**Ευρωπαϊκή Επιτροπή - Δελτίο Τύπου**

# Η κατάσταση της Ένωσης: Νέοι κανόνες κυβερνοασφάλειας της ΕΕ για ασφαλέστερα προϊόντα υλισμικού και λογισμικού

Βρυξέλλες, 15 Σεπτεμβρίου 2022


Σήμερα, η Επιτροπή υπέβαλε πρόταση για μια νέα πράξη για την κυβερνοανθεκτικότητα με σκοπό την προστασία καταναλωτών και επιχειρήσεων από προϊόντα με ανεπαρκή χαρακτηριστικά ασφάλειας. Μια πρώτη στο είδος της νομοθεσία σε επίπεδο ΕΕ θεσπίζει υποχρεωτικές απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία, καθ' όλη τη διάρκεια του κύκλου ζωής τους.

Η πράξη, που ανακοινώθηκε από την πρόεδρο Ούρσουλα **φον ντερ Λάιεν** τον Σεπτέμβριο του 2021 στην ομιλία της για την κατάσταση της Ευρωπαϊκής Ένωσης, και στηρίζεται στη στρατηγική κυβερνοασφάλειας της ΕΕ του 2020, και στη στρατηγική της ΕΕ για την Ένωση Ασφάλειας του 2020, θα διασφαλίσει ότι τα ψηφιακά προϊόντα, όπως τα ασύρματα και ενσύρματα προϊόντα και το λογισμικό, θα είναι ασφαλέστερα για τους καταναλωτές σε ολόκληρη την ΕΕ: εκτός από την αύξηση της ευθύνης των κατασκευαστών, με την επιβολή της υποχρέωσης παροχής υποστήριξης για ζητήματα ασφάλειας και έκδοσης ενημερώσεων του λογισμικού για την αντιμετώπιση προσδιορισμένων τρωτών σημείων, η πράξη θα επιτρέψει στους καταναλωτές να έχουν επαρκείς πληροφορίες σχετικά με την κυβερνοασφάλεια των προϊόντων που αγοράζουν και χρησιμοποιούν.

Η κ. Μαργκρέιτε **Βέστεϊγιερ**, εκτελεστική αντιπρόεδρος για μια Ευρώπη Έτοιμη για την Ψηφιακή Εποχή, δήλωσε: «*Δικαιούμαστε να νιώθουμε ότι τα προϊόντα που αγοράζουμε στην ενιαία αγορά είναι ασφαλή. Όπως μπορούμε να εμπιστευτούμε ένα παιχνίδι ή ένα ψυγείο με σήμανση CE, η πράξη για την κυβερνοανθεκτικότητα θα διασφαλίσει ότι τα συνδεδεμένα αντικείμενα και το λογισμικό που αγοράζουμε συμμορφώνονται με ισχυρές διασφαλίσεις κυβερνοασφάλειας. Η πράξη θα μεταφέρει την ευθύνη εκεί όπου ανήκει, σε εκείνους που διαθέτουν τα προϊόντα στην αγορά.*»

Ο κ. Μαργαρίτης **Σχοινάς**, αντιπρόεδρος για την Προώθηση του Ευρωπαϊκού Τρόπου Ζωής μας, δήλωσε: «*Η πράξη για την κυβερνοανθεκτικότητα είναι η απάντησή μας στις σύγχρονες απειλές κατά της ασφάλειας που είναι πλέον πανταχού παρούσες στην ψηφιακή μας κοινωνία. Η ΕΕ έχει πρωτοστατήσει στη δημιουργία ενός οικοσυστήματος κυβερνοασφάλειας θεσπίζοντας κανόνες για τις υποδομές ζωτικής σημασίας, για την ετοιμότητα και την αντίδραση στον τομέα της κυβερνοασφάλειας, καθώς και για την πιστοποίηση των προϊόντων κυβερνοασφάλειας. Σήμερα ολοκληρώνουμε αυτό το οικοσύστημα μέσω μιας πράξης που φέρνει την ασφάλεια σε όλα τα σπίτια, σε όλες τις επιχειρήσεις μας και σε κάθε διασυνδεδεμένο προϊόν. Η κυβερνοασφάλεια αποτελεί ζήτημα της κοινωνίας και δεν αποτελεί πλέον υπόθεση του κλάδου.*»

Ο κ. Τιερί **Μπρετόν**, επίτροπος Εσωτερικής Αγοράς, δήλωσε σχετικά: «*Σε ό,τι αφορά την κυβερνοασφάλεια, η Ευρώπη είναι τόσο ισχυρή όσο ο πιο αδύναμος κρίκος της: είτε πρόκειται για ένα ευάλωτο κράτος μέλος είτε για ένα μη ασφαλές προϊόν κατά μήκος της αλυσίδας εφοδιασμού. Οι υπολογιστές, τα τηλέφωνα, οι οικιακές συσκευές, οι εικονικές συσκευές υποστήριξης, τα αυτοκίνητα, τα παιχνίδια... καθένα από αυτά τα εκατοντάδες εκατομμύρια συνδεδεμένα προϊόντα αποτελεί δυνητικό σημείο εισόδου για μια κυβερνοεπίθεση. Ωστόσο, σήμερα τα περισσότερα προϊόντα υλισμικού και λογισμικού δεν υπόκεινται σε υποχρεώσεις κυβερνοασφάλειας. Με την εισαγωγή της κυβερνοασφάλειας εκ σχεδιασμού, η πράξη για την κυβερνοανθεκτικότητα θα συμβάλει στην προστασία της ευρωπαϊκής οικονομίας της Ευρώπης και της συλλογικής μας ασφάλειας.*»

Καθώς οι επιθέσεις λυτρισμικού έπληττων έναν οργανισμό ανά 11 δευτερόλεπτα σε όλο τον κόσμο και το εκτιμώμενο ετήσιο κόστος του κυβερνοεγκλήματος ανήλθε σε 5,5 τρισεκατομμύρια EUR το 2021 [έκθεση του Κοινού Κέντρου Ερευνών (2020): "Cybersecurity – Our Digital Anchor, a European perspective" «Κυβερνοασφάλεια — Η ψηφιακή μας άγκυρα, μια ευρωπαϊκή προοπτική»), η εγγύηση

υψηλού επιπέδου κυβερνοασφάλειας και η μείωση των τρωτών σημείων των ψηφιακών προϊόντων — μία από τις κύριες οδούς για επιτυχείς επιθέσεις — είναι πιο σημαντική από ποτέ. Με την ανάπτυξη των έξυπνων και συνδεδεμένων προϊόντων, ένα περιστατικό κυβερνοασφάλειας σε ένα προϊόν μπορεί να έχει αντίκτυπο σε ολόκληρη την αλυσίδα εφοδιασμού, προκαλώντας ενδεχομένως σοβαρή διαταραχή στις οικονομικές και κοινωνικές δραστηριότητες σε ολόκληρη την εσωτερική αγορά, υπονομεύοντας την ασφάλεια ή ακόμη και απειλώντας την ανθρώπινη ζωή.

Τα μέτρα που προτείνονται σήμερα βασίζονται στο νέο νομοθετικό πλαίσιο για ενωσιακή νομοθεσία για τα προϊόντα και θα θεσπίσουν:

α) κανόνες για τη διάθεση στην αγορά προϊόντων με ψηφιακά στοιχεία για την εγγύηση της κυβερνοασφάλειάς τους·

β) βασικές απαιτήσεις για τον σχεδιασμό, την ανάπτυξη και την παραγωγή προϊόντων με ψηφιακά στοιχεία και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τα εν λόγω προϊόντα·

γ) βασικές απαιτήσεις για τις διαδικασίες χειρισμού τρωτών σημείων που εφαρμόζουν οι κατασκευαστές για να εγγυηθούν την κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία καθ' όλη τη διάρκεια του κύκλου ζωής, και υποχρεώσεις για τους οικονομικούς φορείς σε σχέση με τις εν λόγω διαδικασίες. Οι κατασκευαστές θα πρέπει επίσης να αναφέρουν τα τρωτά σημεία που αξιοποιούνται ενεργά και τα περιστατικά·

δ) κανόνες για την εποπτεία της αγοράς και την επιβολή.

Με τους νέους κανόνες η ευθύνη θα μεταφερθεί στους κατασκευαστές, οι οποίοι πρέπει να διασφαλίζουν τη συμμόρφωση με τις απαιτήσεις ασφάλειας των προϊόντων με ψηφιακά στοιχεία που διατίθενται στην αγορά της ΕΕ. Ως εκ τούτου, οι κανόνες θα ωφελήσουν τους καταναλωτές και τους πολίτες, καθώς και τις επιχειρήσεις που χρησιμοποιούν ψηφιακά προϊόντα, καθώς ενισχύουν τη διαφάνεια των ιδιοτήτων ασφάλειας και προάγουν την εμπιστοσύνη σε προϊόντα με ψηφιακά στοιχεία, αλλά και διασφαλίζουν καλύτερη προστασία των θεμελιωδών δικαιωμάτων τους, όπως η προστασία της ιδιωτικότητας και των δεδομένων.

Ενώ άλλες δικαιοδοσίες ανά τον κόσμο εξετάζουν τα ζητήματα αυτά, η πράξη για την κυβερνοανθεκτικότητα είναι πιθανό να αποτελέσει διεθνές σημείο αναφοράς, πέραν της εσωτερικής αγοράς της ΕΕ. Τα πρότυπα της ΕΕ που βασίζονται στην πράξη για την κυβερνοανθεκτικότητα θα διευκολύνουν την εφαρμογή της και θα αποτελέσουν πλεονέκτημα για τον κλάδο της κυβερνοασφάλειας της ΕΕ στις παγκόσμιες αγορές.

Ο προτεινόμενος κανονισμός θα εφαρμόζεται σε όλα τα προϊόντα που συνδέονται άμεσα ή έμμεσα με άλλη συσκευή ή δίκτυο. Υπάρχουν ορισμένες εξαιρέσεις για προϊόντα για τα οποία οι απαιτήσεις κυβερνοασφάλειας προβλέπονται ήδη σε υφιστάμενους κανόνες της ΕΕ, για παράδειγμα για τα ιατροτεχνολογικά προϊόντα, τις αερομεταφορές ή τα αυτοκίνητα.

## Επόμενα βήματα

Εναπόκειται πλέον στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο να εξετάσουν το σχέδιο της πράξης για την κυβερνοανθεκτικότητα. Μόλις εγκριθεί, οι οικονομικοί φορείς και τα κράτη μέλη θα έχουν στη διάθεσή τους δύο έτη για να προσαρμοστούν στις νέες απαιτήσεις. Εξαίρεση στον κανόνα αυτό αποτελεί η υποχρέωση υποβολής εκθέσεων από τους κατασκευαστές για τα τρωτά σημεία που αποτελούν επί του παρόντος αντικείμενο εκμετάλλευσης και τα συμβάντα, η οποία θα ισχύει ήδη ένα έτος από την ημερομηνία έναρξης ισχύος, δεδομένου ότι απαιτεί λιγότερες οργανωτικές προσαρμογές από ό,τι οι άλλες νέες υποχρεώσεις. Η Επιτροπή θα επανεξετάζει τακτικά την πράξη για την κυβερνοανθεκτικότητα και θα υποβάλλει εκθέσεις σχετικά με τη λειτουργία της.

## Ιστορικό

Η κυβερνοασφάλεια αποτελεί μία από τις κορυφαίες προτεραιότητες της Επιτροπής και ακρογωνιαίο λίθο της ψηφιακής και συνδεδεμένης Ευρώπης. Η αύξηση των κυβερνοεπιθέσεων κατά τη διάρκεια της κρίσης του κορονοϊού έδειξε πόσο σημαντική είναι η προστασία των νοσοκομείων, των ερευνητικών κέντρων και άλλων υποδομών. Απαιτείται ισχυρή δράση σε αυτόν τον τομέα προκειμένου η οικονομία και η κοινωνία της ΕΕ να καταστούν ανθεκτικές στις μελλοντικές εξελίξεις. Εκτιμάται ότι το ετήσιο κόστος των παραβιάσεων δεδομένων ανέρχεται σε τουλάχιστον 10 δισ. EUR και ότι το ετήσιο κόστος των κακόβουλων προσπαθειών διακοπής της κίνησης στο διαδίκτυο ανέρχεται σε τουλάχιστον 65 δισ. EUR (έκθεση εκτίμησης επιπτώσεων που συνοδεύει τον κατ᾽ εξουσιοδότηση κανονισμό της Επιτροπής που συμπληρώνει την οδηγία για τον ραδιοεξοπλισμό)

Η στρατηγική κυβερνοασφάλειας, που παρουσιάστηκε τον Δεκέμβριο του 2020, προτείνει την ενσωμάτωση της κυβερνοασφάλειας σε κάθε στοιχείο της αλυσίδας εφοδιασμού και την περαιτέρω συγκέντρωση των δραστηριοτήτων και των πόρων της ΕΕ στις τέσσερις κοινότητες κυβερνοασφάλειας — εσωτερική αγορά, επιβολή του νόμου, διπλωματία και άμυνα. Η στρατηγική αυτή αποτελεί

προέκταση της στρατηγικής για τη διαμόρφωση του ψηφιακού μέλλοντος της Ευρώπης και της στρατηγικής της ΕΕ για την Ένωση Ασφάλειας, και βασίζεται σε σειρά νομοθετικών πράξεων, δράσεων και πρωτοβουλιών που έχει εφαρμόσει η ΕΕ για την ενίσχυση των ικανοτήτων κυβερνοασφάλειας και τη διασφάλιση μιας πιο κυβερνοανθεκτικής Ευρώπης.

Η νέα πράξη για την κυβερνοανθεκτικότητα θα συμπληρώσει το πλαίσιο κυβερνοασφάλειας της ΕΕ: την οδηγία για την ασφάλεια συστημάτων δικτύου και πληροφοριών (οδηγία NIS), την οδηγία σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS 2), η οποία εγκρίθηκε πρόσφατα από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, και την πράξη της ΕΕ για την κυβερνοασφάλεια.

## Για περισσότερες πληροφορίες

Ερωτήσεις και απαντήσεις: Πράξη της ΕΕ για την κυβερνοανθεκτικότητα

Ενημερωτικό δελτίο σχετικά με την πράξη της ΕΕ για την κυβερνοανθεκτικότητα

Πρόταση πράξης για την κυβερνοανθεκτικότητα

Ενημερωτικό δελτίο σχετικά με τη νέα στρατηγική κυβερνοασφάλειας της ΕΕ

Ενημερωτικό δελτίο για την πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS2)

Ενημερωτικό δελτίο για την κυβερνοασφάλεια: εξωτερική δράση της ΕΕ

Ερωτήσεις και απαντήσεις: Νέα στρατηγική κυβερνοασφάλειας της ΕΕ και νέοι κανόνες για την ενίσχυση της ανθεκτικότητας των φυσικών και ψηφιακών κρίσιμων οντοτήτων

Πρόταση οδηγίας σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση (οδηγία NIS 2)

Πρόταση οδηγίας για την ανθεκτικότητα των κρίσιμων οντοτήτων

IP/22/5374

Αρμόδιοι επικοινωνίας:

Johannes BAHRKE (+32 2 295 86 15)
Marietta GRAMMENOU (+32 2 298 35 83)

Ερωτήσεις του κοινού: Europe Direct τηλεφωνικά 00 800 67 89 10 11 ή με ηλεκτρονικό μήνυμα

Related media

Cybersecurity