P7_TA(2012)0237

Προστασία υποδομών πληροφοριών ζωτικής σημασίας: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 12ης Ιουνίου 2012 σχετικά με την προστασία υποδομών πληροφοριών ζωτικής σημασίας – επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο (2011/2284(INI))

Το Ευρωπαϊκό Κοινοβούλιο,

– έχοντας υπόψη το ψήφισμά του της 5ης Μαΐου 2010 με τίτλο «Ένα νέο Ψηφιακό θεματολόγιο για την Ευρώπη: 2015.eu»[1],

– έχοντας υπόψη το ψήφισμά του της 15ης Ιουνίου 2010 με τίτλο «Διοίκηση του διαδικτύου: τα επόμενα βήματα»[2],

– έχοντας υπόψη το ψήφισμά του της 6ης Ιουλίου 2011 με τίτλο «Ευρωπαϊκά δίκτυα ευρυζωνικότητας: επένδυση στην ψηφιακά τροφοδοτούμενη ανάπτυξη»[3],

– έχοντας υπόψη το άρθρο 48 του Κανονισμού του,

– έχοντας υπόψη την έκθεση της Επιτροπής Βιομηχανίας, Έρευνας και Ενέργειας και τη γνωμοδότηση της Επιτροπής Πολιτικών Ελευθεριών, Δικαιοσύνης και Εσωτερικών Υποθέσεων (A7-0167/2012),

Α. λαμβάνοντας υπόψη ότι οι τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) είναι ικανές να αναπτύξουν όλες τους τις δυνατότητες για να προαχθεί η οικονομία και η κοινωνία μόνο εάν οι χρήστες εμπιστεύονται και θεωρούν αξιόπιστη την ασφάλεια και την ανθεκτικότητά τους, και εάν η ισχύουσα νομοθεσία σε θέματα όπως το απόρρητο των δεδομένων και τα δικαιώματα διανοητικής ιδιοκτησίας εφαρμόζεται αποτελεσματικά στο περιβάλλον του Διαδικτύου,

Β. λαμβάνοντας υπόψη ότι ο αντίκτυπος του διαδικτύου και των τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) στις διάφορες πτυχές της ζωής των πολιτών κερδίζει έδαφος με ταχείς ρυθμούς, αποτελώντας καίρια κινητήρια δύναμη για την κοινωνική αλληλεπίδραση, την πολιτιστική αναβάθμιση και την οικονομική ανάπτυξη,

Γ. λαμβάνοντας υπόψη ότι η ασφάλεια των ΤΠΕ και του Διαδικτύου αποτελεί μια ολοκληρωμένη έννοια με παγκόσμια επίδραση στο οικονομικό, το κοινωνικό, το τεχνολογικό και το στρατιωτικό πεδίο, για την επίτευξη της οποίας απαιτείται ο σαφής καθορισμός και η διαφοροποίηση των ευθυνών καθώς και η σύσταση ενός ισχυρού μηχανισμού διεθνούς συνεργασίας,

Δ. λαμβάνοντας υπόψη ότι το πρωτοποριακό Ψηφιακό θεματολόγιο της ΕΕ στοχεύει στην

---

1 ΕΕ C 81 E της 15.3.2011, σ. 45.
2 ΕΕ C 236 E της 12.8.2011, σ. 33.
3 Κείμενα που εγκρίθηκαν, P7_TA(2011)0322.

ενίσχυση της ανταγωνιστικότητας της Ευρώπης, βάσει της προώθησης των ΤΠΕ και της δημιουργίας συνθηκών για υψηλή και υγιή ανάπτυξη και τεχνολογικές θέσεις εργασίας,

Ε. λαμβάνοντας υπόψη ότι ο ιδιωτικός τομέας παραμένει ο κύριος επενδυτής, ιδιοκτήτης και διαχειριστής προϊόντων, υπηρεσιών, εφαρμογών και υποδομών ασφάλειας των πληροφοριών, με επενδύσεις δισεκατομμυρίων ευρώ την τελευταία δεκαετία· λαμβάνοντας υπόψη ότι αυτή η συμμετοχή πρέπει να ενισχυθεί με στρατηγικές εφαρμογής των κατάλληλων πολιτικών για την προώθηση της ανθεκτικότητας των υποδομών που βρίσκονται στην κατοχή και υπό τη λειτουργία του ιδιωτικού ή του δημόσιου τομέα ή και των δύο,

ΣΤ. λαμβάνοντας υπόψη ότι η ανάπτυξη δικτύων, υπηρεσιών και τεχνολογιών ΤΠΕ υψηλού επιπέδου ασφάλειας και ανθεκτικότητας θα αυξήσει την ανταγωνιστικότητα της οικονομίας της ΕΕ, αφενός βελτιώνοντας την εκτίμηση και τη διαχείριση των κινδύνων στον κυβερνοχώρο και αφετέρου παρέχοντας στην οικονομία της ΕΕ πιο γερές υποδομές πληροφοριών για τη στήριξη της καινοτομίας και της ανάπτυξης, δημιουργώντας έτσι νέες ευκαιρίες ώστε οι επιχειρήσεις να καταστούν παραγωγικότερες,

Ζ. λαμβάνοντας υπόψη ότι τα δεδομένα όσον αφορά την επιβολή του νόμου σχετικά με εγκλήματα στον κυβερνοχώρο –που καλύπτουν κυβερνοεπιθέσεις, καθώς και άλλα είδη ηλεκτρονικού εγκλήματος– υποδηλώνουν έντονη αύξηση σε διάφορες ευρωπαϊκές χώρες· λαμβάνοντας, εντούτοις, υπόψη ότι τα αντιπροσωπευτικά στατιστικά δεδομένα σχετικά με κυβερνοεπιθέσεις, που παρέχονται από τους φορείς επιβολής του νόμου και από την CERT (ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική), παραμένουν περιορισμένα και ότι πρέπει να βελτιωθεί η συλλογή τους στο μέλλον, εξασφαλίζοντας ισχυρότερη απόκριση των φορέων επιβολής του νόμου στην επικράτεια της ΕΕ και καλύτερη νομοθετική αντίδραση σε διαρκώς εξελισσόμενες κυβερνοαπειλές,

Η. λαμβάνοντας υπόψη ότι ένα κατάλληλο επίπεδο ασφάλειας των πληροφοριών είναι σημαντικό για τη δυναμική επέκταση των υπηρεσιών που προσφέρονται μέσω του Διαδικτύου,

Θ. λαμβάνοντας υπόψη πρόσφατα περιστατικά στον κυβερνοχώρο, διαταραχές και επιθέσεις εναντίον των υποδομών πληροφοριών οργάνων της ΕΕ, της βιομηχανίας και κρατών μελών, που καταδεικνύουν την ανάγκη να θεσπιστεί ένα ισχυρό, καινοτόμο και αποτελεσματικό σύστημα για την προστασία των υποδομών ζωτικής σημασίας (ΠΥΖΣ), βασισμένο στην πλήρη διεθνή συνεργασία και σε πρότυπα ελάχιστης ανθεκτικότητας που θα ισχύουν στα κράτη μέλη,

Ι. λαμβάνοντας υπόψη ότι η ταχεία ανάπτυξη νέων λεωφόρων ΤΠΕ, όπως το υπολογιστικό νέφος (Cloud computing), απαιτούν αυστηρή εστίαση στη διαδικτυακή ασφάλεια, προκειμένου να είναι δυνατή η πλήρης αξιοποίηση των πλεονεκτημάτων των τεχνολογικών επιτευγμάτων,

ΙΑ. λαμβάνοντας υπόψη ότι το Ευρωπαϊκό Κοινοβούλιο έχει επανειλημμένα επιμείνει στην εφαρμογή υψηλών προτύπων για το απόρρητο και την προστασία των δεδομένων, την ουδετερότητα των δικτύων και τα δικαιώματα διανοητικής ιδιοκτησίας,

Μέτρα για την ενίσχυση της ΠΥΖΣ σε εθνικό επίπεδο και σε επίπεδο ΕΕ

1. χαιρετίζει την εφαρμογή από τα κράτη μέλη του Ευρωπαϊκού Προγράμματος ΠΥΖΣ,

συμπεριλαμβανομένης της δημιουργίας του δικτύου προειδοποίησης σχετικά με τις υποδομές ζωτικής σημασίας (ΔΠΥΖΣ)·

2. θεωρεί ότι οι προσπάθειες που καταβάλλονται για την ΠΥΖΣ όχι μόνο θα αυξήσουν το γενικό επίπεδο ασφάλειας των πολιτών αλλά θα βελτιώσουν επίσης την αντίληψή τους για την ασφάλεια καθώς και την εμπιστοσύνη τους στα μέτρα που θεσπίζουν τα κράτη για την προστασία τους·

3. λαμβάνει υπόψη ότι η Επιτροπή εξετάζει την αναθεώρηση της οδηγίας 2008/114/ΕΚ του Συμβουλίου[1] και απευθύνει έκκληση να παρασχεθούν αποδεικτικά στοιχεία για την αποτελεσματικότητα και τον αντίκτυπο της οδηγίας πριν από την ανάληψη περαιτέρω δράσης· ζητεί να εξετασθεί το ενδεχόμενο να διευρυνθεί το πεδίο εφαρμογής της και να καλύψει, ιδίως, τις ΤΠΕ και τις χρηματοπιστωτικές υπηρεσίες· ζητεί επίσης να τεθούν υπό εξέταση και τομείς όπως τα συστήματα υγείας, υδροδότησης και προμήθειας τροφίμων καθώς και η πυρηνική έρευνα και βιομηχανία (όπου δεν καλύπτονται από ειδικές ρυθμίσεις)· έχει την άποψη ότι αυτοί οι τομείς θα πρέπει επίσης να επωφεληθούν από τη διακλαδική προσέγγιση που έχει υιοθετηθεί από το ΔΠΥΖΣ (η οποία απαρτίζεται από συνεργασία, ένα σύστημα συναγερμού και ανταλλαγή βέλτιστων πρακτικών)·

4. τονίζει πόσο σημαντική είναι η καθιέρωση και η διασφάλιση μιας βιώσιμης ενοποίησης της ευρωπαϊκής έρευνας με σκοπό να διατηρηθεί και να ενισχυθεί η ευρωπαϊκή αριστεία στον τομέα της ΠΥΖΣ·

5. καλεί, λαμβάνοντας υπόψη τη διασυνδεμένη και εξαιρετικά αλληλεξαρτώμενη, ευαίσθητη, στρατηγική και ευάλωτη φύση της ΠΥΖΣ, σε εθνικό επίπεδο και επίπεδο ΕΕ, για την τακτική ενημέρωση των προτύπων ελάχιστης ανθεκτικότητας για ετοιμότητα και αντίδραση απέναντι σε διαταραχές, περιστατικά, απόπειρες καταστροφής ή επιθέσεις, όπως αυτές που είναι αποτέλεσμα ανεπαρκώς ασφαλών υποδομών ή τερματικών·

6. τονίζει τη σημασία των προτύπων και των πρωτοκόλλων στον τομέα της ασφάλειας των πληροφοριών και επικροτεί την εντολή που δόθηκε το 2011 στις επιτροπές CEN και Cenelec καθώς και στον οργανισμό ETSI να καθιερώσουν πρότυπα ασφαλείας·

7. αναμένει ότι οι κάτοχοι και διαχειριστές υποδομών πληροφοριών ζωτικής σημασίας πρέπει να επιτρέπουν και, εφόσον κρίνεται σκόπιμο, να βοηθούν τους χρήστες να χρησιμοποιούν τα κατάλληλα μέσα προστασίας από κακόβουλες επιθέσεις ή/και διαταραχές, μέσω ανθρώπινης και ηλεκτρονικής επίβλεψης, όπου απαιτείται·

8. στηρίζει τη συνεργασία μεταξύ των δημόσιων και ιδιωτικών ενδιαφερόμενων μερών σε επίπεδο Ένωσης και ενθαρρύνει τις προσπάθειές τους να αναπτύξουν και να εφαρμόσουν πρότυπα ασφάλειας και ανθεκτικότητας για εθνικές και ευρωπαϊκές πολιτικές υποδομές ζωτικής σημασίας, στο πλαίσιο του δημόσιου τομέα, του ιδιωτικού τομέα ή σε σύμπραξη δημόσιου και ιδιωτικού τομέα·

9. τονίζει τη σημασία των πανευρωπαϊκών ασκήσεων ετοιμότητας για περιπτώσεις μεγάλης κλίμακας συμβάντων ασφάλειας του δικτύου, και θεωρεί αναγκαίο τον καθορισμό ενιαίας δέσμης προτύπων για την αξιολόγηση απειλών·

10. καλεί την Επιτροπή, σε συνεργασία με τα κράτη μέλη, να αξιολογήσει την εφαρμογή του

---

[1] ΕΕ L 345 της 23.12.2008, σ. 75.

σχεδίου δράσης ΠΥΖΣ· προτρέπει τα κράτη μέλη να συγκροτήσουν εθνικές/κρατικές CERT που θα λειτουργούν καλά, να αναπτύξουν εθνικές στρατηγικές κυβερνοασφάλειας, να οργανώσουν τακτικές εθνικές και πανευρωπαϊκές ασκήσεις περιστατικών στον κυβερνοχώρο, να αναπτύξουν εθνικά σχέδια έκτακτης ανάγκης για περιστατικά στον κυβερνοχώρο και να συμβάλουν στην ανάπτυξη ενός ευρωπαϊκού σχεδίου έκτακτης ανάγκης για περιστατικά στον κυβερνοχώρο έως το τέλος του 2012·

11. συνιστά να τεθούν σε εφαρμογή σχέδια ασφάλειας λειτουργίας ή ισοδύναμα μέτρα σε όλες τις ευρωπαϊκές υποδομές πληροφοριών ζωτικής σημασίας και να διοριστούν σύνδεσμοι ασφαλείας·

12. χαιρετίζει την τρέχουσα αναθεώρηση της απόφασης 2005/222/ΔΕΥ[1] σχετικά με τις επιθέσεις κατά των πληροφορικών συστημάτων· σημειώνει την ανάγκη συντονισμού των προσπαθειών της ΕΕ για την αντιμετώπιση των κυβερνοεπιθέσεων μεγάλης κλίμακας, συμπεριλαμβάνοντας τον ENISA, τις CERT των κρατών μελών και τις αρμοδιότητες της μελλοντικής ευρωπαϊκής CERT.

13. θεωρεί ότι ο ENISA μπορεί να διαδραματίσει καίριο ρόλο σε ευρωπαϊκό επίπεδο όσον αφορά την προστασία των υποδομών πληροφοριών ζωτικής σημασίας, παρέχοντας τεχνική εμπειρογνωμοσύνη στα κράτη μέλη και στα θεσμικά όργανα και τους οργανισμούς της Ευρωπαϊκής Ένωσης, καθώς και εκθέσεις και αναλύσεις σχετικά με την ασφάλεια των συστημάτων πληροφοριών τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο·

Περαιτέρω δραστηριότητες της ΕΕ για ισχυρή ασφάλεια του Διαδικτύου

14. απευθύνει έκκληση στον ENISA να συντονίσει και να διεξάγει κάθε χρόνο στην ΕΕ Μήνες Ευαισθητοποίησης για την Ασφάλεια στο Διαδίκτυο, ούτως ώστε ζητήματα σχετικά με την ασφάλεια στον κυβερνοχώρο να έρθουν στο επίκεντρο της προσοχής των κρατών μελών και των πολιτών της ΕΕ·

15. στηρίζει τον ENISA, σύμφωνα με τους στόχους του Ψηφιακού θεματολογίου, στην εκτέλεση των καθηκόντων του όσον αφορά την ασφάλεια πληροφοριών δικτύου και, ιδίως, παρέχοντας καθοδήγηση και γνωμοδότηση στα κράτη μέλη σχετικά με την ικανοποίηση των βασικών ικανοτήτων για τις CERT τους, καθώς και τη στήριξη της ανταλλαγής βέλτιστων πρακτικών μέσω της ανάπτυξης ενός περιβάλλοντος εμπιστοσύνης· καλεί τον οργανισμό να ξεκινήσει διαδικασία διαβούλευσης με τα ενδιαφερόμενα μέρη προκειμένου να προσδιορίσει παρόμοια μέτρα κυβερνοασφάλειας για κατόχους και διαχειριστές ιδιωτικών δικτύων και υποδομών, καθώς και να στηρίξει την Επιτροπή και τα κράτη μέλη στις προσπάθειές τους να συμβάλλουν στην ανάπτυξη και τη ζήτηση σχεδίων πιστοποίησης ασφάλειας πληροφοριών, προτύπων συμπεριφοράς και πρακτικών συνεργασίας μεταξύ εθνικών και ευρωπαϊκών CERT και κατόχων και διαχειριστών υποδομών, εφόσον και όπου κρίνεται σκόπιμο, μέσω του ορισμού τεχνολογικά ουδέτερων κοινών ελάχιστων απαιτήσεων·

16. εκφράζει ικανοποίηση για την πρόταση αναθεώρησης της εντολής του ENISA, και ιδίως τη διεύρυνσή του και την επέκταση των αρμοδιοτήτων του οργανισμού· θεωρεί ότι, παράλληλα με τη στήριξή του προς τα κράτη μέλη μέσω της παροχής εμπειρογνωμοσύνης και ανάλυσης, ο ENISA πρέπει να έχει τη δυνατότητα διαχείρισης

[1] ΕΕ L 69 της 16.3.2005, σ. 67.

ορισμένων εκτελεστικών καθηκόντων σε επίπεδο ΕΕ και, σε συνεργασία με τις αντίστοιχες υπηρεσίες των ΗΠΑ, καθήκοντα σχετικά με την αποτροπή και τον εντοπισμό περιστατικών ασφαλείας δικτύων και πληροφοριών και την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών· τονίζει ότι, στο πλαίσιο του κανονισμού του, θα μπορούσαν επίσης να ανατεθούν στον ENISA πρόσθετες αρμοδιότητες σχετικά με την απόκριση σε επιθέσεις στο Διαδίκτυο, στο βαθμό που προσθέτει σαφή αξία στους υφιστάμενους εθνικούς μηχανισμούς απόκρισης·

17. εκφράζει ικανοποίηση για τα αποτελέσματα των πανευρωπαϊκών ασκήσεων κυβερνοασφάλειας του 2010 και 2011, οι οποίες διεξήχθησαν σε όλη την Ένωση υπό την παρακολούθηση του ENISA, με στόχο να στηριχθούν τα κράτη μέλη στον σχεδιασμό, την υλοποίηση και τη δοκιμή ενός πανευρωπαϊκού σχεδίου έκτακτης ανάγκης· καλεί τον ENISA να διατηρήσει τέτοιες ασκήσεις στο θεματολόγιό του και σταδιακά να περιλάβει, κατά περίπτωση, σχετικούς ιδιωτικούς φορείς, προκειμένου να αυξήσει τις συνολικές ικανότητες ασφάλειας διαδικτύου της Ευρώπης· προσβλέπει σε περαιτέρω διεθνή επέκταση, περιλαμβάνοντας εταίρους που συμμερίζονται τις ίδιες απόψεις·

18. καλεί τα κράτη μέλη να καταρτίσουν εθνικά σχέδια έκτακτης ανάγκης για την ασφάλεια στον κυβερνοχώρο, τα οποία θα περιλαμβάνουν στοιχεία ζωτικής σημασίας, όπως σημεία επικοινωνίας, προβλέψεις σχετικά με την παροχή βοήθειας, τη συγκράτηση και την επιδιόρθωση σε περίπτωση διαταραχών ή επιθέσεων στον κυβερνοχώρο με περιφερειακή, εθνική ή διασυνοριακή έκταση· σημειώνει ότι τα κράτη μέλη θα πρέπει επίσης να θέσουν σε εφαρμογή κατάλληλους μηχανισμούς και δομές συντονισμού σε εθνικό επίπεδο, γεγονός το οποίο θα βοηθούσε να διασφαλιστεί ένας καλύτερος συντονισμός μεταξύ των αρμόδιων εθνικών αρχών, και να φροντίσουν ώστε να υπάρχει συνοχή στις ενέργειές τους·

19. συνιστά στην Επιτροπή να προτείνει, μέσω του σχεδίου έκτακτης ανάγκης της ΕΕ για περιστατικά στον κυβερνοχώρο, δεσμευτικά μέτρα για τον καλύτερο συντονισμό σε επίπεδο ΕΕ των τεχνικών και διευθυντικών λειτουργιών μεταξύ των εθνικών και κρατικών CERT·

20. καλεί την Επιτροπή και τα κράτη μέλη να θεσπίσουν τα αναγκαία μέτρα για την προστασία των υποδομών ζωτικής σημασίας από τις επιθέσεις στον κυβερνοχώρο και να διαθέσουν μέσα για την πλήρη αποτροπή της πρόσβασης σε υποδομές ζωτικής σημασίας, σε περίπτωση που μια άμεση επίθεση στον κυβερνοχώρο απειλεί σοβαρά την ομαλή λειτουργία τους·

21. προσβλέπει στην πλήρη εφαρμογή της CERT σε επίπεδο ΕΕ, η οποία θα αποτελέσει βασικό παράγοντα αποτροπής, εντοπισμού, απόκρισης και αποκατάστασης σε περίπτωση σκόπιμων και κακόβουλων κυβερνοεπιθέσεων κατά των θεσμικών οργάνων της ΕΕ·

22. συνιστά στην Επιτροπή να προτείνει δεσμευτικά μέτρα σχεδιασμένα για την επιβολή προτύπων ελάχιστης ασφάλειας και ανθεκτικότητας και τη βελτίωση του συντονισμού μεταξύ των εθνικών CERT·

23. καλεί τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ να διασφαλίσουν την ύπαρξη CERT σε εύρυθμη λειτουργία, για τις οποίες θα ισχύουν ελάχιστα όρια δυναμικού ασφάλειας και ανθεκτικότητας βάσει συμφωνημένων βέλτιστων πρακτικών· τονίζει ότι οι εθνικές CERT πρέπει να αποτελούν μέρος ενός αποτελεσματικού δικτύου στο οποίο ανταλλάσσονται πληροφορίες σύμφωνα με τα απαραίτητα πρότυπα εμπιστευτικότητας·

ζητεί την καθιέρωση διαρκούς εικοσιτετράωρης υπηρεσίας ΠΥΖΣ για κάθε κράτος μέλος, καθώς και τη δημιουργία ενός κοινού ευρωπαϊκού πρωτοκόλλου έκτακτης ανάγκης το οποίο θα ισχύει μεταξύ των εθνικών σημείων επικοινωνίας·

24. τονίζει ότι η οικοδόμηση εμπιστοσύνης και η προώθηση της συνεργασίας μεταξύ των κρατών μελών είναι ζωτικής σημασίας για την προστασία των δεδομένων και των εθνικών δικτύων και υποδομών· καλεί την Επιτροπή να προτείνει μια κοινή διαδικασία εύρεσης και καθορισμού μιας κοινής προσέγγισης για την αντιμετώπιση διασυνοριακών απειλών ΤΠΕ, αναμένοντας από τα κράτη μέλη να παρέχουν στην Επιτροπή γενικές πληροφορίες σχετικά με κινδύνους, απειλές και ευάλωτα σημεία των ΥΖΣ τους·

25. επικροτεί την πρωτοβουλία της Επιτροπής για την ανάπτυξη ενός Ευρωπαϊκού συστήματος ανταλλαγής πληροφοριών και έγκαιρης προειδοποίησης έως το 2013·

26. χαιρετίζει τις ποικίλες διαβουλεύσεις των εμπλεκόμενων φορέων για την ασφάλεια στο Διαδίκτυο και την ΠΥΖΣ, που ξεκίνησαν με πρωτοβουλία της Επιτροπής, όπως η Ευρωπαϊκή συνεργασία δημόσιου-ιδιωτικού τομέα για την ανθεκτικότητα· αναγνωρίζει την ήδη σημαντική συμμετοχή και δέσμευση των παρόχων ΤΠΕ σε τέτοιες προσπάθειες και προτρέπει την Επιτροπή να καταβάλει περαιτέρω προσπάθειες, ώστε να παροτρύνει την ακαδημαϊκή κοινότητα και τις ενώσεις χρηστών ΤΠΕ να αναλάβουν έναν πιο ενεργό ρόλο και να καλλιεργήσουν έναν εποικοδομητικό, πολύπλευρο διάλογο σε θέματα ασφάλειας στον κυβερνοχώρο· στηρίζει την περαιτέρω ανάπτυξη της Ψηφιακής Συνέλευσης ως πλαίσιο διακυβέρνησης της ΠΥΖΣ·

27. εκφράζει ικανοποίηση για το έργο που έχει επιτευχθεί έως τώρα από το Ευρωπαϊκό φόρουμ των κρατών μελών όσον αφορά τον καθορισμό ειδικών για τον κάθε κλάδο κριτηρίων για να προσδιοριστούν οι ευρωπαϊκές υποδομές ζωτικής σημασίας, εστιάζοντας στα σταθερά και κινητά τηλεπικοινωνιακά δίκτυα, καθώς και στην εξέταση των αρχών και των κατευθυντηρίων γραμμών της ΕΕ για την ανθεκτικότητα και τη σταθερότητα του διαδικτύου· προσβλέπει στη συνέχιση της διαμόρφωσης συναίνεσης μεταξύ των κρατών μελών, και, σε αυτό το πλαίσιο, ενθαρρύνει το φόρουμ να συμβάλει στην τρέχουσα προσέγγιση η οποία εστιάζει σε υλικά στοιχεία επιδιώκοντας να συμπεριληφθούν, επίσης, στοιχεία λογικών υποδομών, τα οποία, καθώς η τεχνολογία εικονικής παρουσίασης και υπολογιστικών νεφών εξελίσσεται, θα αποκτούν ολοένα και περισσότερη σημασία για την αποτελεσματικότητα της ΠΥΖΣ·

28. προτείνει να εγκαινιάσει η Επιτροπή μια δημόσια πανευρωπαϊκή εκπαιδευτική πρωτοβουλία, η οποία θα εστιάζει στην εκπαίδευση και την ευαισθητοποίηση των τελικών χρηστών, ιδιωτών και επιχειρηματιών, σχετικά με τις πιθανές απειλές κατά του διαδικτύου και των σταθερών και κινητών συσκευών ΤΠΕ σε κάθε επίπεδο της αλυσίδας χρήσης, καθώς και στην προώθηση ασφαλέστερων προσωπικών συμπεριφορών στον κυβερνοχώρο· υπενθυμίζει, εν προκειμένω, τους κινδύνους που σχετίζονται με τον απαρχαιωμένο εξοπλισμό και λογισμικό τεχνολογίας πληροφοριών·

29. καλεί τα κράτη μέλη να ενισχύσουν, με τη στήριξη της Επιτροπής, τα προγράμματα κατάρτισης και εκπαίδευσης σχετικά με την ασφάλεια των πληροφοριών τα οποία προορίζονται για τις εθνικές αρχές επιβολής του νόμου, τις εθνικές δικαστικές αρχές και τους σχετικούς οργανισμούς της ΕΕ·

30. στηρίζει τη δημιουργία ενός ενωσιακού προγράμματος σπουδών για ακαδημαϊκούς εμπειρογνώμονες στον τομέα της ασφάλειας πληροφοριών, καθώς θα είχε θετικές

επιπτώσεις στην εμπειρογνωμοσύνη και την ετοιμότητα της ΕΕ όσον αφορά τον διαρκώς εξελισσόμενο κυβερνοχώρο και τις εναντίον του απειλές·

31. τάσσεται υπέρ της προώθησης της εκπαίδευσης στον τομέα της ασφάλειας του κυβερνοχώρου (περίοδοι πρακτικής άσκησης για διδακτορικούς φοιτητές, μαθήματα στο πανεπιστήμιο, εργαστήρια, εκπαίδευση σπουδαστών, κ.λπ.) και των εξειδικευμένων εκπαιδευτικών ασκήσεων στον τομέα της ΠΥΖΣ·

32. καλεί την Επιτροπή να εισηγηθεί, έως το τέλος του 2012, μια συνολική στρατηγική ασφάλειας στο Διαδίκτυο για την Ένωση, βασισμένη σε σαφή ορολογία· έχει την άποψη ότι η στρατηγική ασφάλειας στο Διαδίκτυο θα πρέπει να αποσκοπεί στο να δημιουργηθεί ένας κυβερνοχώρος –υποστηριζόμενος από ασφαλείς και ανθεκτικές υποδομές και ανοικτά πρότυπα– ο οποίος να συμβάλλει στην καινοτομία και την ευημερία μέσω της ελεύθερης ροής πληροφοριών, διασφαλίζοντας ταυτόχρονα την αυστηρή προστασία του απόρρητου και άλλες ατομικές ελευθερίες· υποστηρίζει ότι η στρατηγική αυτή θα πρέπει να παρουσιάζει αναλυτικά τις αρχές, τους στόχους, τις μεθόδους, τους μηχανισμούς και τις πολιτικές (τόσο εσωτερικές όσο και εξωτερικές) που απαιτούνται, προκειμένου να ευθυγραμμιστούν οι προσπάθειες σε εθνικό επίπεδο και επίπεδο ΕΕ και να καθιερωθούν πρότυπα ελάχιστης ανθεκτικότητας μεταξύ των κρατών μελών, για να εξασφαλιστούν ασφαλείς, συνεχείς, ισχυρές και ανθεκτικές υπηρεσίες, είτε αυτό αφορά υποδομές ζωτικής σημασίας είτε γενική χρήση του Διαδικτύου·

33. τονίζει ότι, στο πλαίσιο της αναμενόμενης στρατηγικής της Επιτροπής για την ασφάλεια στο Διαδίκτυο, οι εργασίες στον τομέα της ΠΥΖΣ πρέπει να αποτελούν βασικό σημείο αναφοράς και να στοχεύουν σε μια ολιστική και συστηματική προσέγγιση της ασφάλειας στον κυβερνοχώρο, περιλαμβάνοντας όχι μόνο προληπτικά μέτρα, όπως η καθιέρωση ελάχιστων απαιτήσεων για τα μέτρα ασφάλειας ή η εκπαίδευση μεμονωμένων χρηστών, επιχειρήσεων και κρατικών οργανισμών, αλλά και μέτρα αντίδρασης, όπως ποινικές, αστικές και διοικητικές κυρώσεις·

34. ζητεί από την Επιτροπή να προτείνει έναν ισχυρό μηχανισμό για τον συντονισμό της εφαρμογής και της τακτικής αναθεώρησης της στρατηγικής ασφάλειας του Διαδικτύου. πιστεύει ότι ο μηχανισμός αυτός πρέπει να υποστηρίζεται από επαρκείς διοικητικούς, γνωστικούς και οικονομικούς πόρους και στο πεδίο αρμοδιοτήτων του να περιλαμβάνεται η διευκόλυνση της θεμελίωσης θέσεων της ΕΕ στο πλαίσιο των σχέσεών της τόσο με εσωτερικά όσο και διεθνή ενδιαφερόμενα μέρη για θέματα ασφάλειας Διαδικτύου·

35. καλεί την Επιτροπή να εισηγηθεί ένα πλαίσιο της ΕΕ σχετικά με την ειδοποίηση για παραβιάσεις της ασφάλειας σε τομείς ζωτικής σημασίας, όπως αυτοί της ενέργειας, των μεταφορών, της υδροδότησης και της προμήθειας τροφίμων, αλλά και στους τομείς των ΤΠΕ και των χρηματοπιστωτικών υπηρεσιών, ώστε να εξασφαλισθεί ότι ενημερώνονται τα κράτη μέλη και οι χρήστες για περιστατικά, επιθέσεις και διαταραχές στον κυβερνοχώρο·

36. ζητεί από την Επιτροπή να βελτιώσουν τη διαθεσιμότητα στατιστικά αντιπροσωπευτικών δεδομένων σχετικά με το κόστος των κυβερνοεπιθέσεων στην ΕΕ, τα κράτη μέλη και τη βιομηχανία (ιδίως στις χρηματοπιστωτικές υπηρεσίες και τον τομέα των ΤΠΕ) ενισχύοντας τις ικανότητες συλλογής δεδομένων του σχεδιαζόμενου ευρωπαϊκού κέντρου ηλεκτρονικού εγκλήματος, το οποίο προγραμματίζεται να δημιουργηθεί έως το 2013, των CERT και άλλων πρωτοβουλιών της Επιτροπής όπως το ευρωπαϊκό σύστημα ανταλλαγής πληροφοριών και έγκαιρης προειδοποίησης, ώστε να διασφαλισθεί η συστηματική

υποβολή αναφοράς και η παροχή δεδομένων σχετικά με κυβερνοεπιθέσεις και άλλες μορφές κυβερνοεγκλήματος οι οποίες πλήττουν την ευρωπαϊκή βιομηχανία και τα κράτη μέλη, αλλά και να ενισχυθεί η επιβολή του νόμου·

37. τάσσεται υπέρ της στενής συνεργασίας και αλληλεπίδρασης μεταξύ του εθνικού ιδιωτικού τομέα και του ENISA με σκοπό τη διασύνδεση των εθνικών/κρατικών CERT με την ανάπτυξη του ευρωπαϊκού συστήματος ανταλλαγής πληροφοριών και έγκαιρης προειδοποίησης (EISAS)·

38. επισημαίνει ότι η κυρίαρχη κινητήρια δύναμη πίσω από την ανάπτυξη και τη χρήση των τεχνολογιών που έχουν σχεδιαστεί για να αυξηθεί η ασφάλεια στο Διαδίκτυο είναι η βιομηχανία των ΤΠΕ· υπενθυμίζει ότι οι πολιτικές της ΕΕ δεν πρέπει να θέτουν εμπόδια στην ανάπτυξη της ευρωπαϊκής οικονομίας του Διαδικτύου και πρέπει να συμπεριλαμβάνουν τις απαραίτητες πρωτοβουλίες, προκειμένου να αξιοποιηθούν στο έπακρο οι δυνατότητες συνεργασίας μεταξύ επιχειρήσεων και δημοσίου και ιδιωτικού τομέα· συνιστά τη διερεύνηση περαιτέρω κινήτρων για τη βιομηχανία ώστε να αναπτύξει ισχυρότερα σχέδια ασφάλειας για τους διαχειριστές, σύμφωνα με την οδηγία 2008/114/ΕΚ·

39. καλεί την Επιτροπή να υποβάλει νομοθετική πρόταση για την περαιτέρω ποινικοποίηση των κυβερνοεπιθέσεων (π.χ. του ηλεκτρονικού «ψαρέματος» τύπου spear (spear-phishing), της ηλεκτρονικής απάτης κ.λπ.)·

Διεθνής συνεργασία

40. υπενθυμίζει ότι η διεθνής συνεργασία αποτελεί το κυρίαρχο μέσο για να θεσπιστούν αποτελεσματικά μέτρα ασφάλειας στον κυβερνοχώρο· αναγνωρίζει ότι, σήμερα, η ΕΕ δεν συμμετέχει ενεργά και σε διαρκή βάση σε διαδικασίες διεθνούς συνεργασίας και στον διάλογο για την ασφάλεια στον κυβερνοχώρο· απευθύνει έκκληση στην Επιτροπή και την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) να ξεκινήσει έναν εποικοδομητικό διάλογο με όλες τις χώρες που συμμερίζονται τις ίδιες απόψεις, με σκοπό να αναπτυχθεί μια κοινή κατανόηση και πολιτικές που αποσκοπούν στην αύξηση της ανθεκτικότητας του Διαδικτύου και των υποδομών ζωτικής σημασίας· υποστηρίζει ότι, ταυτόχρονα, η ΕΕ θα πρέπει να συμπεριλαμβάνει, σε μόνιμη βάση, τα θέματα της ασφάλειας του Διαδικτύου στο πεδίο των εξωτερικών της σχέσεων, μεταξύ άλλων και όταν σχεδιάζει διάφορους χρηματοδοτικούς μηχανισμούς ή όταν συνάπτει διεθνείς συμφωνίες οι οποίες περιλαμβάνουν την ανταλλαγή και αποθήκευση ευαίσθητων δεδομένων·

41. σημειώνει τα θετικά αποτελέσματα της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο, που υπογράφηκε στη Βουδαπέστη το 2001· τονίζει, ωστόσο, ότι παράλληλα με την ενθάρρυνση περισσότερων χωρών να υπογράψουν και να επικυρώσουν τη σύμβαση, η ΕΥΕΔ πρέπει επίσης να οικοδομήσει διμερείς και πολυμερείς συμφωνίες για την ασφάλεια και την ανθεκτικότητα του Διαδικτύου με διεθνείς εταίρους που συμμερίζονται τις ίδιες απόψεις·

42. τονίζει ότι οι πολυάριθμες τρέχουσες δραστηριότητες των διαφόρων διεθνών οργανισμών, των θεσμικών και άλλων οργάνων και οργανισμών της ΕΕ, καθώς και των κρατών μελών, πρέπει να συντονιστούν ώστε να αποφευχθούν οι επικαλύψεις· για τον σκοπό αυτό, κρίνεται σκόπιμος ο ορισμός αξιωματούχου αρμόδιου για τον συντονισμό, πιθανώς με καθήκοντα συντονιστή της ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ·

43. υπογραμμίζει τη σημασία ενός δομημένου διαλόγου μεταξύ των βασικών συντελεστών και των νομοθετών της ΕΕ και των ΗΠΑ που συμμετέχουν στην ΠΥΖΣ, με σκοπό μια κοινή κατανόηση, ερμηνεία και τοποθέτηση σχετικά με το νομικό πλαίσιο και το πλαίσιο διακυβέρνησης·

44. χαιρετίζει τη σύσταση, στη σύνοδο κορυφής ΕΕ-ΗΠΑ τον Νοέμβριο 2010, της ομάδας εργασίας ΕΕ-ΗΠΑ για την ασφάλεια στον κυβερνοχώρο και το έγκλημα στον κυβερνοχώρο και υποστηρίζει τις προσπάθειές της για την ενσωμάτωση θεμάτων ασφάλειας Διαδικτύου στον διατλαντικό πολιτικό διάλογο· επιδοκιμάζει τη διαμόρφωση, από την Επιτροπή και την κυβέρνηση των ΗΠΑ και υπό την κάλυψη της ομάδας εργασίας ΕΕ-ΗΠΑ, ενός κοινού προγράμματος και ενός χάρτη πορείας προς την πραγματοποίηση κοινών/συγχρονισμένων διηπειρωτικών κυβερνοασκήσεων το 2012/2013·

45. εισηγείται τη θέσπιση δομημένου διαλόγου ανάμεσα στους νομοθέτες της ΕΕ και των ΗΠΑ, προκειμένου να συζητούνται θέματα σχετικά με το Διαδίκτυο στο πλαίσιο της αναζήτησης κοινής κατανόησης, ερμηνείας και θέσεων·

46. καλεί την ΕΥΕΔ και την Επιτροπή, με βάση το έργο που έχει επιτελεστεί από το ευρωπαϊκό φόρουμ των κρατών μελών, να διασφαλιστεί μια δραστήρια στάση εντός των συναφών διεθνών φόρουμ, μεταξύ άλλων και συντονίζοντας τις θέσεις των κρατών μελών με σκοπό να προαχθούν οι βασικές αξίες, στόχοι και πολιτικές της ΕΕ στο πεδίο της ασφάλειας και της ανθεκτικότητας του Διαδικτύου· σημειώνει ότι στα φόρουμ αυτά περιλαμβάνονται το ΝΑΤΟ, τα Ηνωμένα Έθνη (ιδιαίτερα μέσω της Διεθνούς Ένωσης Τηλεπικοινωνιών και του Φόρουμ Διακυβέρνησης του Διαδικτύου), το Σώμα του Διαδικτύου για την εκχώρηση ονομάτων και αριθμών, η Αρχή Εκχωρημένων Αριθμών του Διαδικτύου, ο ΟΑΣΕ, ο ΟΟΣΑ και η Παγκόσμια Τράπεζα·

47. ενθαρρύνει την Επιτροπή και τον ENISA να συμμετάσχουν στους διαλόγους των βασικών ενδιαφερομένων μερών προκειμένου να καθορίσουν τεχνικά και νομικά πρότυπα στον κυβερνοχώρο σε διεθνές επίπεδο·

o

o o

48. αναθέτει στον Πρόεδρό του να διαβιβάσει το παρόν ψήφισμα στο Συμβούλιο και την Επιτροπή.