



Οι διαπραγματευτές της ΕΕ κατέληξαν σε συμφωνία για την ενίσχυση της κυβερνοασφάλειας στην Ευρώπη

Βρυξέλλες, 10 Δεκεμβρίου 2018

Το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και η Ευρωπαϊκή Επιτροπή κατέληξαν απόψε σε πολιτική συμφωνία σχετικά με την πράξη για την ασφάλεια στον κυβερνοχώρο, η οποία ενισχύει την εντολή του οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο (Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών, ENISA), με σκοπό την καλύτερη στήριξη των κρατών μελών στην αντιμετώπιση κυβερνοαπειλών και κυβερνοεπιθέσεων. Η πράξη θεσπίζει επίσης ένα ενωσιακό πλαίσιο για την πιστοποίηση της κυβερνοασφάλειας, ενισχύοντας έτσι την κυβερνοασφάλεια των επιγραμμικών υπηρεσιών και των καταναλωτικών συσκευών.

Ο αντιπρόεδρος Άντρους **Άνσιπ**, ο οποίος είναι αρμόδιος για την Ψηφιακή Ενιαία Αγορά, δήλωσε: «Σ' ένα ψηφιακό περιβάλλον, οι πολίτες και οι εταιρείες πρέπει να αισθάνονται ασφαλείς· έτσι μόνο θα μπορέσουν να αξιοποιήσουν πλήρως την ψηφιακή οικονομία της Ευρώπης. Η εμπιστοσύνη και η ασφάλεια έχουν καθοριστική σημασία για την ορθή λειτουργία της Ψηφιακής Ενιαίας Αγοράς μας. Η αποψινή συμφωνία για την ολοκληρωμένη πιστοποίηση προϊόντων κυβερνοασφάλειας, αφενός, και για έναν ισχυρότερο οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο, αφετέρου, αποτελεί ακόμα ένα βήμα προς την ολοκλήρωσή της.»

Η Επίτροπος κ. Μαρίγια **Γκαμπριέλ**, υπεύθυνη για την ψηφιακή οικονομία και κοινωνία, δήλωσε επίσης: «Η ενίσχυση της κυβερνοασφάλειας στην Ευρώπη και η αύξηση της εμπιστοσύνης των πολιτών και των επιχειρήσεων στην ψηφιακή κοινωνία αποτελούν ύψιστη προτεραιότητα για την Ευρωπαϊκή Ένωση. Σημαντικά περιστατικά κυβερνοεπιθέσεων, όπως το Wannacry και το NotPetya, κρούουν τον κώδωνα του κινδύνου, επειδή δείχνουν τις επιπτώσεις που μπορούν να επιφέρουν οι κυβερνοεπιθέσεις μεγάλης κλίμακας. Από αυτήν την άποψη, πιστεύω ακράδαντα ότι η αποψινή συμφωνία θα βελτιώσει τη συνολική ασφάλεια της Ένωσης και θα τονώσει την ανταγωνιστικότητα των επιχειρήσεων.»

Η [πράξη για την ασφάλεια στον κυβερνοχώρο](#), η οποία προτάθηκε το 2017 ως μέρος μιας ευρείας σειράς μέτρων για την αντιμετώπιση των κυβερνοεπιθέσεων και την οικοδόμηση ισχυρής κυβερνοασφάλειας στην ΕΕ, περιλαμβάνει τα εξής:

- Μόνιμη εντολή του οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο (ENISA) προς αντικατάσταση της περιορισμένης εντολής που θα έληγε το 2020, αλλά και διάθεση περισσότερων πόρων στον οργανισμό με σκοπό την εκπλήρωση των στόχων του, και
- ισχυρότερη βάση για τον ENISA στο νέο ευρωπαϊκό πλαίσιο πιστοποίησης της κυβερνοασφάλειας, προκειμένου να συνδράμει τα κράτη μέλη στην αποτελεσματική αντιμετώπιση των κυβερνοεπιθέσεων με ενίσχυση του ρόλου του στη συνεργασία και τον συντονισμό σε επίπεδο Ένωσης.

Επιπλέον, ο ENISA θα συμβάλει στην αύξηση των δυνατοτήτων ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ και θα στηρίξει την ανάπτυξη ικανοτήτων και την ετοιμότητα. Τέλος, ο ENISA θα αποτελεί ανεξάρτητο κέντρο εμπειρογνωμοσύνης, το οποίο θα συμβάλει στην προώθηση υψηλού επιπέδου ευαισθητοποίησης των πολιτών και των επιχειρήσεων και θα στηρίξει τα θεσμικά όργανα της ΕΕ και τα κράτη μέλη στη χάραξη και εφαρμογή πολιτικής.

Η πράξη για την ασφάλεια στον κυβερνοχώρο δημιουργεί επίσης **πλαίσιο για τα ευρωπαϊκά πιστοποιητικά ασφάλειας στον κυβερνοχώρο** για προϊόντα, διαδικασίες και υπηρεσίες, τα οποία θα ισχύουν σε ολόκληρη την ΕΕ. Πρόκειται για πρωτοποριακή εξέλιξη, καθώς είναι ο πρώτος νόμος της εσωτερικής αγοράς που ανταποκρίνεται στην πρόκληση και ενισχύει την ασφάλεια των συνδεδεμένων προϊόντων, των συσκευών του «διαδικτύου των πραγμάτων» και των υποδομών ζωτικής σημασίας μέσω τέτοιων πιστοποιητικών. Η δημιουργία αυτού του πλαισίου πιστοποίησης της κυβερνοασφάλειας ενσωματώνει χαρακτηριστικά ασφαλείας στα αρχικά στάδια του τεχνικού τους σχεδιασμού και ανάπτυξης (ασφάλεια βάσει σχεδιασμού). Επιτρέπει επίσης στους χρήστες να βεβαιώνουν το επίπεδο διασφάλισης της ασφάλειας και εξασφαλίζει την ανεξάρτητη επαλήθευση των εν λόγω χαρακτηριστικών ασφαλείας.

Οφέλη για πολίτες και επιχειρήσεις

Οι νέοι κανόνες θα συμβάλουν στην ανάπτυξη εμπιστοσύνης των πολιτών στις συσκευές που χρησιμοποιούν σε καθημερινή βάση, καθώς θα μπορούν να επιλέγουν μεταξύ προϊόντων, όπως συσκευές του «διαδικτύου των πραγμάτων», που είναι ασφαλή στον κυβερνοχώρο.

Το πλαίσιο πιστοποίησης θα αποτελεί υπηρεσία ενιαίας εξυπηρέτησης για τη χορήγηση πιστοποιητικών κυβερνοασφάλειας, γεγονός το οποίο θα εξασφαλίσει σημαντική εξοικονόμηση κόστους για τις επιχειρήσεις, και κυρίως για τις μικρομεσαίες επιχειρήσεις, οι οποίες υπό άλλες συνθήκες θα έπρεπε να υποβάλουν αίτηση για τη χορήγηση διαφόρων πιστοποιητικών σε διάφορες χώρες. Μια ενιαία πιστοποίηση θα άρει επίσης πιθανά εμπόδια εισόδου στην αγορά. Επιπλέον, παρέχονται κίνητρα στις εταιρείες να επενδύσουν στην κυβερνοασφάλεια των προϊόντων τους και να την μετατρέψουν σε ανταγωνιστικό πλεονέκτημά τους.

Επόμενα βήματα

Μετά την αποφινική πολιτική συμφωνία, ο νέος κανονισμός θα πρέπει να εγκριθεί επίσημα από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ. Στη συνέχεια, θα δημοσιευθεί στην Επίσημη Εφημερίδα της ΕΕ και αμέσως μετά θα τεθεί επισήμως σε ισχύ, ανοίγοντας τον δρόμο για την παραγωγή ευρωπαϊκών συστημάτων πιστοποίησης και για την έναρξη των εργασιών του οργανισμού της ΕΕ για την ασφάλεια στον κυβερνοχώρο (ENISA) βάσει της εν λόγω σαφούς και μόνιμης εντολής.

Ιστορικό

Η πράξη για την ασφάλεια στον κυβερνοχώρο προτάθηκε ως μέρος της δέσμης μέτρων της 13ης Σεπτεμβρίου 2017 για την ασφάλεια στον κυβερνοχώρο και ως μία από τις προτεραιότητες της [στρατηγικής για την ψηφιακή ενιαία αγορά](#). Για να καταστεί δυνατή η παρακολούθηση της διαρκώς μεταβαλλόμενης απειλής της κυβερνοασφάλειας, η Επιτροπή πρότεινε - έναν χρόνο αργότερα, τον Σεπτέμβριο του 2018 - τη δημιουργία ενός ευρωπαϊκού κέντρου βιομηχανίας, τεχνολογίας και έρευνας για την κυβερνοασφάλεια και ενός δικτύου κέντρων ικανοτήτων στον τομέα της κυβερνοασφάλειας με σκοπό την καλύτερη στόχευση και τον συντονισμό της διαθέσιμης χρηματοδότησης για τη συνεργασία, την έρευνα και την καινοτομία στον τομέα της κυβερνοασφάλειας. Το ευρωπαϊκό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας που προτάθηκε θα διαχειρίζεται τη χρηματοδοτική υποστήριξη από τον προϋπολογισμό της ΕΕ για τον τομέα αυτόν και θα διευκολύνει τις κοινές επενδύσεις Ένωσης, κρατών μελών και κλάδου, ώστε να δοθεί ώθηση στον ενωσιακό κλάδο της κυβερνοασφάλειας και να εξασφαλιστεί ότι τα αμυντικά μας συστήματα χρησιμοποιούν τεχνολογία αιχμής.

Περισσότερες πληροφορίες

[Δελτίο Τύπου – Κατάσταση της Ένωσης 2017 – Κυβερνοασφάλεια: Η Επιτροπή αναβαθμίζει την απόκρισή της στις κυβερνοεπιθέσεις](#)

[Ενημερωτικό δελτίο σχετικά με τη δέσμη μέτρων για την ασφάλεια στον κυβερνοχώρο](#)

[Ενημερωτικό δελτίο σχετικά με τον ENISA και το πλαίσιο της ΕΕ για την πιστοποίηση της κυβερνοασφάλειας](#)

[Όλα τα έγγραφα σχετικά με τη δέσμη μέτρων](#)

IP/18/6759

Αρμόδιοι επικοινωνίας:

[Nathalie VANDYSTADT](#) (+32 2 296 70 83)

[Joseph WALDSTEIN](#) (+ 32 2 29 56184)

Ερωτήσεις του κοινού: [Europe Direct](#) τηλεφωνικά [00 800 67 89 10 11](#) ή με [ηλεκτρονικό μήνυμα](#)