Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 17 Οκτωβρίου 2022
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΩΝ ΕΡΓΑΣΙΩΝ

Αποστολέας:	Γενική Γραμματεία του Συμβουλίου
Με ημερομηνία:	17 Οκτωβρίου 2022
Αποδέκτης:	Αντιπροσωπίες
αριθ. προηγ. εγγρ.:	12930/22
Θέμα:	Συμπεράσματα του Συμβουλίου σχετικά με την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ — Συμπεράσματα του Συμβουλίου τα οποία ενέκρινε το Συμβούλιο κατά τη σύνοδο της 17ης Οκτωβρίου 2022

Διαβιβάζονται συνημμένως στις αντιπροσωπίες τα συμπεράσματα του Συμβουλίου σχετικά με την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ, όπως εγκρίθηκαν από το Συμβούλιο κατά τη σύνοδο της 17ης Οκτωβρίου 2022.

ΠΑΡΑΡΤΗΜΑ

Συμπεράσματα του Συμβουλίου σχετικά με την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ

ΤΟ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματά του σχετικά με

– την κοινή ανακοίνωση της 20ής Νοεμβρίου 2017 προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ»,

– την οικοδόμηση ικανοτήτων και δυνατοτήτων κυβερνοασφάλειας στην ΕΕ,

– τη σημασία του 5G για την ευρωπαϊκή οικονομία και την ανάγκη μετριασμού των κινδύνων ασφάλειας που συνδέονται με το 5G,

– τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης,

– «Μια ανάκαμψη που προωθεί τη μετάβαση προς μια πιο δυναμική, ανθεκτική και ανταγωνιστική ευρωπαϊκή βιομηχανία»,

– την κυβερνοασφάλεια των συνδεδεμένων συσκευών,

– τη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία,

– τη διαμόρφωση της στάσης της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο,

– την ειδική έκθεση αριθ. 03/2022 του Ευρωπαϊκού Ελεγκτικού Συνεδρίου με τίτλο «Τεχνολογία 5G στην ΕΕ: καθυστερήσεις στην ανάπτυξη των δικτύων και ανεπίλυτα ζητήματα ασφάλειας»,

ΥΠΕΝΘΥΜΙΖΟΝΤΑΣ τα συμπεράσματα του Ευρωπαϊκού Συμβουλίου με θέμα:

– την πανδημία COVID-19, την ενιαία αγορά, τη βιομηχανική πολιτική, την ψηφιακή διάσταση και τις εξωτερικές σχέσεις, της 1ης-2ας Οκτωβρίου 2020,

– τη ρωσική στρατιωτική επίθεση κατά της Ουκρανίας, την ασφάλεια και την άμυνα, την ενέργεια, οικονομικά ζητήματα, την COVID-19 και τις εξωτερικές σχέσεις, της 24ης-25ης Μαρτίου 2022,

– την Ουκρανία, την επισιτιστική ασφάλεια, την ασφάλεια και άμυνα και την ενέργεια, της 30ής-31ης Μαΐου 2022,

1. Λόγω της αυξανόμενης συνάφειας της γεωπολιτικής ως προς την ασφάλεια στον κυβερνοχώρο, ΤΟΝΙΖΕΙ ότι η Ευρωπαϊκή Ένωση και τα κράτη μέλη της πρέπει να προσεγγίζουν την ασφάλεια στον κυβερνοχώρο με ολοκληρωμένο και στρατηγικό τρόπο. Η στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας έχει μεταβάλει ριζικά το στρατηγικό περιβάλλον και το περιβάλλον ασφάλειας της Ευρωπαϊκής Ένωσης και έχει καταδείξει την ανάγκη για μια ισχυρότερη και ικανότερη Ευρωπαϊκή Ένωση στον τομέα της ασφάλειας και της άμυνας. Έχει τονίσει ότι έχει ύψιστη σημασία το γεωπολιτικό περιβάλλον να λαμβάνεται δεόντως υπόψη όχι μόνο για την αντίδραση σε κακόβουλες δραστηριότητες στον κυβερνοχώρο, αλλά και κατά την οικοδόμηση και διατήρηση της ανθεκτικότητας των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ). Αυτό έχει ιδιαίτερη σημασία για τις αλυσίδες εφοδιασμού προϊόντων και υπηρεσιών ΤΠΕ (αλυσίδες εφοδιασμού ΤΠΕ), οι οποίες θα μπορούσαν αφενός να βρεθούν εκτεθειμένες εξαιτίας γεωπολιτικών αντιπαλοτήτων, όπως φάνηκε με την επίθεση SolarWinds, και αφετέρου να επηρεάζονται από γεωπολιτικές εντάσεις και αστάθεια, όπως φάνηκε στη στρατιωτική επίθεση της Ρωσίας κατά της Ουκρανίας, με την απειλή λόγω της εξάρτησης από Ρώσους παρόχους ΤΠΕ.

2. ΣΗΜΕΙΩΝΕΙ ότι ο χαρακτήρας των κινδύνων που συνδέονται με την αλυσίδα εφοδιασμού ΤΠΕ, η οποία αποτελείται από ένα αλληλένδετο σύνολο πόρων και διαδικασιών μεταξύ οικονομικών φορέων (όπως ορίζονται στον κανονισμό (ΕΕ) 2019/1020) που ξεκινά με την προμήθεια των πρώτων υλών και επεκτείνεται στην κατασκευή, την επεξεργασία, το χειρισμό και την παράδοση προϊόντων και υπηρεσιών ΤΠΕ, καθώς και στην παροχή στήριξης κατά τη διάρκεια του κύκλου ζωής των προϊόντων και των υπηρεσιών ΤΠΕ, δημιουργεί μοναδικές προκλήσεις και δυνητικά εκτεταμένες συνέπειες. Εκτός από τον κίνδυνο προϊόντα ΤΠΕ να μην είναι διαθέσιμα, για παράδειγμα, λόγω ελλείψεων κρίσιμων πρώτων υλών και ημιαγωγών που απαιτούνται για την παραγωγή τους, οι αλυσίδες εφοδιασμού προϊόντων και υπηρεσιών ΤΠΕ είναι εκτεθειμένες και σε άλλες απειλές. Πιο συγκεκριμένα, μπορεί να αποτελούν στόχο ή να χρησιμοποιούνται καταχρηστικά από κακόβουλους δρώντες που διαθέτουν εξελιγμένους, συχνά συγκεκαλυμμένους, τρόπους, οι οποίοι έχουν επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των μεταδιδόμενων και αποθηκευόμενων ευαίσθητων δεδομένων.

3. Έχοντας επίγνωση ότι, για να είναι ασφαλείς οι πόροι ΤΠΕ, απαιτείται μια προσέγγιση που θα συνυπολογίζει όλους τους κινδύνους, ΑΝΑΓΝΩΡΙΖΕΙ ότι η πρόταση οδηγίας για την ανθεκτικότητα των κρίσιμων οντοτήτων είναι ορθή για τη βελτίωση της φυσικής ασφάλειας των κρίσιμων οντοτήτων, και ΤΟΝΙΖΕΙ ότι, εκτός από την ενίσχυση της ανθεκτικότητας έναντι επιθέσεων κατά της αλυσίδας εφοδιασμού που πραγματοποιούνται με μέσα του κυβερνοχώρου, είναι εξίσου σημαντικό να ενισχυθεί η συνολική ανθεκτικότητα και ασφάλεια των αλυσίδων εφοδιασμού ΤΠΕ έναντι ολόκληρου του φάσματος των παραγόντων απειλής, όπως φυσικά συμβάντα, αστοχίες συστημάτων, εκ των έσω απειλές ή ανθρώπινα σφάλματα. Υπό την έννοια αυτή, ΑΝΑΓΝΩΡΙΖΕΙ ότι η ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ περιλαμβάνει τη διασφάλιση της προστασίας των προϊόντων και των υπηρεσιών ΤΠΕ που παράγονται, παραδίδονται, αποτελούν αντικείμενο προμήθειας και χρησιμοποιούνται σε αλυσίδες εφοδιασμού ΤΠΕ, μεταξύ άλλων μέσω της προστασίας των επιμέρους συνιστωσών και των διαβιβαζόμενων δεδομένων.

4. Με βάση τα διδάγματα που αντλούνται από τις συνέπειες των στρατηγικών εξαρτήσεων της Ευρωπαϊκής Ένωσης από τα ρωσικά ορυκτά καύσιμα, καθώς και από τις επιπτώσεις των διαταραχών στις αλυσίδες εφοδιασμού κατά τη διάρκεια της πανδημίας COVID-19, ιδίως σε ό,τι αφορά τα φαρμακευτικά προϊόντα και τους ημιαγωγούς, όπου αναδείχθηκαν οι στρατηγικές εξαρτήσεις της ΕΕ, ΠΑΡΟΤΡΥΝΕΙ τα κράτη μέλη να εργαστούν για την αποφυγή παρόμοιων καταστάσεων με ανεπιθύμητες στρατηγικές εξωτερικές εξαρτήσεις σε σχέση με προϊόντα και υπηρεσίες ΤΠΕ. Λόγω της εντεινόμενης ψηφιοποίησης της κοινωνίας και της συνεχώς αυξανόμενης χρήσης των ΤΠΕ σε υποδομές ζωτικής σημασίας, οι στρατηγικές εξωτερικές εξαρτήσεις που σχετίζονται με προϊόντα και υπηρεσίες ΤΠΕ και τις αλυσίδες εφοδιασμού τους θα πρέπει να αξιολογούνται συνεχώς και, κατά περίπτωση, να αντιμετωπίζονται.

5. ΥΠΕΝΘΥΜΙΖΕΙ ότι η επίτευξη στρατηγικής αυτονομίας με παράλληλη διατήρηση μιας ανοικτής οικονομίας αποτελεί βασικό στόχο της Ένωσης, ο οποίος περιλαμβάνει τον εντοπισμό και τον περιορισμό των στρατηγικών εξαρτήσεων και την αύξηση της ανθεκτικότητας στα πιο ευαίσθητα βιομηχανικά οικοσυστήματα και σε συγκεκριμένους τομείς, μεταξύ άλλων στον ψηφιακό τομέα. Η στρατιωτική αυτονομία περνά μέσα από την ανάπτυξη και την υλοποίηση στρατηγικών ψηφιακών ικανοτήτων και υποδομών, καθώς και την ενίσχυση της ικανότητας πραγματοποίησης αυτόνομων τεχνολογικών επιλογών και, ως έναν από τους κύριους πυλώνες, τη διασφάλιση ανθεκτικών και ασφαλών υποδομών, προϊόντων και υπηρεσιών για να οικοδομηθεί εμπιστοσύνη στην ψηφιακή ενιαία αγορά και στους κόλπους της ευρωπαϊκής κοινωνίας, διατηρώντας παράλληλα τον ανοικτό χαρακτήρα, την παγκόσμια συνεργασία με ομόφρονες εταίρους και την ανταγωνιστικότητα, αξιοποιώντας τα οφέλη που μπορούν να αποφέρουν. Οι θεμελιώδεις αξίες της Ευρωπαϊκής Ένωσης προασπίζονται ειδικότερα την ιδιωτική ζωή, την ασφάλεια, την ισότητα, την ανθρώπινη αξιοπρέπεια, το κράτος δικαίου και το ανοικτό διαδίκτυο ως προϋποθέσεις για την επίτευξη μιας ανθρωποκεντρικής κοινωνίας, οικονομίας και βιομηχανίας με κινητήρια δύναμη την ψηφιακή διάσταση.

6. ΣΗΜΕΙΩΝΕΙ ότι, λόγω των εξελίξεων στο τοπίο των κυβερνοαπειλών —όπου τα τελευταία χρόνια καταγράφεται τάση για εξελιγμένες και σοβαρού αντικτύπου επιθέσεις στην αλυσίδα εφοδιασμού, όπως οι επιθέσεις SolarWinds, Mimecast ή Kaseya, οι οποίες εμφανίζονται μαζί με την εξωτερική ανάθεση βασικών υπηρεσιών ΤΠΕ και επιτείνονται από τη συνολική εξάρτηση από προϊόντα και υπηρεσίες ΤΠΕ που κατασκευάζονται, παρέχονται ή εξυπηρετούνται από τρίτους— είναι εξαιρετικά πιθανό να υπάρξουν στο μέλλον περισσότερες επιθέσεις στην αλυσίδα εφοδιασμού, ζημιώνοντας σημαντικά την οικονομία και την κοινωνία. Με βάση τα ανωτέρω, ΤΟΝΙΖΕΙ τη σημασία της ενίσχυσης της ασφάλειας και της ανθεκτικότητας των αλυσίδων εφοδιασμού ΤΠΕ για τη λειτουργία της ενιαίας αγοράς, σε συνδυασμό με την ανάγκη να εξασφαλιστεί διαθεσιμότητα, ασφάλεια και ποικιλομορφία προϊόντων και υπηρεσιών ΤΠΕ στην ενιαία αγορά. Ως εκ τούτου, ΑΝΑΓΝΩΡΙΖΕΙ την ανάγκη μεγιστοποίησης και εξορθολογισμού της χρήσης των υφιστάμενων μέσων και προσεγγίσεων της ΕΕ για να επιτευχθούν αυτοί οι στόχοι, καθώς και την ανάγκη συνεχούς προσαρμογής στο μεταβαλλόμενο τοπίο των κυβερνοαπειλών με τη θέσπιση πρόσθετων κατάλληλων μέτρων και μηχανισμών, μεταξύ άλλων σε σχέση με πιθανούς κινδύνους για την ασφάλεια λόγω αναδυόμενων και ανατρεπτικών τεχνολογιών. ΠΑΡΟΤΡΥΝΕΙ τα κράτη μέλη να υιοθετούν, στο πλαίσιο αυτό, την προσέγγιση βάσει κινδύνου για να αντιμετωπίζουν νέες τεχνολογικές εξελίξεις.

7. ΑΝΑΓΝΩΡΙΖΕΙ ότι η κατανόηση του διαρκώς εξελισσόμενου τοπίου των κυβερνοαπειλών καθώς και της πολυπλοκότητας των επιθέσεων στην αλυσίδα εφοδιασμού έχει καθοριστική σημασία για τον αποτελεσματικό μετριασμό των κινδύνων που συνδέονται με τις αλυσίδες εφοδιασμού ΤΠΕ. Στο πλαίσιο αυτό, ΤΟΝΙΖΕΙ την ανάγκη για προσαρμογή στις νέες απειλές μέσω της ενεργού και συνεχούς παρακολούθησης, ανάλυσης και αξιολόγησης του τοπίου των απειλών στην αλυσίδα εφοδιασμού, για αύξηση της ευαισθητοποίησης και για απόκτηση γνώσεων σχετικά με τις απειλές και τα τρωτά σημεία, καθώς και για προορατική προειδοποίηση των σχετικών οντοτήτων με εξατομικευμένο τρόπο. ΧΑΙΡΕΤΙΖΕΙ το έργο του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) σχετικά με την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ, ιδίως δε την έκθεσή του με θέμα «Το τοπίο απειλών για επιθέσεις στην αλυσίδα εφοδιασμού».

ΔΙΑΤΟΜΕΑΚΑ ΜΕΣΑ ΚΑΙ ΠΡΟΣΕΓΓΙΣΕΙΣ

8. ΕΠΙΒΕΒΑΙΩΝΕΙ ότι είναι σημαντικό τα κράτη μέλη να εξετάζουν την ανάγκη διαφοροποίησης των προμηθευτών κρίσιμων ΤΠΕ, ώστε να αποφεύγεται ή να περιορίζεται η δημιουργία σοβαρών εξαρτήσεων από μεμονωμένους προμηθευτές και ιδίως από προμηθευτές υψηλού κινδύνου, καθώς αυτές αυξάνουν την έκθεση στις συνέπειες πιθανών διαταραχών. ΑΝΑΓΝΩΡΙΖΕΙ ότι η αποφυγή του εγκλωβισμού σε συγκεκριμένο πάροχο και η διαφοροποίηση των προμηθευτών ΤΠΕ συνιστούν σημαντική παράμετρο για τη διασφάλιση της σταθερότητας και της ασφάλειας της εσωτερικής αγοράς. ΤΟΝΙΖΕΙ την ανάγκη προώθησης και υλοποίησης κατάλληλων στρατηγικών που θα διευκολύνουν τη διαφοροποίηση των παρόχων και την ανταγωνιστικότητα με τεχνολογικά ουδέτερο τρόπο. Επιπλέον, ΠΑΡΟΤΡΥΝΕΙ να ενσωματωθούν στη νομοθεσία της ΕΕ πτυχές σχετικές με την πρόληψη του εγκλωβισμού σε συγκεκριμένο πάροχο. Στο πλαίσιο αυτό, ΕΠΙΔΟΚΙΜΑΖΕΙ την πρόταση κανονισμού για εναρμονισμένους κανόνες σχετικά με τη δίκαιη πρόσβαση σε δεδομένα και τη δίκαιη χρήση τους (πράξη για τα δεδομένα), που αποσκοπεί στη βελτίωση της διαλειτουργικότητας των υπηρεσιών επεξεργασίας δεδομένων και την άρση των εμποδίων στην αλλαγή παρόχων υπηρεσιών επεξεργασίας δεδομένων.

9. ΑΝΑΓΝΩΡΙΖΕΙ ότι η ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ συνδέεται με τις δημόσιες συμβάσεις. ΤΟΝΙΖΕΙ την ανάγκη οι διαδικασίες σύναψης δημόσιων συμβάσεων να λαμβάνουν προσηκόντως υπόψη τη σημασία της ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ, επιβάλλοντας, κατά περίπτωση, αντικειμενικά και βάσει κινδύνου κριτήρια επιλογής σε ό,τι αφορά την ικανότητα των προσφερόντων να διασφαλίζουν υψηλό επίπεδο ασφάλειας των παρεχόμενων υπηρεσιών. ΖΗΤΕΙ την εξεύρεση της σωστής ισορροπίας μεταξύ, αφενός, δημόσιου συμφέροντος σε σχέση με όσο το δυνατόν πιο αποτελεσματική και θεμιτή χρήση των δημόσιων πόρων και, αφετέρου, δημόσιου συμφέροντος σε σχέση με τη διασφάλιση των συστημάτων πληροφοριών και τη διασφάλιση της ομαλής λειτουργίας της ενιαίας αγοράς. Για να διευκολυνθεί η εφαρμογή των σχετικών κανόνων περί δημοσίων συμβάσεων υπό το πρίσμα της αύξησης της κυβερνοασφάλειας, ΚΑΛΕΙ την Επιτροπή να αναπτύξει μεθοδολογικές κατευθυντήριες γραμμές έως το τρίτο τρίμηνο του 2023, προκειμένου να παροτρύνει τις αναθέτουσες αρχές να δίνουν τη δέουσα έμφαση στις πρακτικές κυβερνοασφάλειας των προσφερόντων και των υπεργολάβων τους και, εάν απαιτείται, να αξιολογεί και να διατυπώνει προτάσεις για την αναθεώρηση ή τη συμπλήρωση της περί δημοσίων συμβάσεων νομοθεσίας.

10. ΑΝΑΓΝΩΡΙΖΕΙ ότι οι άμεσες ξένες επενδύσεις που σχετίζονται με προϊόντα και υπηρεσίες ΤΠΕ παρέχουν μεν οικονομικά και κοινωνικά οφέλη στα κράτη μέλη, τις επιχειρήσεις και τους πολίτες, όμως ενδέχεται να περικλείουν κινδύνους για την ασφάλεια και τη δημόσια τάξη και ΣΗΜΕΙΩΝΕΙ ότι ο μηχανισμός ελέγχου των άμεσων ξένων επενδύσεων της ΕΕ, παράλληλα με τα οικεία εθνικά συστήματα ελέγχου, τα οποία παρέχουν μέσα για την αντιμετώπιση των εν λόγω κινδύνων, θα μπορούσε επίσης να εφαρμοστεί ως χρήσιμο εργαλείο για τη διαφύλαξη της ασφάλειας και της ανθεκτικότητας της αλυσίδας εφοδιασμού ΤΠΕ, συμβάλλοντας στην εξάλειψη των επενδύσεων υψηλού κινδύνου που θα μπορούσαν να επηρεάσουν αυτή την ασφάλεια και ανθεκτικότητα. ΑΝΑΓΝΩΡΙΖΕΙ ότι οι πληροφορίες που ανταλλάσσονται και διαμοιράζονται μέσω αυτού του μηχανισμού μπορούν να βοηθήσουν τα κράτη μέλη να αξιολογούν καλύτερα τις πιθανές απειλές για την ασφάλεια των αλυσίδων εφοδιασμού ΤΠΕ και να λαμβάνουν αναλόγως τα αναγκαία μέτρα. ΚΑΛΕΙ τους αρμόδιους εθνικούς φορείς να λαμβάνουν επίσης υπόψη αυτή τη διάσταση του μηχανισμού ελέγχου, όποτε συντρέχει περίπτωση.

11. Όσον αφορά την άμυνα, ΕΠΑΝΑΛΑΜΒΑΝΕΙ την πρόσκλησή του προς την Επιτροπή να αξιολογήσει το 2023, από κοινού με τα κράτη μέλη, τους κινδύνους για τις αλυσίδες εφοδιασμού υποδομών ζωτικής σημασίας σε διάφορους τομείς, συμπεριλαμβανομένου του ψηφιακού τομέα, που σχετίζονται με τα συμφέροντα ασφάλειας και άμυνας της ΕΕ, καθώς και να διερευνήσει επιλογές για την αύξηση της κυβερνοασφάλειας σε ολόκληρη την αλυσίδα εφοδιασμού της αμυντικής τεχνολογικής και βιομηχανικής βάσης της ΕΕ. Επιπλέον, ΚΑΛΕΙ τα κράτη μέλη και την Επιτροπή να μελετήσουν την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ κατά την υλοποίηση των δεσμεύσεων και των δράσεων της Στρατηγικής Πυξίδας.

12. Αναγνωρίζοντας τη σημασία των κρίσιμων πρώτων υλών, καθώς και όλων των ειδών ημιαγωγών ως βασικών δομικών στοιχείων για τα προϊόντα ΤΠΕ, ΕΝΘΑΡΡΥΝΕΙ τη διεξαγωγή εποικοδομητικών διαπραγματεύσεων της πρότασης κανονισμού για τη θέσπιση πλαισίου μέτρων για την ενίσχυση του οικοσυστήματος ημιαγωγών της Ευρώπης (πράξη για τα μικροκυκλώματα) και της πρότασης κανονισμού του Συμβουλίου για την τροποποίηση του κανονισμού (ΕΕ) 2021/2085 σχετικά με τη σύσταση των κοινών επιχειρήσεων στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη», όσον αφορά την κοινή επιχείρηση «Μικροκυκλώματα».

ΜΕΣΑ ΓΙΑ ΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

13. Ειδικότερα σε ό,τι αφορά τις τηλεπικοινωνιακές υποδομές, ΑΝΑΓΝΩΡΙΖΕΙ τα επιτεύγματα σε επίπεδο Ένωσης προκειμένου να βελτιωθεί η ασφάλεια της αλυσίδας εφοδιασμού των δικτύων 5G, ιδίως μέσω της εργαλειοθήκης της ΕΕ για την ασφάλεια του 5G (εργαλειοθήκη 5G της ΕΕ). ΚΑΛΕΙ τα κράτη μέλη να ανταλλάξουν περαιτέρω πληροφορίες περί βέλτιστων πρακτικών και μεθοδολογιών σχετικά με την εφαρμογή μέτρων που συνιστώνται στην εργαλειοθήκη 5G της ΕΕ και, ιδίως, να εφαρμόσουν τους σχετικούς περιορισμούς όσον αφορά τους προμηθευτές υψηλού κινδύνου για βασικά στοιχεία που ορίζονται ως ουσιώδη και ευαίσθητα στη συντονισμένη εκτίμηση κινδύνου της ΕΕ. ΕΠΙΣΗΜΑΙΝΕΙ ότι η εργαλειοθήκη 5G της ΕΕ αποτελεί ένα ευέλικτο μέσο βάσει κινδύνου για την αντιμετώπιση εντοπισμένων προκλήσεων στον τομέα της ασφάλειας, το οποίο επιτρέπει τον έγκαιρο και αποτελεσματικό χειρισμό πτυχών κυβερνοασφάλειας 5G, με παράλληλο σεβασμό των αρμοδιοτήτων των κρατών μελών, και ΑΝΑΓΝΩΡΙΖΕΙ ότι αποτελεί πολύτιμο μέσο για να ενισχυθεί περαιτέρω, με απόλυτη διαφάνεια, η ασφάλεια της αλυσίδας εφοδιασμού των τηλεπικοινωνιακών δικτύων με συντονισμένο τρόπο που θα μπορούσε να χρησιμεύσει ως πηγή έμπνευσης για εργαλεία εκτίμησης και μετριασμού των κινδύνων σχετιζόμενα με άλλους ζωτικούς τομείς. ΥΠΕΝΘΥΜΙΖΕΙ την πρόσκληση προς τις των αρμόδιες αρχές να διατυπώσουν συστάσεις, βάσει εκτιμήσεων κινδύνου, προς τα κράτη μέλη και την Επιτροπή, προκειμένου να ενισχυθεί η ανθεκτικότητα των δικτύων και των υποδομών επικοινωνιών εντός της Ευρωπαϊκής Ένωσης, συμπεριλαμβανομένης της συνεχιζόμενης υλοποίησης της εργαλειοθήκης 5G της ΕΕ.

14. ΣΗΜΕΙΩΝΕΙ τη σημασία που έχουν οι διαλειτουργικές προσεγγίσεις για την αντιμετώπιση του φαινομένου του εγκλωβισμού σε συγκεκριμένο πάροχο και την άμβλυνση του κινδύνου συγκέντρωσης, ενώ παράλληλα βελτιώνουν την ασφάλεια της αλυσίδας εφοδιασμού σε όλο το φάσμα των υποδομών και των υπηρεσιών ΤΠΕ. Ιδίως όσον αφορά τα δίκτυα 5G, ΑΝΑΓΝΩΡΙΖΕΙ τα δυνητικά οφέλη της έννοιας Open RAN εν προκειμένω, ενώ ταυτόχρονα ΥΠΕΝΘΥΜΙΖΕΙ την έκθεση σχετικά με την κυβερνοασφάλεια του ανοικτού δικτύου ραδιοπρόσβασης Open RAN που δημοσίευσε η ομάδα συνεργασίας για την ασφάλεια δικτύων και πληροφοριών, επισημαίνοντας ότι η έννοια αυτή βρίσκεται ακόμη υπό ανάπτυξη και ότι η ασφάλεια, η διαφάνεια και η τυποποίησή της είναι σε πρώιμο στάδιο ωρίμανσης, ΤΟΝΙΖΕΙ δε τη σημασία που έχει η εκτίμηση των κινδύνων πριν από οιαδήποτε μετάβαση προς νέα πρότυπα ή αρχιτεκτονικές.

15. ΕΠΙΣΗΜΑΙΝΕΙ τη σημασία των υφιστάμενων και των προσεχών οριζόντιων νομοθετικών πράξεων για την κυβερνοασφάλεια, ιδίως του κανονισμού σχετικά με τον ENISA (Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια) και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών (πράξη για την κυβερνοασφάλεια), της προσεχούς οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (NIS2), της πρότασης κανονισμού για τον καθορισμό μέτρων για υψηλό κοινό επίπεδο κυβερνοασφάλειας στα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και της πρότασης κανονισμού για τις οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία (πράξη για την κυβερνοανθεκτικότητα), για την αύξηση της ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ. Επιπροσθέτως, ΣΗΜΕΙΩΝΕΙ τις σημαντικές εξελίξεις στους τομεακούς κανονισμούς κυβερνοασφάλειας, ιδίως στον μελλοντικό κανονισμό σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα (DORA), ο οποίος περιλαμβάνει πλαίσιο εποπτείας για τους τρίτους παρόχους υπηρεσιών ΤΠΕ που έχουν κρίσιμη σημασία για τις χρηματοπιστωτικές οντότητες. Οι κανονισμοί αυτοί προβλέπουν γενικές υποχρεώσεις που σχετίζονται με την ασφάλεια της αλυσίδας εφοδιασμού, καθώς και λεπτομερείς και ειδικές απαιτήσεις που αφορούν τον συγκεκριμένο τομέα. Ταυτόχρονα, ΤΟΝΙΖΕΙ ότι οι προμηθευτές συχνά προμηθεύουν τα προϊόντα και τις υπηρεσίες τους σε πολλαπλούς τομείς και όχι σε έναν μόνο κλάδο. Ως εκ τούτου, είναι εξαιρετικά σημαντικό να διασφαλιστεί ότι οι απαιτήσεις ασφάλειας της αλυσίδας εφοδιασμού ευθυγραμμίζονται κατά το δυνατόν σε όλους τους σχετικούς τομείς, ιδίως στους καλυπτόμενους από τη μελλοντική οδηγία NIS2, προκειμένου να αποφευχθούν αποκλίσεις μεταξύ των υποχρεώσεων που επιβάλλονται στους προμηθευτές, καθώς και να μειωθεί η επιβάρυνση για τους φορείς εκμετάλλευσης κρίσιμων τομέων όσον αφορά την αξιολόγηση της συμμόρφωσης των προμηθευτών προς τις εν λόγω υποχρεώσεις, λαμβάνοντας παράλληλα υπόψη τα ιδιαίτερα χαρακτηριστικά κάθε τομέα.

16. ΕΠΙΚΡΟΤΕΙ την πρόταση πράξης για την κυβερνοανθεκτικότητα ως σημαντικό νομοθετικό μέσο που θα προωθεί την ασφαλή ανάπτυξη προϊόντων με ψηφιακά στοιχεία και θα διασφαλίζει ότι συνεκτιμάται η κυβερνοασφάλεια σε ολόκληρο τον κύκλο ζωής των προϊόντων με ψηφιακά στοιχεία. ΣΗΜΕΙΩΝΕΙ ότι η πρόταση πράξης για την κυβερνοανθεκτικότητα έχει δυνατότητα να συμβάλει σημαντικά στην ενίσχυση της ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ. ΕΝΘΑΡΡΥΝΕΙ τη διεξαγωγή εποικοδομητικών διαπραγματεύσεων και την έγκαιρη έγκριση της πράξης.

17. Εν προκειμένω, ΑΝΑΓΝΩΡΙΖΕΙ το συνεχιζόμενο έργο του ENISA, από κοινού με τα κράτη μέλη και άλλα ενδιαφερόμενα μέρη, που σκοπό έχει να καταστήσει διαθέσιμα στην ΕΕ συστήματα πιστοποίησης για προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ, σύμφωνα με την πράξη για την κυβερνοασφάλεια, που θα πρέπει να συμβάλλουν στην αύξηση του συνολικού επιπέδου κυβερνοασφάλειας εντός της ψηφιακής ενιαίας αγοράς. ΠΑΡΟΤΡΥΝΕΙ όλα τα ενδιαφερόμενα μέρη να συμμετάσχουν στις προπαρασκευαστικές εργασίες για τα επιμέρους ευρωπαϊκά συστήματα πιστοποίησης, προκειμένου να οικοδομηθεί εμπιστοσύνη προς τα ασφαλή προϊόντα, διαδικασίες και υπηρεσίες ΤΠΕ και να ενισχυθεί η ανθεκτικότητά τους και ΚΑΛΕΙ την Επιτροπή να εκπονήσει εν τάχει εκτελεστικές πράξεις σχετικά με τα ευρωπαϊκά συστήματα πιστοποίησης μετά την ολοκλήρωση των προπαρασκευαστικών εργασιών, ιδίως το ευρωπαϊκό σύστημα πιστοποίησης της κυβερνοασφάλειας (EUCC) βάσει κοινών κριτηρίων. ΣΗΜΕΙΩΝΕΙ ότι τα ευρωπαϊκά συστήματα πιστοποίησης θα πρέπει να περιλαμβάνουν, όπου χρειάζεται, απαιτήσεις σχετικά με την ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχέσεων με τους προμηθευτές.

18. ΕΠΙΣΗΜΑΙΝΕΙ την ανάγκη για ενδελεχή εφαρμογή όλων των προσεχών διατάξεων NIS2 που σχετίζονται με την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ. Στο πλαίσιο αυτό, ΥΠΟΓΡΑΜΜΙΖΕΙ τη σημασία των ενωσιακών συντονισμένων εκτιμήσεων κινδύνου των κρίσιμων αλυσίδων εφοδιασμού (συντονισμένες εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού), των εθνικών πολιτικών για την ασφάλεια της αλυσίδας εφοδιασμού και των μέτρων ασφαλείας που σχετίζονται με την αλυσίδα εφοδιασμού. ΣΗΜΕΙΩΝΕΙ ότι θα πρέπει να δοθεί προσοχή όχι μόνο στους κύριους προμηθευτές αλλά και στους σχετιζόμενους υπεργολάβους όσον αφορά τους κινδύνους προς την ασφάλεια του κύριου προμηθευτή ή του τελικού πελάτη. Προκειμένου να διευκολυνθεί η εφαρμογή των μέτρων διαχείρισης κινδύνων της αλυσίδας εφοδιασμού, ΠΑΡΟΤΡΥΝΕΙ τον ENISA να προβεί, με τη βοήθεια της ομάδας συνεργασίας NIS, σε απολογισμό των βέλτιστων πρακτικών που είναι διαθέσιμες για τη διαχείριση κινδύνων της αλυσίδας εφοδιασμού και να τις συντάξει σε μεθοδολογικές κατευθυντήριες γραμμές. Επιπλέον, ΠΑΡΟΤΡΥΝΕΙ τον ENISA να παρακολουθεί τις επενδύσεις στην ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ των οντοτήτων που θα ρυθμίζονται από την προσεχή οδηγία NIS2.

19. ΕΠΙΣΗΜΑΙΝΕΙ επίσης τα οφέλη και τους κινδύνους που ενέχει η χρήση των παρόχων διαχειριζόμενων υπηρεσιών (MSP) και των παρόχων διαχειριζόμενων υπηρεσιών ασφαλείας (MSSP) στο πλαίσιο της ασφάλειας της αλυσίδας εφοδιασμού. Ενώ η χρήση των εν λόγω παρόχων μπορεί να βελτιώσει σημαντικά την ασφάλεια των οργανισμών και να επιφέρει υψηλότερα επίπεδα κυβερνοασφάλειας, η εξ αποστάσεως διαχείριση των συστημάτων και των υπηρεσιών ΤΠΕ σε συνδυασμό με την προνομιακή πρόσβαση στο περιβάλλον ΤΠΕ των πελατών, το οποίο ενδέχεται να χρειάζονται οι MSP και οι MSSP, μπορεί, σε περίπτωση εκτεθειμένων MSP ή MSSP, να οδηγήσει σε αλυσιδωτές επιπτώσεις με σοβαρό αντίκτυπο σε μεγάλο αριθμό πελατών. Ως εκ τούτου είναι εξαιρετικά σημαντικό οι MSP και οι MSSP να διατηρούν την εσωτερική τους ασφάλεια και την ασφάλεια των υπηρεσιών που παρέχουν σε υψηλό επίπεδο και να υιοθετούν διαφανή προσέγγιση έναντι των πελατών τους όσον αφορά την ασφάλεια των υπηρεσιών που παρέχουν. Στο πλαίσιο αυτό ΕΠΙΔΟΚΙΜΑΖΕΙ τη μελλοντική προσθήκη τους στο πεδίο εφαρμογής της προσεχούς οδηγίας NIS2.

20. Όσον αφορά την εφαρμογή του μηχανισμού για συντονισμένες εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού σύμφωνα με την προσεχή οδηγία NIS2, ΣΗΜΕΙΩΝΕΙ τη σημασία των μη τεχνικών παραγόντων κινδύνου εν προκειμένω, όπως η αθέμιτη επιρροή τρίτου κράτους επί προμηθευτών και παρόχων υπηρεσιών και, στο πλαίσιο αυτό, ΑΝΑΓΝΩΡΙΖΕΙ τους παράγοντες που μπορούν να χρησιμοποιηθούν για την αξιολόγηση του προφίλ κινδύνου, όπως αναφέρεται στην ενωσιακή συντονισμένη εκτίμηση κινδύνου της κυβερνοασφάλειας των δικτύων 5G. ΚΑΛΕΙ την Επιτροπή να προσδιορίσει έως το δεύτερο τρίμηνο του 2023, κατόπιν διαβούλευσης με την ομάδα συνεργασίας NIS και τον ENISA, τις συγκεκριμένες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ που θα μπορούσαν να αποτελέσουν κατά προτεραιότητα αντικείμενο των συντονισμένων εκτιμήσεων κινδύνου της αλυσίδας εφοδιασμού.

21. ΣΗΜΕΙΩΝΕΙ ότι οι εξαρτήσεις από προμηθευτές προϊόντων και υπηρεσιών ΤΠΕ υψηλού κινδύνου που χρησιμοποιούνται για τη λειτουργία κρίσιμων δικτύων και συστημάτων συνιστούν στρατηγική απειλή που πρέπει να μετριαστεί μέσω κατάλληλων πολιτικών τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο και μέσω της συνεργασίας μεταξύ των κρατών μελών και με ομόφρονες διεθνείς εταίρους. Προκειμένου να διευκολυνθεί ο μετριασμός αυτού του στρατηγικού κινδύνου και να υποστηριχθούν οι συντονισμένες εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού, ΚΑΛΕΙ την ομάδα συνεργασίας NIS, σε συνεργασία με την Επιτροπή και τον ENISA, να αναπτύξει μια εργαλειοθήκη μέτρων για μείωση των κρίσιμων κινδύνων της αλυσίδας εφοδιασμού ΤΠΕ (εργαλειοθήκη για την αλυσίδα εφοδιασμού ΤΠΕ).
Η εργαλειοθήκη για την αλυσίδα εφοδιασμού ΤΠΕ θα πρέπει να βασίζεται σε σενάρια στρατηγικών απειλών που έχουν προσδιοριστεί για τις αλυσίδες εφοδιασμού ΤΠΕ και να προβλέπει μέτρα για την ανταπόκριση σε αυτά τα σενάρια, αξιοποιώντας αφενός τις εμπειρίες από την εργαλειοθήκη 5G και αφετέρου όσες αποκτήθηκαν σε εθνικό επίπεδο. Θα πρέπει να συμπληρώνει με διαφάνεια τις συντονισμένες εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού για συγκεκριμένες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ στο πλαίσιο της προσεχούς οδηγίας NIS2, προσφέροντας γενικά μέτρα για τη μείωση των κινδύνων που μπορούν να προσαρμοστούν κλιμακωτά για συγκεκριμένες υπηρεσίες, συστήματα ή προϊόντα ΤΠΕ, με βάση τους κινδύνους που εντοπίζονται στις επιμέρους συντονισμένες εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού.

22. ΤΟΝΙΖΕΙ τον σημαντικό ρόλο των δραστηριοτήτων έρευνας, καινοτομίας και επενδύσεων και των επιχειρηματικών δραστηριοτήτων στον ψηφιακό τομέα και στον τομέα της κυβερνοασφάλειας, καθώς και της χρηματοδότησης των εν λόγω δραστηριοτήτων, όσον αφορά την αποφυγή δυνητικών μελλοντικών ανεπιθύμητων στρατηγικών εξαρτήσεων και την ενίσχυση της συνολικής ανθεκτικότητας των αλυσίδων εφοδιασμού ΤΠΕ. Στο πλαίσιο αυτό ΤΟΝΙΖΕΙ τον ρόλο και τη συνάφεια τόσο των στρατηγικών όσο και των εκτελεστικών καθηκόντων του Ευρωπαϊκού Κέντρου Αρμοδιότητας για Βιομηχανικά, Τεχνολογικά και Ερευνητικά Θέματα Κυβερνοασφάλειας (ECCC) και του δικτύου εθνικών κέντρων συντονισμού για τη συμβολή στη μεγιστοποίηση των αποτελεσμάτων των επενδύσεων ώστε να ενισχυθούν ο ηγετικός ρόλος και η ανοικτή στρατηγική αυτονομία της Ένωσης στον τομέα της κυβερνοασφάλειας, να στηριχθούν οι τεχνολογικές ικανότητες και δεξιότητες της Ένωσης και να αυξηθεί η παγκόσμια ανταγωνιστικότητα της Ένωσης. Στο πλαίσιο αυτό ΖΗΤΕΙ την εν τάχει θέση σε λειτουργία του ECCC. ΚΑΛΕΙ το ECCC να λάβει υπόψη τις πτυχές της ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ, συμπεριλαμβανομένης λ.χ. της ανάπτυξης ασφαλούς λογισμικού, στο στρατηγικό του θεματολόγιο, διασφαλίζοντας παράλληλα τη συνοχή και τη συμπληρωματικότητα και αποφεύγοντας ενδεχόμενη αλληλεπικάλυψη προσπαθειών. ΥΠΟΣΤΗΡΙΖΕΙ την ενίσχυση της ευρωπαϊκής ανταγωνιστικότητας στον τομέα της κυβερνοασφάλειας μέσω χρηματοδοτικών προγραμμάτων, όπως το πρόγραμμα Ορίζων Ευρώπη για την έρευνα και την καινοτομία, καθώς και το πρόγραμμα Ψηφιακή Ευρώπη για την ενίσχυση, την οικοδόμηση και την απόκτηση βασικών ικανοτήτων στην ψηφιακή οικονομία, την κοινωνία και τη δημοκρατία της ΕΕ.

ΥΠΟΣΤΗΡΙΚΤΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ

23. ΕΝΘΑΡΡΥΝΕΙ την ενίσχυση των κινήτρων χρηματοδοτικής στήριξης σχετικά με μέτρα που αποσκοπούν στην ενίσχυση της ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ. ΚΑΛΕΙ, ως προτεραιότητα και ενόψει της προσεχούς εφαρμογής της οδηγίας NIS2, το ECCC, την Επιτροπή και τα σχετικά ενδιαφερόμενα μέρη να διερευνήσουν δυνατότητες για τη συμπερίληψη πτυχών ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ στις προσεχείς προσκλήσεις υποβολής προτάσεων στο πλαίσιο των προγραμμάτων εργασίας για την κυβερνοασφάλεια του προγράμματος Ψηφιακή Ευρώπη και του προγράμματος Ορίζων Ευρώπη, ή οποιωνδήποτε άλλων συναφών ευκαιριών χρηματοδότησης. Οι εν λόγω ευκαιρίες χρηματοδότησης θα πρέπει, μεταξύ άλλων, να έχουν ως στόχο να επιτρέψουν στους οργανισμούς να στηρίζουν τη διατήρηση υψηλού επιπέδου κυβερνοασφάλειας όσον αφορά την προμήθεια προϊόντων και υπηρεσιών ΤΠΕ σε ολόκληρη την αλυσίδα εφοδιασμού, ιδίως σε σχέση με την αντικατάσταση συγκεκριμένων κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ που αναγνωρίζονται ως υψηλού κινδύνου σύμφωνα με τις μελλοντικές συντονισμένες εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού.

24. ΑΝΑΓΝΩΡΙΖΕΙ ότι η παγκοσμιοποίηση και η εξειδίκευση των υπηρεσιών ΤΠΕ καθώς και η αυξημένη εξάρτηση από προϊόντα και υπηρεσίες τρίτων μερών συνεπάγεται την ανάγκη στενής συνεργασίας εντός της ΕΕ και διεθνώς για την ανταλλαγή γνώσεων και εμπειρογνωσίας μεταξύ των σχετικών ενδιαφερόμενων μερών και τα ΠΑΡΟΤΡΥΝΕΙ να βρουν ισχυρή και συντονισμένη θέση που θα διασφαλίζει ολοκληρωμένα την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ. ΑΝΑΓΝΩΡΙΖΕΙ επίσης την ανάγκη για περαιτέρω διερεύνηση συναφών προηγμένων προσεγγίσεων και τεχνικών, τόσο για την κατάλληλη βασική κυβερνοϋγιεινή όσο και για μακροπρόθεσμες λύσεις προς την επίτευξη ασφαλών και ανθεκτικών αλυσίδων εφοδιασμού ΤΠΕ, καθώς και των καταλληλότερων τρόπων προώθησης και δυνητικής ενσωμάτωσής τους σε πολιτικές ή άλλες πρωτοβουλίες. ΑΝΑΓΝΩΡΙΖΕΙ εν προκειμένω ότι θα πρέπει να δοθεί ιδιαίτερη προσοχή στη διερεύνηση των οφελών και των μειονεκτημάτων των συστηματικών λύσεων, όπως είναι οι αρχές μηδενικής εμπιστοσύνης, οι κατάλογοι υλικών λογισμικού και παρόμοιες μακροπρόθεσμες λύσεις. ΣΥΝΙΣΤΑ τη χρήση της ομάδας συνεργασίας NIS προς τον σκοπό αυτόν.

25. ΣΗΜΕΙΩΝΕΙ τα οφέλη από την παρακολούθηση και την αποτελεσματική ανταλλαγή πληροφοριών σχετικά με περιστατικά και απειλές στον κυβερνοχώρο για την πρόληψη, τον εντοπισμό και τον μετριασμό των επιπτώσεων των επιθέσεων στην αλυσίδα εφοδιασμού. ΤΟΝΙΖΕΙ την ανάγκη να συνεχιστεί η οικοδόμηση αξιοπιστίας και εμπιστοσύνης μεταξύ των κρατών μελών για αποτελεσματική ανταλλαγή των εν λόγω πληροφοριών. ΣΗΜΕΙΩΝΕΙ εν προκειμένω την πρόταση της Επιτροπής να στηριχθούν τα κράτη μέλη στη δημιουργία και την ενίσχυση κέντρων επιχειρήσεων ασφάλειας (ΚΕΑ) ώστε να συγκροτηθεί ένα δίκτυο ΚΕΑ σε ολόκληρη την ΕΕ, για την περαιτέρω παρακολούθηση και πρόβλεψη των σημάτων επιθέσεων σε δίκτυα. ΥΠΕΝΘΥΜΙΖΕΙ την ανάγκη συμπληρωματικότητας και συντονισμού στο πλαίσιο των υφιστάμενων δικτύων και μηχανισμών, ιδίως δε ΕΠΙΣΗΜΑΙΝΕΙ εν προκειμένω τον ρόλο του δικτύου CSIRT, καθώς και την ανάγκη περαιτέρω διερεύνησης των δυνατοτήτων των δικτύων αυτών για την προώθηση μιας αποτελεσματικής, ασφαλούς και αξιόπιστης νοοτροπίας ανταλλαγής πληροφοριών. ΥΠΕΝΘΥΜΙΖΕΙ τις προσπάθειες που καταβάλλουν τα κράτη μέλη, με την υποστήριξη της ΕΕ, για τη δημιουργία τομεακών, εθνικών και περιφερειακών CSIRT και εθνικών ή ευρωπαϊκών κέντρων κοινοχρησίας και ανάλυσης πληροφοριών (ISAC) στο πλαίσιο ενός αποτελεσματικού δικτύου εταιρικών σχέσεων για την κυβερνοασφάλεια στην Ένωση.

26. Λόγω του διασυνδεδεμένου και παγκόσμιου χαρακτήρα των απειλών της αλυσίδας εφοδιασμού ΤΠΕ, ΤΟΝΙΖΕΙ τη σημασία της προσέγγισης και της ενίσχυσης της ασφάλειας της αλυσίδας εφοδιασμού ΤΠΕ σε παγκόσμιο επίπεδο. Στο πλαίσιο αυτό, ΣΥΝΙΣΤΑ τη χρήση ψηφιακών εταιρικών σχέσεων, κυβερνοδιαλόγων και άλλων συναφών πρωτοβουλιών της ΕΕ, συμπεριλαμβανομένων, κατά περίπτωση, συμφωνιών ελεύθερων συναλλαγών, για την προώθηση αξιολογήσεων βάσει κινδύνου των προμηθευτών προϊόντων ΤΠΕ και των παρόχων υπηρεσιών ΤΠΕ, τη χρήση αξιόπιστων προμηθευτών και τη λειτουργία ενός ασφαλούς και καινοτόμου ψηφιακού οικοσυστήματος που θα βασίζεται σε ανοικτά, διαλειτουργικά και διαφανή πρότυπα. Επιπλέον, ΕΠΑΝΑΛΑΜΒΑΝΕΙ το όραμα των εταιρικών σχέσεων της Global Gateway, καθώς και του Συμβουλίου Εμπορίου και Τεχνολογίας ΕΕ-ΗΠΑ, και των δραστηριοτήτων στο πλαίσιο των ομάδων εργασίας του, για την προαγωγή της χρήσης αξιόπιστων/μη υψηλού κινδύνου προμηθευτών και για την ανάπτυξη ενός μηχανισμού χρηματοδότησης για τη διευκόλυνση έργων που καθιστούν τις υποδομές και τις υπηρεσίες ΤΠΕ σε τρίτες χώρες πιο ασφαλείς, ανθεκτικές και αξιόπιστες, μεταξύ άλλων αποφεύγοντας τη χρηματοδότηση αγορών από αναξιόπιστους/υψηλού κινδύνου προμηθευτές με τρόπο τεχνολογικά ουδέτερο.

27. ΕΠΙΒΕΒΑΙΩΝΕΙ τη δέσμευσή του να προωθήσει με τη συμβολή του και να προαγάγει έναν ανοικτό, ελεύθερο, παγκόσμιο, σταθερό και ασφαλή κυβερνοχώρο και να τηρήσει τα πρότυπα, τους κανόνες και τις αρχές της υπεύθυνης κρατικής συμπεριφοράς στον κυβερνοχώρο που έχουν ορισθεί στο πλαίσιο των Ηνωμένων Εθνών. Όσον αφορά ειδικότερα την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ, ΥΠΕΝΘΥΜΙΖΕΙ το πρότυπο που εγκρίθηκε από την Ομάδα κυβερνητικών εμπειρογνωμόνων (GGE) των Ηνωμένων Εθνών και την ομάδα ανοιχτής σύνθεσης (OEWG) με παρότρυνση προς τα κράτη να λάβουν εύλογα μέτρα για τη διασφάλιση της ακεραιότητας της αλυσίδας εφοδιασμού, μεταξύ άλλων μέσω της ανάπτυξης αντικειμενικών μέτρων συνεργασίας, ώστε οι τελικοί χρήστες να μπορούν να έχουν εμπιστοσύνη στην ασφάλεια των προϊόντων ΤΠΕ, και να επιδιώκουν την πρόληψη της διάδοσης κακόβουλων εργαλείων και τεχνικών ΤΠΕ και της χρήσης επιβλαβών κρυφών λειτουργιών, και ΤΑΣΣΕΤΑΙ ΥΠΕΡ της ευρείας εφαρμογής του.