και τα συμφέροντα των τελικών χρηστών, και με τον ευρωπαϊκό κώδικα ηλεκτρονικών επικοινωνιών ([7]) επιδιώκει τον πρόσθετο στόχο της συνδεσιμότητας, ο οποίος διαρθρώνεται με βάση τα αποτελέσματα: ευρεία πρόσβαση σε πολύ υψηλής δυναμικότητας σταθερή και κινητή συνδεσιμότητα και εξάπλωση αυτής για όλους τους πολίτες και τις επιχειρήσεις της Ένωσης, με παράλληλη διασφάλιση των συμφερόντων των πολιτών. Η οδηγία 2002/21/ΕΚ απαιτεί από τα κράτη μέλη να εγγυώνται τη διατήρηση της ακεραιότητας και της ασφάλειας των δημόσιων δικτύων επικοινωνιών, με υποχρεώσεις να διασφαλίζουν ότι οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό λαμβάνουν τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση των κινδύνων για την ασφάλεια των δικτύων και των υπηρεσιών. Προβλέπει επίσης ότι οι αρμόδιες εθνικές ρυθμιστικές αρχές διαθέτουν εξουσίες, συμπεριλαμβανομένης της εξουσίας έκδοσης δεσμευτικών οδηγιών, για να διασφαλίζουν τη συμμόρφωση με τις εν λόγω υποχρεώσεις.

(12) Επιπλέον, η οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([8]) επιτρέπει στα κράτη μέλη να συνδέουν με τη γενική άδεια όρους σχετικούς με την προστασία των δημόσιων δικτύων έναντι μη εξουσιοδοτημένης πρόσβασης, με σκοπό την προστασία του απορρήτου των επικοινωνιών σύμφωνα με την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([9]).

(13) Για τη στήριξη της υλοποίησης των εν λόγω υποχρεώσεων, η Ένωση έχει συστήσει μια σειρά φορέων συνεργασίας. Ο Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), η Επιτροπή, τα κράτη μέλη και οι εθνικές ρυθμιστικές αρχές έχουν εκπονήσει τεχνικές κατευθυντήριες γραμμές για τις εθνικές ρυθμιστικές αρχές σχετικά με την αναφορά συμβάντων, τα μέτρα προστασίας, τις απειλές και τα περιουσιακά στοιχεία ([10]). Η ομάδα συνεργασίας που συστάθηκε με την οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([11]) («η ομάδα συνεργασίας») συγκεντρώνει αρμόδιες αρχές με σκοπό τη στήριξη και τη διευκόλυνση της συνεργασίας, ιδίως διά της παροχής στρατηγικής καθοδήγησης για τις δραστηριότητες του δικτύου των ομάδων απόκρισης σε συμβάντα που αφορούν την ασφάλεια των υπολογιστών, το οποίο διευκολύνει σε τεχνικό επίπεδο την επιχειρησιακή συνεργασία.

(14) Το μελλοντικό ευρωπαϊκό πλαίσιο για την πιστοποίηση της κυβερνοασφάλειας ([12]) αναμένεται να παρέχει ένα ουσιαστικό εργαλείο στήριξης για την προώθηση συνεκτικών επιπέδων προστασίας. Θα επιτρέπει την ανάπτυξη συστημάτων πιστοποίησης της κυβερνοασφάλειας τα οποία θα ανταποκρίνονται στις ανάγκες των χρηστών εξοπλισμού και λογισμικού που σχετίζεται με το 5G. Λόγω της κρίσιμης σημασίας των υποδομών αυτών, η ανάπτυξη των σχετικών ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας των προϊόντων, των υπηρεσιών ή των διαδικασιών των τεχνολογιών πληροφοριών και επικοινωνιών που χρησιμοποιούνται στα δίκτυα 5G θα πρέπει να καταστεί άμεση προτεραιότητα. Τα κράτη μέλη και οι παράγοντες της αγοράς θα πρέπει να συμμετάσχουν ενεργά στην ανάπτυξη των εν λόγω συστημάτων πιστοποίησης, μεταξύ άλλων με την παροχή στήριξης για τον ορισμό ειδικών χαρακτηριστικών προστασίας για τα δίκτυα 5G.

(15) Ελλείψει εναρμονισμένης ενωσιακής νομοθεσίας, τα κράτη μέλη δύνανται να καθορίζουν, μέσω εθνικών τεχνικών κανονισμών, οι οποίοι εκδίδονται σύμφωνα με το ενωσιακό δίκαιο, ότι ένα ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας θα πρέπει να είναι υποχρεωτικό. Τα κράτη μέλη προσφεύγουν επίσης σε ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας στο πλαίσιο δημοσίων συμβάσεων και της οδηγίας 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([13]) και θα μπορούσαν να υποστηρίξουν την ανάπτυξη μηχανισμών συνδρομής — όπως ένας κόμβος παροχής βοήθειας— για την αγορά λύσεων κυβερνοασφάλειας από δημόσιους αγοραστές.

(16) Η υψηλή στάθμη προστασίας των δεδομένων και της ιδιωτικής ζωής αποτελεί σημαντικό στοιχείο για την κατοχύρωση της ασφάλειας των δικτύων 5G. Επίσης, έχουν οριστεί κανόνες σε ενωσιακό επίπεδο οι οποίοι κατοχυρώνουν την ασφάλεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων στις ηλεκτρονικές επικοινωνίες. Ο γενικός κανονισμός για την προστασία δεδομένων ([14]) θεσπίζει την υποχρέωση επεξεργασίας των δεδομένων προσωπικού

([6]) Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία-πλαίσιο) (ΕΕ L 108 της 24.4.2002, σ. 33) και οι ειδικές οδηγίες.

([7]) Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Δεκεμβρίου 2018, για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (ΕΕ L 321 της 17.12.2018, σ. 36).

([8]) Οδηγία 2002/20/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών (οδηγία για την αδειοδότηση) (ΕΕ L 108 της 24.4.2002, σ. 21).

([9]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) 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 (ΕΕ L 194 της 19.7.2016, σ. 1).

([12]) 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 — 2017/0225 (COD)].

([13]) Οδηγία 2014/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Φεβρουαρίου 2014, σχετικά με τις δημόσιες προμήθειες και την κατάργηση της οδηγίας 2004/18/ΕΚ (ΕΕ L 94 της 28.3.2014, σ. 65).

([14]) 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) (ΕΕ L 119 της 4.5.2016, σ. 1).

χαρακτήρα κατά τρόπο που να κατοχυρώνει την ασφάλειά τους, μεταξύ άλλων για την πρόληψη της μη εξουσιοδοτημένης πρόσβασης ή χρήσης δεδομένων προσωπικού χαρακτήρα και του εξοπλισμού που χρησιμοποιείται για την επεξεργασία. Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θεσπίζει ειδικούς κανόνες για την προστασία του απορρήτου των επικοινωνιών και του τερματικού εξοπλισμού των τελικών χρηστών. Επιβάλλει επίσης στους παρόχους υπηρεσιών την υποχρέωση λήψης κατάλληλων τεχνικών και οργανωτικών μέτρων για τη διαφύλαξη της ασφάλειας των υπηρεσιών τους.

(17) Η Ένωση εξέδωσε επίσης ένα μέσο που θα προστατεύει τις υποδομές και τις τεχνολογίες ζωτικής σημασίας, όπως αυτές που χρησιμοποιούνται στις επικοινωνίες, επιτρέποντας στα κράτη μέλη να ελέγχουν τις άμεσες ξένες επενδύσεις για λόγους ασφάλειας ή δημόσιας τάξης, και δημιουργώντας έναν μηχανισμό συνεργασίας όπου τα κράτη μέλη και η Επιτροπή θα είναι σε θέση να ανταλλάσσουν πληροφορίες και να εκφράζουν τις ανησυχίες τους σχετικά με συγκεκριμένες επενδύσεις ([15]).

(18) Τα κράτη μέλη και οι φορείς εκμετάλλευσης πραγματοποιούν επί του παρόντος σημαντικά προπαρασκευαστικά βήματα που θα καταστήσουν δυνατή την εισαγωγή των δικτύων 5G σε ευρεία κλίμακα. Αρκετά κράτη μέλη έχουν εκφράσει ανησυχίες σχετικά με τους δυνητικούς κινδύνους για την ασφάλεια που συνδέονται με τα δίκτυα 5G στο πλαίσιο της διεξαγωγής διαδικασιών για τη χορήγηση δικαιωμάτων χρήσης σε ζώνες ραδιοφάσματος που ορίζονται για τα δίκτυα 5G ([16]) και εξετάζουν μέτρα για την αντιμετώπιση αυτών των κινδύνων.

(19) Για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας στα δίκτυα 5G θα πρέπει να λαμβάνονται υπόψη τόσο οι τεχνικοί παράγοντες όσο και παράγοντες άλλου είδους. Στους τεχνικούς παράγοντες μπορεί να συγκαταλέγονται τρωτά σημεία κυβερνοασφάλειας τα οποία μπορούν να αξιοποιηθούν για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες (κυβερνοκατασκοπεία, είτε για οικονομικούς είτε για πολιτικούς λόγους) ή για άλλους κακόβουλους σκοπούς (κυβερνοεπιθέσεις που αποσκοπούν στη διατάραξη ή την καταστροφή συστημάτων και δεδομένων). Οι σημαντικές πτυχές που πρέπει να εξεταστούν θα πρέπει να είναι η ανάγκη προστασίας των δικτύων καθ' όλη τη διάρκεια του κύκλου ζωής τους και η ανάγκη κάλυψης όλου του σχετικού εξοπλισμού, συμπεριλαμβανομένων των φάσεων σχεδιασμού, ανάπτυξης, προμήθειας, εγκατάστασης, λειτουργίας και συντήρησης των δικτύων 5G.

(20) Άλλοι παράγοντες μπορούν, μεταξύ άλλων, να είναι οι κανονιστικές ή άλλες απαιτήσεις που επιβάλλονται στους προμηθευτές εξοπλισμού τεχνολογιών της πληροφορίας και των επικοινωνιών. Μια εκτίμηση της σημασίας των παραγόντων αυτών θα πρέπει να λαμβάνει υπόψη, μεταξύ άλλων, τον συνολικό κίνδυνο επιρροής από τρίτη χώρα, ιδίως σε σχέση με το μοντέλο διακυβέρνησης της εν λόγω χώρας, την απουσία συμφωνιών συνεργασίας για την ασφάλεια ή παρόμοιων ρυθμίσεων, όπως αποφάσεις επάρκειας, όσον αφορά την προστασία των δεδομένων μεταξύ της Ένωσης και της εν λόγω τρίτης χώρας, ή το κατά πόσον η εν λόγω χώρα είναι συμβαλλόμενο μέρος σε πολυμερείς, διεθνείς ή διμερείς συμφωνίες κυβερνοασφάλειας, καθώς και την καταπολέμηση του κυβερνοεγκλήματος ή την προστασία των δεδομένων.

(21) Ως σημαντικό βήμα για την ανάπτυξη μιας ενωσιακής προσέγγισης στην κυβερνοασφάλεια των δικτύων 5G, θα πρέπει να διενεργείται και να ολοκληρώνεται εκτίμηση επικινδυνότητας σε εθνικό επίπεδο. Αυτό θα βοηθήσει τα κράτη μέλη να προσαρμόσουν τα εθνικά μέτρα σχετικά με τις απαιτήσεις ασφάλειας και τη διαχείριση της επικινδυνότητας υπό το πρίσμα της εκτίμησης αυτής.

(22) Θα πρέπει να αναπτυχθεί συντονισμός για να διασφαλιστεί η αποτελεσματικότητα των μέτρων που στοχεύουν στην αντιμετώπιση των εν λόγω απειλών κυβερνοασφάλειας, τα οποία είναι απαραίτητα για την ομαλή λειτουργία της εσωτερικής αγοράς και για την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής.

(23) Οι εθνικές εκτιμήσεις επικινδυνότητας θα πρέπει να αποτελέσουν τη βάση για μια συντονισμένη ενωσιακή εκτίμηση επικινδυνότητας, η οποία θα αποτελείται από τη χαρτογράφηση των απειλών και από κοινή επανεξέταση που θα διενεργηθεί από τα κράτη μέλη, με τη στήριξη της Επιτροπής και από κοινού με τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ENISA).

(24) Λαμβάνοντας υπόψη τις εθνικές και τις ενωσιακές εκτιμήσεις επικινδυνότητας, η ομάδα συνεργασίας θα πρέπει να δημιουργήσει εργαλειοθήκη η οποία θα προσδιορίζει τους τύπους των κινδύνων κυβερνοασφάλειας και πιθανά μέτρα για τον μετριασμό των κινδύνων σε τομείς όπως η πιστοποίηση, οι δοκιμές και οι έλεγχοι πρόσβασης. Θα πρέπει επίσης να προσδιορίζει πιθανά ειδικά μέτρα αντιμετώπισης των κινδύνων που εντοπίζονται από ένα ή περισσότερα κράτη μέλη. Η ομάδα συνεργασίας θα πρέπει να βασιστεί στη στήριξη του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA), της Ευρωπόλ, του Φορέα Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC) και του Κέντρου Ανάλυσης και Πληροφοριών της ΕΕ (EU Intelligence and Situation Centre). Η εν λόγω εργαλειοθήκη θα χρησιμεύσει για την παροχή συμβουλών στην Επιτροπή σχετικά με την ανάπτυξη ελάχιστων κοινών απαιτήσεων για την περαιτέρω διασφάλιση υψηλού επιπέδου κυβερνοασφάλειας των δικτύων 5G σε ολόκληρη την Ένωση.

(25) Όταν λαμβάνονται μέτρα για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας, θα πρέπει να λαμβάνεται υπόψη η προώθηση της κυβερνοασφάλειας μέσω της ποικιλίας των προμηθευτών κατά την κατασκευή ενός μεμονωμένου δικτύου.

([15]) Κανονισμός (ΕΕ) 2019/452 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 19ης Μαρτίου 2019, για τη θέσπιση πλαισίου για τον έλεγχο των άμεσων ξένων επενδύσεων στην Ένωση (ΕΕ L 79Ι της 21.3.2019, σ. 1).

([16]) Η διαδικασία δημοπρασίας για τουλάχιστον μία ζώνη φάσματος έχει προγραμματιστεί εντός του 2019 σε 11 κράτη μέλη: Αυστρία, Βέλγιο, Τσεχία, Γαλλία, Γερμανία, Ελλάδα, Ουγγαρία, Ιρλανδία, Κάτω Χώρες, Λιθουανία, Πορτογαλία. Έξι ακόμη δημοπρασίες έχουν προγραμματιστεί για το 2020: Ισπανία, Μάλτα, Λιθουανία (διαφορετικές συχνότητες), Σλοβακία, Πολωνία, Ηνωμένο Βασίλειο. *Πηγή*: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Η παρούσα σύσταση δεν θα πρέπει να θίγει τις αρμοδιότητες των κρατών μελών όσον αφορά δραστηριότητες σχετικές με τη δημόσια ασφάλεια, την άμυνα, την εθνική ασφάλεια και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου, συμπεριλαμβανομένου του δικαιώματος των κρατών μελών να αποκλείουν παρόχους ή προμηθευτές από τις αγορές τους για λόγους εθνικής ασφάλειας,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΣΤΑΣΗ:

I. **ΣΤΟΧΟΙ**

1) Προκειμένου να υποστηριχθεί η ανάπτυξη μιας ενωσιακής προσέγγισης για την κατοχύρωση της κυβερνοασφάλειας των δικτύων 5G, η παρούσα σύσταση προσδιορίζει τις δράσεις που πρέπει να αναληφθούν ώστε να επιτραπεί:

α) στα κράτη μέλη να εκτιμούν τους κινδύνους κυβερνοασφάλειας που επηρεάζουν τα δίκτυα 5G σε εθνικό επίπεδο και να λαμβάνουν τα αναγκαία μέτρα ασφαλείας·

β) στα κράτη μέλη και στα σχετικά όργανα, οργανισμούς και άλλους φορείς της Ένωσης να εκπονούν από κοινού συντονισμένη ενωσιακή εκτίμηση επικινδυνότητας, η οποία θα βασίζεται στην εθνική εκτίμηση επικινδυνότητας.

γ) Στην ομάδα συνεργασίας που συστάθηκε βάσει της οδηγίας (ΕΕ) 2016/1148 (ομάδα συνεργασίας) να προσδιορίζει ένα πιθανό κοινό σύνολο μέτρων μετριασμού των κινδύνων για την κυβερνοασφάλεια που σχετίζονται με τις υποδομές στις οποίες βασίζεται το ψηφιακό οικοσύστημα, ιδίως τα δίκτυα 5G.

II. **ΟΡΙΣΜΟΙ**

2) Για τους σκοπούς της παρούσας σύστασης:

α) «δίκτυα 5G»: το σύνολο όλων των σχετικών στοιχείων των δικτυακών υποδομών για τεχνολογίες κινητών και ασύρματων επικοινωνιών που χρησιμοποιούνται για συνδεσιμότητα και υπηρεσίες προστιθέμενης αξίας με προηγμένα χαρακτηριστικά επιδόσεων, όπως πολύ μεγάλες ταχύτητες μεταφοράς δεδομένων και πολύ μεγάλη χωρητικότητα, για επικοινωνίες μικρού λανθάνοντα χρόνου, για υπερυψηλή αξιοπιστία, ή που υποστηρίζουν μεγάλο αριθμό συνδεδεμένων συσκευών. Στα στοιχεία αυτά μπορεί να περιλαμβάνονται κληροδοτημένα στοιχεία δικτύου που βασίζονται σε προηγούμενες γενιές τεχνολογιών κινητών και ασύρματων επικοινωνιών, όπως 4G ή 3G. Τα δίκτυα 5G θα πρέπει να θεωρείται ότι περιλαμβάνουν όλα τα σχετικά τμήματα του δικτύου·

β) «υποδομές που υποστηρίζουν το ψηφιακό οικοσύστημα»: οι υποδομές που χρησιμοποιούνται για να καταστεί δυνατή η ψηφιοποίηση σε ευρύ φάσμα κρίσιμων εφαρμογών στην οικονομία και την κοινωνία.

III. **ΔΡΑΣΗ ΣΕ ΕΘΝΙΚΟ ΕΠΙΠΕΔΟ**

3) Έως τις 30 Ιουνίου 2019, τα κράτη μέλη θα πρέπει να εκπονήσουν εκτίμηση επικινδυνότητας της δικτυακής υποδομής 5G, στην οποία θα πρέπει να συμπεριλαμβάνεται προσδιορισμός των πλέον ευαίσθητων στοιχείων τυχόν παραβιάσεις της ασφάλειας των οποίων θα είχαν σημαντικό αρνητικό αντίκτυπο. Έως την ίδια ημερομηνία, τα κράτη μέλη θα πρέπει επίσης να επανεξετάσουν τις απαιτήσεις ασφάλειας και τις μεθόδους διαχείρισης επικινδυνότητας που εφαρμόζονται σε εθνικό επίπεδο, ώστε να λάβουν υπόψη απειλές για την κυβερνοασφάλεια που μπορεί να προκύψουν από i) τεχνικούς παράγοντες, όπως τα ειδικά τεχνικά χαρακτηριστικά των δικτύων 5G, και ii) άλλους παράγοντες, όπως το νομικό πλαίσιο και το πλαίσιο πολιτικής στο οποίο ενδέχεται να υπόκεινται οι προμηθευτές εξοπλισμού τεχνολογιών των πληροφοριών και των επικοινωνιών σε τρίτες χώρες.

4) Με βάση την εν λόγω εθνική εκτίμηση επικινδυνότητας και την επανεξέταση, και λαμβάνοντας υπόψη την εν εξελίξει συντονισμένη δράση σε ενωσιακό επίπεδο, τα κράτη μέλη θα πρέπει:

α) να επικαιροποιούν τις απαιτήσεις ασφάλειας και τις μεθόδους διαχείρισης επικινδυνότητας που εφαρμόζονται σε σχέση με τα δίκτυα 5G·

β) να επικαιροποιούν τις σχετικές υποχρεώσεις που επιβάλλονται στις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών, δυνάμει των άρθρων 13α και 13β της οδηγίας 2002/21/ΕΚ·

γ) να συνδέουν με τη γενική άδεια όρους σχετικούς με την προστασία των δημόσιων δικτύων έναντι της μη εξουσιοδοτημένης πρόσβασης και να ζητούν από τις επιχειρήσεις που συμμετέχουν σε κάθε επικείμενη διαδικασία χορήγησης δικαιωμάτων χρήσης φάσματος στις ζώνες 5G δεσμεύσεις συμμόρφωσης με τις απαιτήσεις ασφάλειας για τα δίκτυα, δυνάμει της οδηγίας 2002/20/ΕΚ·

δ) να εφαρμόζουν άλλα προληπτικά μέτρα που αποσκοπούν στον μετριασμό των δυνητικών κινδύνων κυβερνοασφάλειας.

5) Τα μέτρα που αναφέρονται στο σημείο 4 θα πρέπει να περιλαμβάνουν ενισχυμένες υποχρεώσεις για τους προμηθευτές και τους φορείς εκμετάλλευσης όσον αφορά την κατοχύρωση της ασφάλειας ευαίσθητων τμημάτων των δικτύων, καθώς και υποχρεώσεις, κατά περίπτωση, όπως η παροχή σχετικών πληροφοριών στις αρμόδιες εθνικές αρχές σχετικά με σχεδιαζόμενες αλλαγές στα δίκτυα ηλεκτρονικών επικοινωνιών και απαιτήσεις εκ των προτέρων εξέτασης ειδικών κατασκευαστικών στοιχείων και συστημάτων τεχνολογίας πληροφοριών για σκοπούς ασφάλειας και ακεραιότητας από εθνικά εργαστήρια ελέγχου/πιστοποίησης.

6) Οι κοινές επανεξετάσεις ασφάλειας θα πρέπει να διενεργούνται από δύο ή περισσότερα κράτη μέλη, με χρήση και ανταλλαγή της κατάλληλης τεχνικής εμπειρογνωσίας και των εγκαταστάσεων που σχετίζονται με τις υποδομές στις οποίες βασίζονται το ψηφιακό οικοσύστημα και τα δίκτυα 5G, για παράδειγμα όταν η ίδια επιχείρηση εκμεταλλεύεται ή αναπτύσσει υποδομή δικτύου σε περισσότερα του ενός κράτη μέλη ή όταν υπάρχουν σημαντικές ομοιότητες στη διαμόρφωση των δικτύων. Ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA), η Ευρωπόλ και ο Φορέας Ευρωπαϊκών Ρυθμιστικών Αρχών για τις Ηλεκτρονικές Επικοινωνίες (BEREC) θα πρέπει να δίνουν προτεραιότητα σε αιτήματα για παροχή στήριξης από τα κράτη μέλη σε αυτόν τον τομέα. Τα αποτελέσματα των επανεξετάσεων αυτών θα πρέπει να διαβιβάζονται στην ομάδα συνεργασίας και στο δίκτυο των ομάδων απόκρισης σε συμβάντα που αφορούν την ασφάλεια υπολογιστών.

IV. **ΣΥΝΤΟΝΙΣΜΕΝΗ ΔΡΑΣΗ ΣΕ ΕΠΙΠΕΔΟ ΕΝΩΣΗΣ**

7) Προκειμένου να αναπτύξουν μια κοινή προσέγγιση για την αντιμετώπιση των κινδύνων κυβερνοασφάλειας σε σχέση με τα δίκτυα 5G, τα κράτη μέλη θα πρέπει να αρχίσουν να αναπτύσσουν δραστηριότητες στο πλαίσιο ειδικής ροής εργασίας στην ομάδα συνεργασίας έως τις 30 Απριλίου 2019. Τα κράτη μέλη θα πρέπει, κατά περίπτωση, να καλούν τις αρμόδιες αρχές να συμμετέχουν στις εργασίες της ομάδας συνεργασίας.

Συντονισμένη ευρωπαϊκή εκτίμηση επικινδυνότητας

8) Τα κράτη μέλη θα πρέπει να ανταλλάσσουν πληροφορίες μεταξύ τους και με τους αρμόδιους φορείς της Ένωσης για την οικοδόμηση κοινής επίγνωσης των υφιστάμενων και των δυνητικών κινδύνων κυβερνοασφάλειας που αφορούν τα δίκτυα 5G.

9) Τα κράτη μέλη θα πρέπει να διαβιβάσουν τις εθνικές τους εκτιμήσεις επικινδυνότητας στην Επιτροπή και στον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ENISA) έως τις 15 Ιουλίου 2019.

10) Ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA) θα πρέπει να ολοκληρώσει μια χαρτογράφηση των απειλών που αφορούν ειδικά τα δίκτυα 5G. Η ομάδα συνεργασίας και το δίκτυο των ομάδων απόκρισης σε συμβάντα που αφορούν την ασφάλεια των υπολογιστών, το οποίο έχει συσταθεί βάσει της οδηγίας (ΕΕ) 2016/1148 θα πρέπει να υποστηρίξουν τη διαδικασία αυτή.

11) Λαμβάνοντας υπόψη όλα αυτά τα στοιχεία και έως την 1η Οκτωβρίου 2019, τα κράτη μέλη με την υποστήριξη της Επιτροπής και από κοινού με τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ENISA) θα πρέπει να ολοκληρώσουν κοινή επανεξέταση της ενωσιακής έκθεσης σε κινδύνους που αφορούν υποδομές οι οποίες υποστηρίζουν το ψηφιακό οικοσύστημα, ιδίως δίκτυα 5G.

12) Η εν λόγω κοινή επανεξέταση θα πρέπει να δώσει προτεραιότητα στην ανάλυση των κινδύνων για τα ιδιαίτερα ευαίσθητα ή ευάλωτα στοιχεία που περιλαμβάνονται στα βασικά στοιχεία των δικτύων 5G, στο κέντρο επιχειρήσεων και συντήρησης, καθώς και στα στοιχεία του δικτύου πρόσβασης 5G που χρησιμοποιούνται για βιομηχανικές εφαρμογές.

13) Σε δεύτερο στάδιο, αυτή η κοινή επανεξέταση θα πρέπει να επεκταθεί και σε άλλα στρατηγικά στοιχεία της ψηφιακής αλυσίδας αξίας.

Κοινή εργαλειοθήκη της Ένωσης για την αντιμετώπιση των κινδύνων

14) Οι εργασίες της ομάδας συνεργασίας θα πρέπει να προσδιορίζουν τα μέτρα βέλτιστων πρακτικών που εφαρμόζονται σε εθνικό επίπεδο του τύπου που προβλέπεται στο σημείο 4. Με βάση αυτές τις εθνικές βέλτιστες πρακτικές, θα πρέπει να συμφωνηθεί έως τις 31 Δεκεμβρίου 2019 μια εργαλειοθήκη κατάλληλων, αποτελεσματικών και αναλογικών μέτρων διαχείρισης επικινδυνότητας για τον μετριασμό των προσδιορισμένων κινδύνων κυβερνοασφάλειας σε εθνικό και ενωσιακό επίπεδο, για την παροχή συμβουλών στην Επιτροπή σχετικά με τη θέσπιση ελάχιστων κοινών απαιτήσεων για την περαιτέρω εγγύηση υψηλού επιπέδου κυβερνοασφάλειας των δικτύων 5G σε ολόκληρη την Ένωση.

15) Η εν λόγω εργαλειοθήκη θα πρέπει να περιλαμβάνει:

α) κατάλογο των ειδών κινδύνων που μπορούν να επηρεάσουν την κυβερνοασφάλεια των δικτύων 5G (π.χ. κίνδυνος αλυσίδας εφοδιασμού, κίνδυνος ευπάθειας του λογισμικού, κίνδυνος του ελέγχου πρόσβασης, κίνδυνοι που απορρέουν από το νομικό πλαίσιο και το πλαίσιο πολιτικής στο οποίο ενδέχεται να υπόκεινται οι προμηθευτές εξοπλισμού τεχνολογιών της πληροφορίας και των επικοινωνιών σε τρίτες χώρες)· και

β) δέσμη πιθανών μέτρων μετριασμού (π.χ. πιστοποίηση τρίτων μερών για υλισμικό, λογισμικό ή υπηρεσίες, τυπικές δοκιμές ή έλεγχοι συμμόρφωσης υλισμικού και λογισμικού, διαδικασίες διασφάλισης της ύπαρξης και εφαρμογής ελέγχων πρόσβασης, προσδιορισμός των προϊόντων, υπηρεσιών ή προμηθευτών που θεωρούνται δυνητικά μη ασφαλή κ. λπ.). Τα μέτρα αυτά θα πρέπει να αντιμετωπίζουν κάθε είδος κινδύνου ασφάλειας που προσδιορίζεται σε ένα ή περισσότερα κράτη μέλη μετά την εκτίμηση επικινδυνότητας.

16) Μόλις ολοκληρωθούν τα ευρωπαϊκά συστήματα πιστοποίησης της κυβερνοασφάλειας που αφορούν δίκτυα 5G, τα κράτη μέλη θα πρέπει να εγκρίνουν, σύμφωνα με το δίκαιο της Ένωσης, εθνικούς τεχνικούς κανονισμούς που προβλέπουν την υποχρεωτική πιστοποίηση προϊόντων, υπηρεσιών ή συστημάτων τεχνολογιών της πληροφορίας και των επικοινωνιών που καλύπτονται από τα εν λόγω συστήματα.

17) Τα κράτη μέλη, από κοινού με την Επιτροπή, θα πρέπει να προσδιορίσουν τους όρους προστασίας των δημόσιων δικτύων από μη εξουσιοδοτημένη πρόσβαση οι οποίοι πρέπει να συνδέονται με τη γενική άδεια και τις απαιτήσεις ασφάλειας των δικτύων για τους σκοπούς των υποχρεωτικών δεσμεύσεων των επιχειρήσεων που συμμετέχουν σε διαδικασίες χορήγησης δικαιωμάτων χρήσης φάσματος στις ζώνες 5G δυνάμει της οδηγίας 2002/20/ΕΚ. Οι απαιτήσεις αυτές θα πρέπει να αντικατοπτρίζονται, όπου είναι δυνατόν, στα μέτρα που λαμβάνονται στο σημείο 4 στοιχείο γ).

18) Τα κράτη μέλη θα πρέπει να συνεργάζονται με την Επιτροπή για την εκπόνηση ειδικών απαιτήσεων ασφάλειας που θα μπορούσαν να εφαρμόζονται στο πλαίσιο δημοσίων συμβάσεων που συνδέονται με δίκτυα 5G. Εν προκειμένω θα πρέπει να περιλαμβάνονται υποχρεωτικές απαιτήσεις για την εφαρμογή συστημάτων πιστοποίησης της κυβερνοασφάλειας στις δημόσιες συμβάσεις, εφόσον τα εν λόγω συστήματα δεν είναι ακόμη δεσμευτικά για όλους τους προμηθευτές και τους φορείς εκμετάλλευσης.

V. **ΕΠΑΝΕΞΕΤΑΣΗ**

19) Τα κράτη μέλη θα πρέπει να συνεργαστούν με την Επιτροπή για την επανεξέταση των επιπτώσεων της παρούσας σύστασης έως την 1η Οκτωβρίου 2020, με σκοπό να καθορίσουν την πορεία που θα πρέπει να ακολουθήσουν. Η επανεκτίμηση αυτή θα πρέπει να λαμβάνει υπόψη το πόρισμα της συντονισμένης ενωσιακής εκτίμησης επικινδυνότητας και την ενωσιακή εργαλειοθήκη.

Στρασβούργο, 26 Μαρτίου 2019.

Για την Επιτροπή
Julian KING
Μέλος της Επιτροπής