



Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 16 Σεπτεμβρίου 2022
(OR. en)

Διοργανικός φάκελος:
2022/0272 (COD)

12429/22
ADD 6

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	15 Σεπτεμβρίου 2022
Αποδέκτης:	Γενική Γραμματεία του Συμβουλίου
Αριθ. εγγρ. Επιτρ.:	SWD(2022) 283 final
Θέμα:	ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΘΕΣΗΣ ΕΚΤΙΜΗΣΗΣ ΕΠΙΠΤΩΣΕΩΝ για την πράξη για την κυβερνοανθεκτικότητα που συνοδεύει το έγγραφο ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - SWD(2022) 283 final.

συνημμ.: SWD(2022) 283 final



ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 15.9.2022
SWD(2022) 283 final

ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ
ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΘΕΣΗΣ ΕΚΤΙΜΗΣΗΣ ΕΠΙΠΤΩΣΕΩΝ

για την πράξη για την κυβερνοανθεκτικότητα

που συνοδεύει το έγγραφο

**ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ
ΣΥΜΒΟΥΛΙΟΥ**

**σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία
και με την τροποποίηση του κανονισμού (ΕΕ) 2019/1020**

{COM(2022) 454 final} - {SEC(2022) 321 final} - {SWD(2022) 282 final}

Δελτίο συνοπτικής παρουσίασης (έως 2 σελίδες)
Εκτίμηση επιπτώσεων της πράξης για την κυβερνοανθεκτικότητα (CRA)
A. Ανάγκη ανάληψης δράσης
Ποιο είναι το πρόβλημα και γιατί αποτελεί πρόβλημα σε επίπεδο ΕΕ;
Τα προϊόντα υλισμικού και λογισμικού συχνά δέχονται επιτυχείς κυβερνοεπιθέσεις· ως αποτέλεσμα το εκτιμώμενο ετήσιο κόστος του κυβερνοεγκλήματος ανήλθε σε 5,5 τρισ. € το 2021. Τα προϊόντα αυτά πάσχουν από δύο σημαντικά προβλήματα που αυξάνουν το κόστος για τους χρήστες και την κοινωνία: 1) χαμηλό επίπεδο κυβερνοασφάλειας, το οποίο αντικατοπτρίζεται από τα εκτεταμένα τρωτά σημεία και την ελλιπή και ασυνεπή παροχή ενημερώσεων ασφάλειας για την αντιμετώπισή τους, και 2) ελλιπή κατανόηση και πρόσβαση των χρηστών σε πληροφορίες, γεγονός που τους εμποδίζει να επιλέγουν προϊόντα με κατάλληλα χαρακτηριστικά κυβερνοασφάλειας ή να τα χρησιμοποιούν με ασφαλή τρόπο. Η κυβερνοασφάλεια προϊόντων με ψηφιακά στοιχεία έχει ισχυρή διασυνοριακή διάσταση, καθώς τα προϊόντα που κατασκευάζονται σε μία χώρα συχνά χρησιμοποιούνται σε ολόκληρη την εσωτερική αγορά. Επιπλέον, τα συμβάντα που αρχικά πλήττουν μία μόνο οντότητα ή ένα μόνο κράτος μέλος συχνά εξαπλώνονται εντός λίγων λεπτών σε ολόκληρη την εσωτερική αγορά. Ενώ η ισχύουσα νομοθεσία για την εσωτερική αγορά εφαρμόζεται σε ορισμένα προϊόντα με ψηφιακά στοιχεία, τα περισσότερα προϊόντα υλισμικού και λογισμικού δεν καλύπτονται επί του παρόντος από ενωσιακή νομοθεσία που αφορά ζητήματα κυβερνοασφάλειας. Ειδικότερα, το ισχύον νομικό πλαίσιο της ΕΕ δεν εξετάζει το ζήτημα της κυβερνοασφάλειας του μη ενσωματωμένου λογισμικού, ακόμη και αν οι κυβερνοεπιθέσεις στοχεύουν όλο και περισσότερο τα τρωτά σημεία των προϊόντων αυτών, με αποτέλεσμα να προκαλείται σημαντικό κοινωνικό και οικονομικό κόστος. Πρόσφατα παραδείγματα είναι το κατασκοπευτικό λογισμικό Pegasus, το οποίο εκμεταλλευόταν τα τρωτά σημεία των κινητών τηλεφώνων, ή το λυτρισμικό WannaCry, το οποίο εκμεταλλεύτηκε ένα τρωτό σημείο των Windows, με αποτέλεσμα να πληγούν υπολογιστές σε όλο τον κόσμο.
Τι θα πρέπει να επιτευχθεί;
Προσδιορίστηκαν δύο κύριοι στόχοι που αποσκοπούν στη διασφάλιση της ορθής λειτουργίας της εσωτερικής αγοράς: 1) να δημιουργηθούν συνθήκες για την ανάπτυξη ασφαλών προϊόντων με ψηφιακά στοιχεία μέσω της διασφάλισης ότι στην αγορά διατίθενται προϊόντα υλισμικού και λογισμικού με λιγότερα τρωτά σημεία και ότι οι κατασκευαστές λαμβάνουν σοβαρά υπόψη το ζήτημα της ασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής των προϊόντων· και 2) να δημιουργηθούν συνθήκες που επιτρέπουν στους χρήστες να λαμβάνουν υπόψη την κυβερνοασφάλεια κατά την επιλογή και τη χρήση προϊόντων με ψηφιακά στοιχεία. Καθορίστηκαν τέσσερις ειδικοί στόχοι: i) να διασφαλιστεί ότι οι κατασκευαστές βελτιώνουν την ασφάλεια των προϊόντων με ψηφιακά στοιχεία ήδη από το στάδιο σχεδιασμού και ανάπτυξης και καθ' όλη τη διάρκεια του κύκλου ζωής· ii) να διασφαλιστεί ένα συνεκτικό πλαίσιο κυβερνοασφάλειας, το οποίο θα διευκολύνει τη συμμόρφωση των κατασκευαστών υλισμικού και λογισμικού· iii) να ενισχυθεί η διαφάνεια των ιδιοτήτων ασφάλειας των προϊόντων με ψηφιακά στοιχεία και iv) να παρέχεται στις επιχειρήσεις και στους καταναλωτές η δυνατότητα να χρησιμοποιούν με ασφάλεια τα προϊόντα με ψηφιακά στοιχεία.
Ποια είναι η προστιθέμενη αξία της δράσης σε επίπεδο ΕΕ (επικουρικότητα);
Ο ισχυρός διασυνοριακός χαρακτήρας της κυβερνοασφάλειας και ο αυξανόμενος αριθμός των συμβάντων με δευτερογενείς επιπτώσεις σε διασυνοριακό επίπεδο, καθώς και σε τομείς και προϊόντα, σημαίνουν ότι οι στόχοι δεν μπορούν να επιτευχθούν αποτελεσματικά μόνο από τα κράτη μέλη. Δεδομένου του

παγκόσμιου χαρακτήρα των αγορών προϊόντων με ψηφιακά στοιχεία, τα κράτη μέλη αντιμετωπίζουν τους ίδιους κινδύνους για το ίδιο προϊόν με ψηφιακά στοιχεία στην επικράτειά τους. Το κατακερματισμένο πλαίσιο δυνητικά αποκλινόντων εθνικών κανόνων που αναδύεται, ενέχει επίσης τον κίνδυνο να παρεμποδίσει την ύπαρξη μιας ανοικτής και ανταγωνιστικής ενιαίας αγοράς για προϊόντα με ψηφιακά στοιχεία. Ως εκ τούτου, η κοινή δράση σε επίπεδο ΕΕ είναι αναγκαία για την αύξηση του επιπέδου εμπιστοσύνης μεταξύ των χρηστών και της ελκυστικότητας των ενωσιακών προϊόντων με ψηφιακά στοιχεία που διατίθενται στην αγορά της ΕΕ. Μπορεί επίσης να ωφελήσει την εσωτερική αγορά, παρέχοντας ασφάλεια δικαίου και εξασφαλίζοντας ισότιμους όρους ανταγωνισμού για τους κατασκευαστές προϊόντων με ψηφιακά στοιχεία.
Β. Λύσεις
Ποιες είναι οι διάφορες επιλογές για την επίτευξη των στόχων; Υπάρχει προτιμώμενη επιλογή ή όχι; Αν όχι, γιατί;
Αναλύθηκαν τέσσερις επιλογές πολιτικής και σχετικές επιμέρους επιλογές που υπερβαίνουν το status quo: 1) προσέγγιση μη δεσμευτικού δικαίου και προαιρετικά μέτρα· 2) ειδική για κάθε προϊόν ad hoc ρυθμιστική παρέμβαση για την κυβερνοασφάλεια υλικών προϊόντων με ψηφιακά στοιχεία και το αντίστοιχο ενσωματωμένο λογισμικό· 3) μικτή προσέγγιση, συμπεριλαμβανομένων οριζόντιων υποχρεωτικών κανόνων για την κυβερνοασφάλεια υλικών προϊόντων με ψηφιακά στοιχεία και αντίστοιχου ενσωματωμένου λογισμικού και κλιμακωτή προσέγγιση για μη ενσωματωμένο λογισμικό, με δύο επιμέρους επιλογές για την αξιολόγηση της συμμόρφωσης· και 4) οριζόντια ρυθμιστική παρέμβαση με την οποία θεσπίζονται απαιτήσεις κυβερνοασφάλειας για ευρύ φάσμα προϊόντων με ψηφιακά στοιχεία, συμπεριλαμβανομένου του μη ενσωματωμένου λογισμικού, με επιμέρους επιλογές για το πεδίο εφαρμογής και την αξιολόγηση της συμμόρφωσης. Η εκτίμηση επιπτώσεων κατέληξε στο συμπέρασμα ότι η προτιμώμενη επιλογή είναι η επιλογή 4, η οποία καλύπτει όλα τα προϊόντα με ψηφιακά στοιχεία και προβλέπει υποχρεωτική αξιολόγηση από τρίτους για τα κρίσιμα προϊόντα, με βάση την αξιολόγηση της αποτελεσματικότητας σε σχέση με τους ειδικούς στόχους, την αποδοτικότητα του κόστους έναντι των οφελών και τη συνοχή.
Ποιες απόψεις διατύπωσαν τα διάφορα ενδιαφερόμενα μέρη; Ποιος υποστηρίζει την κάθε επιλογή;
Όταν τους ζητήθηκε να βαθμολογήσουν την αποτελεσματικότητα των παρεμβάσεων πολιτικής, οι συμμετέχοντες στη δημόσια διαβούλευση συμφώνησαν ότι η επιλογή 4 θα ήταν το αποτελεσματικότερο μέτρο (4,08 σε κλίμακα από το 1 έως το 5). Σε αυτούς περιλαμβάνονται οι οργανώσεις καταναλωτών (5,00), οι συμμετέχοντες που αυτοπροσδιορίζονται ως χρήστες (4,22), οι κοινοποιημένοι οργανισμοί (4,17), οι αρχές εποπτείας της αγοράς (5,00) και οι κατασκευαστές προϊόντων με ψηφιακά στοιχεία (3,85), συμπεριλαμβανομένων επιχειρήσεων μικρού και μεσαίου μεγέθους (4,05).
Γ. Επιπτώσεις της προτιμώμενης επιλογής
Ποια είναι τα οφέλη της προτιμώμενης επιλογής (ειδιάλλως, των κυριότερων επιλογών);
Η προτιμώμενη επιλογή θα αποφέρει σημαντικά οφέλη στα διάφορα ενδιαφερόμενα μέρη. Όσον αφορά τις επιχειρήσεις, θα αποτρέψει την ύπαρξη αποκλινόντων κανόνων ασφάλειας για προϊόντα με ψηφιακά στοιχεία και θα μειώσει το κόστος συμμόρφωσης όσον αφορά τη σχετική νομοθεσία για την κυβερνοασφάλεια. Με τον τρόπο αυτόν, θα μειωθεί ο αριθμός των κυβερνοσυμβάντων, το κόστος διαχείρισης συμβάντων και η ζημία στη φήμη τους. Όσον αφορά ολόκληρη την ΕΕ, εκτιμάται ότι η πρωτοβουλία θα μπορούσε να οδηγήσει σε μείωση του κόστους από συμβάντα που πλήττουν τις επιχειρήσεις κατά περίπου 180 έως 290 δισ. EUR ετησίως. Επιπλέον, η πρωτοβουλία θα οδηγήσει σε

αύξηση του κύκλου εργασιών λόγω της αυξανόμενης χρήσης προϊόντων με ψηφιακά στοιχεία. Επίσης, θα βελτιώσει την παγκόσμια φήμη των εταιρειών, με αποτέλεσμα την αύξηση της ζήτησης εκτός ΕΕ. Για τους τελικούς χρήστες, η προτιμώμενη επιλογή θα ενισχύσει τη διαφάνεια των ιδιοτήτων ασφάλειας και θα διευκολύνει τη χρήση προϊόντων με ψηφιακά στοιχεία. Οι καταναλωτές και οι πολίτες θα ωφεληθούν επίσης από την καλύτερη προστασία των θεμελιωδών δικαιωμάτων τους, όπως η προστασία της ιδιωτικής ζωής και των δεδομένων.
Ποιο είναι το κόστος της προτιμώμενης επιλογής (ειδιάλλως, των κυριότερων επιλογών);
Η προτιμώμενη επιλογή θα αυξήσει το κόστος συμμόρφωσης και επιβολής για τις επιχειρήσεις, τους κοινοποιημένους οργανισμούς και τις δημόσιες αρχές, συμπεριλαμβανομένων των αρχών κοινοποίησης, διαπίστευσης και εποπτείας της αγοράς. Για τους κατασκευαστές λογισμικού και υλισμικού, θα αυξήσει το άμεσο κόστος συμμόρφωσης για τις νέες απαιτήσεις κυβερνοασφάλειας, την αξιολόγηση της συμμόρφωσης, την τεκμηρίωση και τις υποχρεώσεις υποβολής εκθέσεων, με αποτέλεσμα το συνολικό κόστος συμμόρφωσης να ανέρχεται σε περίπου 29 δισ. EUR για εκτιμώμενη τρέχουσα αξία των προϊόντων με ψηφιακά στοιχεία, ύψους 1 485 δισ. EUR σε κύκλο εργασιών. Οι τελικοί χρήστες, συμπεριλαμβανομένων των επιχειρηματικών τελικών χρηστών, των καταναλωτών και των πολιτών ενδέχεται να αντιμετωπίσουν αύξηση τιμών στα προϊόντα με ψηφιακά στοιχεία. Ωστόσο, αυτές οι αυξημένες τιμές θα πρέπει να εξεταστούν στο πλαίσιο των σημαντικών οφελών που περιγράφονται ανωτέρω. Για τους κοινοποιημένους οργανισμούς, το πρόσθετο κόστος αναμένεται να αντισταθμιστεί από αύξηση του κύκλου εργασιών.
Ποιες είναι οι επιπτώσεις στις ΜΜΕ και στην ανταγωνιστικότητα;
Οι ΜΜΕ θα επηρεαστούν από τις νέες απαιτήσεις τόσο ως κατασκευαστές όσο και ως τελικοί χρήστες. Όσον αφορά το κόστος συμμόρφωσης, οι ΜΜΕ θα επηρεαστούν καταρχήν περισσότερο από τις μεγάλες εταιρείες, οι οποίες έχουν συνήθως καλύτερες οικονομίες κλίμακας και μεγαλύτερη ευαισθητοποίηση σχετικά με την κυβερνοασφάλεια. Ωστόσο, οι ΜΜΕ θα επωφεληθούν σε μεγάλο βαθμό από την πρωτοβουλία, καθώς η κυβερνοασφάλεια που είναι ενσωματωμένη σε προϊόντα με ψηφιακά στοιχεία θα επιφέρει σημαντική εξοικονόμηση κόστους για τις ΜΜΕ ως χρήστες. Ως κατασκευαστές, οι ΜΜΕ θα επωφεληθούν από τη μεγαλύτερη εμπιστοσύνη των τελικών χρηστών και τους νέους πελάτες. Η απρόσκοπτη πρόσβαση στην εσωτερική αγορά και η μείωση του κατακερματισμού της αγοράς μπορεί να αποφέρουν ακόμη περισσότερα οφέλη για τις ΜΜΕ, δεδομένου ότι διαθέτουν λιγότερα εφόδια για την αντιμετώπιση των διαφόρων κανονιστικών απαιτήσεων. Ενώ τονίζουν την ανάγκη εφαρμογής αναλογικής προσέγγισης και υποστηρικτικών μέτρων, οι ΜΜΕ υποστήριξαν γενικά την ύπαρξη ισότιμων όρων ανταγωνισμού μεταξύ όλων των εταιρειών και δεν πιστεύουν ότι θα βρεθούν σε μειονεκτική θέση σε σύγκριση με τις μεγαλύτερες εταιρείες σε ένα σενάριο οριζόντιων υποχρεωτικών απαιτήσεων.
Θα υπάρξουν σημαντικές επιπτώσεις στους εθνικούς προϋπολογισμούς και στις εθνικές διοικήσεις;
Η πρωτοβουλία θα έχει αντίκτυπο στις εθνικές αρχές, όπως οι εθνικές κοινοποιούσες αρχές, οι αρχές διαπίστευσης και οι αρχές εποπτείας της αγοράς που έχουν αρμοδιότητες παρακολούθησης και επιβολής των προτεινόμενων μέτρων. Οι εν λόγω αρχές θα επωμιστούν πρόσθετο κόστος προσαρμογών (π.χ. κατάρτιση και ανθρώπινο δυναμικό) και επιβολής ώστε να ληφθούν υπόψη οι νέες απαιτήσεις. Ωστόσο, οι πόροι που δαπανώνται από τους οργανισμούς διαπίστευσης αντισταθμίζονται και καλύπτονται σε μεγάλο βαθμό από τους οργανισμούς αξιολόγησης της συμμόρφωσης μέσω της αγοράς υπηρεσιών διαπίστευσης.
Θα υπάρξουν άλλες σημαντικές επιπτώσεις;
Δεν αναμένονται άλλες σημαντικές αρνητικές επιπτώσεις. Η προτιμώμενη επιλογή πολιτικής θα συμβάλει στη μείωση του αριθμού και της σοβαρότητας των συμβάντων, συμπεριλαμβανομένων των παραβιάσεων

δεδομένων προσωπικού χαρακτήρα, και θα έχει θετικές κοινωνικές επιπτώσεις, όπως η μείωση του κυβερνοεγκλήματος. Η ζήτηση για επαγγελματίες στον τομέα της ασφάλειας είναι πιθανό να αυξηθεί, ενώ και οι ασυμμετρίες πληροφόρησης στον τομέα της κυβερνοασφάλειας θα μειωθούν.
Όσον αφορά την αναλογικότητα;
Η προτιμώμενη επιλογή δεν υπερβαίνει τα αναγκαία για την ικανοποιητική επίτευξη των ειδικών στόχων. Η παρέμβαση θα διασφαλίσει ότι τα προϊόντα με ψηφιακά στοιχεία είναι ασφαλή καθ' όλη τη διάρκεια του κύκλου ζωής τους και ότι η προστασία είναι ανάλογη των κινδύνων που αντιμετωπίζονται.
Δ. Παρακολούθηση
Πότε θα επανεξεταστεί η πολιτική;
Έως [36 μήνες] μετά την ημερομηνία εφαρμογής της πρωτοβουλίας και στη συνέχεια κάθε τέσσερα έτη, η Επιτροπή υποβάλλει στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο έκθεση σχετικά με την αξιολόγηση και την επανεξέταση της πρωτοβουλίας.