



Συμβούλιο
της Ευρωπαϊκής Ένωσης

Βρυξέλλες, 18 Δεκεμβρίου 2020
(OR. en)

Διοργανικός φάκελος:
2020/0359(COD)

14150/20
ADD 3

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

ΔΙΑΒΙΒΑΣΤΙΚΟ ΣΗΜΕΙΩΜΑ

Αποστολέας:	Για τη Γενική Γραμματέα της Ευρωπαϊκής Επιτροπής, η κα Martine DEPREZ, Διευθύντρια
Ημερομηνία Παραλαβής:	16 Δεκεμβρίου 2020
Αποδέκτης:	κ. Jeppe TRANHOLM-MIKKELSEN, Γενικός Γραμματέας του Συμβουλίου της Ευρωπαϊκής Ένωσης
Αριθ. εγγρ. Επιτρ.:	SWD(2020) 344 final
Θέμα:	ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΕΚΘΕΣΗΣ ΕΚΤΙΜΗΣΗΣ ΕΠΙΠΤΩΣΕΩΝ που συνοδεύει το έγγραφο πρόταση για οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

Διαβιβάζεται συνημμένως στις αντιπροσωπίες το έγγραφο - SWD(2020) 344 final.

σνημμ.: SWD(2020) 344 final

Βρυξέλλες, 16.12.2020
SWD(2020) 344 final

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

που συνοδεύει το έγγραφο

πρόταση για οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου
σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση
και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 345 final}

Δελτίο συνοπτικής παρουσίασης

Εκτίμηση επιπτώσεων σχετικά με την επανεξέταση της οδηγίας (ΕΕ) 2016/1148, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (οδηγία NIS).

A. Ανάγκη ανάληψης δράσης

Ποιο είναι το πρόβλημα και γιατί είναι πρόβλημα σε επίπεδο ΕΕ;

Παρά τα αξιοσημείωτα επιτεύγματά της, η οδηγία NIS, η οποία άνοιξε το δρόμο για μια σημαντική αλλαγή νοοτροπίας, θεσμικής και κανονιστικής προσέγγισης στην κυβερνοασφάλεια σε πολλά κράτη μέλη, έχει ήδη δείξει τα όριά της. Ο ψηφιακός μετασχηματισμός της κοινωνίας (που εντάθηκε από την κρίση της COVID-19) έχει διευρύνει το τοπίο των απειλών και δημιουργεί νέες προκλήσεις, που απαιτούν προσαρμοσμένες και καινοτόμες απαντήσεις. Ο αριθμός των κυβερνοεπιθέσεων εξακολουθεί να αυξάνεται, και οι ολοένα και πιο εξελιγμένες επιθέσεις προέρχονται από ευρύ φάσμα πηγών εντός και εκτός ΕΕ.

Με βάση την αξιολόγηση της λειτουργίας της οδηγίας NIS, η εκτίμηση επιπτώσεων προσδιόρισε τα ακόλουθα προβλήματα: το χαμηλό επίπεδο κυβερνοανθεκτικότητας των επιχειρήσεων που δραστηριοποιούνται στην ΕΕ· τις διαφορές όσον αφορά την ανθεκτικότητα μεταξύ κρατών μελών και τομέων και το χαμηλό επίπεδο κοινής επίγνωσης της κατάστασης και την έλλειψη κοινής αντιμετώπισης κρίσεων. Για παράδειγμα, λόγω ορισμένων τέτοιων προβλημάτων και κινητήριων παραγόντων, υπάρχουν περιπτώσεις στις οποίες μεγάλα νοσοκομεία σε ένα κράτος μέλος δεν emπίπτουν στο πεδίο εφαρμογής της οδηγίας NIS και, ως εκ τούτου, δεν υποχρεούνται να εφαρμόζουν τα σχετικά μέτρα ασφαλείας, ενώ σε άλλο κράτος μέλος σχεδόν όλες οι νοσοκομειακές μονάδες καλύπτονται από τις απαιτήσεις ασφαλείας της οδηγίας NIS.

Τι πρέπει να επιτευχθεί;

Η επανεξέταση της οδηγίας NIS αποβλέπει σε τρεις γενικούς στόχους:

- 1. Αύξηση του επιπέδου κυβερνοανθεκτικότητας ενός ευρέος συνόλου επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση σε όλους τους σχετικούς τομείς**, με τη θέσπιση κανόνων που διασφαλίζουν ότι όλες οι δημόσιες και ιδιωτικές οντότητες σε ολόκληρη την εσωτερική αγορά, οι οποίες επιτελούν σημαντικές λειτουργίες για την οικονομία και την κοινωνία στο σύνολό της, υποχρεούνται να λαμβάνουν επαρκή μέτρα κυβερνοασφάλειας.
- 2. Μείωση των διαφορών στην ανθεκτικότητα εντός της εσωτερικής αγοράς στους τομείς που καλύπτονται ήδη από την οδηγία**, με περαιτέρω ευθυγράμμιση 1) του εκ των πραγμάτων πεδίου εφαρμογής, 2) των απαιτήσεων ασφαλείας και αναφοράς συμβάντων, 3) των διατάξεων που διέπουν την εθνική εποπτεία και επιβολή και 4) των ικανοτήτων των αρμόδιων αρχών στα κράτη μέλη.
- 3. Βελτίωση του επιπέδου κοινής επίγνωσης της κατάστασης και της συλλογικής ικανότητας προετοιμασίας και αντίδρασης**, με τη λήψη μέτρων για την αύξηση του επιπέδου εμπιστοσύνης μεταξύ των αρμόδιων αρχών, την ανταλλαγή περισσότερων πληροφοριών και τον καθορισμό κανόνων και διαδικασιών σε περίπτωση περιστατικού ή κρίσης μεγάλης κλίμακας.

Ποια είναι η προστιθέμενη αξία της δράσης σε επίπεδο ΕΕ (επικουρικότητα);

Η ανθεκτικότητα της κυβερνοασφάλειας σε ολόκληρη την Ένωση δεν μπορεί να είναι αποτελεσματική εάν προσεγγιστεί με κατακερματισμένο τρόπο με εθνικά ή περιφερειακά στεγανά. Η οδηγία NIS είχε ως

στόχο να αντιμετωπίσει αυτή την αδυναμία, διαμορφώνοντας ένα πλαίσιο για την ασφάλεια των δικτυακών πληροφοριακών συστημάτων σε εθνικό και ενωσιακό επίπεδο. Ωστόσο, η μεταφορά της οδηγίας στο εθνικό δίκαιο και η εφαρμογή της ανέδειξαν επίσης εγγενείς αδυναμίες ορισμένων διατάξεων ή προσεγγίσεων, όπως η ασαφής οριοθέτηση του πεδίου εφαρμογής της οδηγίας NIS. Επιπλέον, μετά την κρίση της νόσου COVID-19, η ευρωπαϊκή οικονομία εξαρτάται ακόμη περισσότερο από δικτυακά και πληροφοριακά συστήματα και υπάρχει ολοένα και μεγαλύτερη διασύνδεση μεταξύ τομέων και υπηρεσιών. Ως εκ τούτου, η πρώτη περιοδική επανεξέταση της οδηγίας NIS δημιούργησε την ευκαιρία για περαιτέρω δράση σε επίπεδο ΕΕ. Η παρέμβαση της ΕΕ που υπερβαίνει τα ισχύοντα μέτρα της οδηγίας NIS δικαιολογείται κυρίως από: i) τον διασυννοριακό χαρακτήρα του προβλήματος· ii) τις δυνατότητες που έχει η δράση σε επίπεδο ΕΕ να βελτιώσει και να διευκολύνει αποτελεσματικές εθνικές πολιτικές· iii) τη συμβολή συντονισμένων και συνεργατικών δράσεων πολιτικής NIS στην αποτελεσματική προστασία των δεδομένων και της ιδιωτικής ζωής.

B. Λύσεις

Ποιες είναι οι διάφορες επιλογές για την επίτευξη των στόχων; Υπάρχει προτιμώμενη επιλογή ή όχι; Εάν όχι, γιατί;

Στην εκτίμηση επιπτώσεων αναλύονται τέσσερις επιλογές πολιτικής: (0) διατήρηση του status quo· (1) μη νομοθετικά μέτρα για την ευθυγράμμιση της μεταφοράς στο εθνικό δίκαιο· (2) περιορισμένες αλλαγές στην οδηγία NIS για περαιτέρω εναρμόνιση· (3) συστημικές και διαρθρωτικές αλλαγές της οδηγίας NIS. Η επιλογή 1 απορρίφθηκε σε πρώιμο στάδιο, καθώς δεν αποκλίνει σημαντικά από το status quo. Η εκτίμηση επιπτώσεων καταλήγει στο συμπέρασμα ότι **προτιμώμενη επιλογή** είναι η επιλογή 3 (δηλαδή **συστημικές και διαρθρωτικές αλλαγές του πλαισίου NIS**), καθώς προβλέπει μια πιο θεμελιώδη αλλαγή προσέγγισης προς την κάλυψη ενός ευρύτερου τμήματος των οικονομιών σε ολόκληρη την Ένωση, αλλά με πιο εστιασμένη εποπτεία που στοχεύει αναλογικά μεγάλες και βασικές εταιρείες, καθορίζοντας παράλληλα με σαφήνεια το πεδίο εφαρμογής. Επίσης, θα εξορθολογίσει και θα εναρμονίσει περαιτέρω τις σχετικές με την ασφάλεια υποχρεώσεις των εταιρειών, θα δημιουργήσει ένα πιο αποτελεσματικό πλαίσιο για τις επιχειρησιακές πτυχές και θα δημιουργήσει μια ξεκάθαρη βάση για κοινές ευθύνες και λογοδοσία των σχετικών φορέων και θα παρέχει κίνητρα για την ανταλλαγή πληροφοριών.

Ποιες απόψεις διατύπωσαν οι διάφοροι ενδιαφερόμενοι; Ποιος υποστηρίζει την κάθε επιλογή;

Οι περισσότερες αρμόδιες αρχές και επιχειρήσεις τάχθηκαν υπέρ της αναθεώρησης της οδηγίας NIS. Σε αρκετές διαβουλεύσεις, επεσήμαναν ότι μια αναθεωρημένη οδηγία NIS θα πρέπει να καλύπτει πρόσθετους (υπο)τομείς, να εναρμονίζει ή να εξορθολογίζει περαιτέρω τα μέτρα ασφάλειας και τις υποχρεώσεις αναφοράς περιστατικών. Τα ενδιαφερόμενα μέρη έδειξαν επίσης υποστήριξη για νέες ιδέες ή μέτρα πολιτικής, τα οποία αποτελούν μέρος μόνο της προτιμώμενης επιλογής (π.χ. πολιτικές για την ασφάλεια της αλυσίδας εφοδιασμού, θεσμοθέτηση ενός επιχειρησιακού πλαισίου διαχείρισης κρίσεων σε επίπεδο ΕΕ).

Γ. Επιπτώσεις της προτιμώμενης επιλογής

Ποια είναι τα οφέλη της προτιμώμενης επιλογής (ειδάλλως, των κυριότερων επιλογών);

Η προτιμώμενη επιλογή αναμένεται να αποφέρει σημαντικά οφέλη: οι εκτιμήσεις που έγιναν βάσει οικονομικής μοντελοποίησης που βασίστηκε σε υποστηρικτική μελέτη για την επανεξέταση της NIS δείχνουν ότι η προτιμώμενη επιλογή μπορεί να οδηγήσει σε μείωση του κόστους των περιστατικών κυβερνοασφάλειας κατά 11,3 δισ. EUR.

Το τομεακό πεδίο εφαρμογής θα διευρυνθεί σημαντικά στο πλαίσιο NIS, ωστόσο, παράλληλα με τα

<p>ανωτέρω οφέλη, η επιβάρυνση που ενδέχεται να προκύψει από τις απαιτήσεις NIS, ιδίως από την πλευρά της επίβλεψης, θα είναι επίσης ισορροπημένη τόσο για τις νέες οντότητες που θα καλύπτονται όσο και για τις αρμόδιες αρχές. Αυτό οφείλεται στο γεγονός ότι το νέο πλαίσιο NIS θα καθιερώσει προσέγγιση δύο επιπέδων, με έμφαση στις μεγάλες και βασικές οντότητες, και διαφοροποίηση του εποπτικού καθεστώτος που επιτρέπει την εκ των υστέρων μόνο επίβλεψη (δηλ. μόνο ως αντίδραση και χωρίς τη θέσπιση γενικής υποχρέωσης συστηματικής τεκμηρίωσης της συμμόρφωσης) για μεγάλο αριθμό εξ αυτών, ιδίως εκείνων που θεωρούνται «σημαντικές» αλλά όχι «βασικές».</p> <p>Συνολικά, η προτιμώμενη επιλογή πολιτικής θα οδηγήσει σε αποδοτικές αντισταθμίσεις και συνέργειες, με τις βέλτιστες δυνατότητες από όλες τις επιλογές πολιτικής που αναλύθηκαν, ώστε να διασφαλιστεί αυξημένο και συνεκτικό επίπεδο κυβερνοανθεκτικότητας βασικών οντοτήτων σε ολόκληρη την Ένωση, το οποίο θα οδηγήσει εν τέλει σε εξοικονόμηση κόστους τόσο για τις επιχειρήσεις όσο και για την κοινωνία.</p>
<p>Ποιο είναι το κόστος της προτιμώμενης επιλογής (ειδάλλως, των κυριότερων επιλογών);</p>
<p>Από την προτιμώμενη επιλογή πολιτικής θα προκύψει ορισμένο κόστος συμμόρφωσης και επιβολής για τις αρμόδιες αρχές των κρατών μελών (εκτιμήθηκε συνολική αύξηση κατά περίπου 20-30 % των πόρων). Ωστόσο, το νέο πλαίσιο θα αποφέρει επίσης σημαντικά οφέλη μέσω καλύτερης επισκόπησης των βασικών επιχειρήσεων και αλληλεπίδρασης μαζί τους, ενισχυμένης διασυννοριακής επιχειρησιακής συνεργασίας, καθώς και μέσω αμοιβαίας συνδρομής και μηχανισμών αξιολόγησης από ομοτίμους. Τα οφέλη αυτά θα οδηγήσουν σε συνολική αύξηση των ικανοτήτων κυβερνοασφάλειας σε όλα τα κράτη μέλη.</p> <p>Για τις εταιρείες που θα εμπίπτουν στο πεδίο εφαρμογής του πλαισίου NIS, εκτιμάται ότι θα χρειαστούν αύξηση των τρεχουσών δαπανών τους για την ασφάλεια ΤΠΕ κατά 22 % το πολύ για τα πρώτα έτη μετά τη θέσπιση του νέου πλαισίου NIS (το ποσοστό αυτό θα ανέρχεται σε 12 % για εταιρείες που εμπίπτουν ήδη στο πεδίο εφαρμογής της ισχύουσας οδηγίας NIS). Ωστόσο, αυτή η μέση αύξηση των δαπανών για την ασφάλεια ΤΠΕ θα οδηγήσει σε αναλογικό όφελος από τις εν λόγω επενδύσεις, ιδίως χάρη σε σημαντική μείωση του κόστους των περιστατικών κυβερνοασφάλειας (που εκτιμάται σε 11,3 δις. EUR σε διάστημα δέκα ετών).</p>
<p>Ποιες είναι οι επιπτώσεις στις ΜΜΕ και στην ανταγωνιστικότητα;</p>
<p>Στην προτιμώμενη επιλογή, οι μικρές και οι πολύ μικρές επιχειρήσεις θα εξαιρούνται από το πεδίο εφαρμογής του πλαισίου NIS. Για τις μεσαίες επιχειρήσεις, αναμένεται να σημειωθεί αύξηση του επιπέδου των δαπανών για την ασφάλεια ΤΠΕ κατά τα πρώτα έτη μετά τη θέσπιση του νέου πλαισίου NIS. Ταυτόχρονα, η αύξηση του επιπέδου των απαιτήσεων ασφάλειας για τις εν λόγω οντότητες θα τους παράσχει επίσης κίνητρα να αναπτύξουν τις ικανότητες κυβερνοασφάλειας και θα συμβάλει στη βελτίωση της διαχείρισης κινδύνου ΤΠΕ εκ μέρους τους.</p>
<p>Θα υπάρξουν σημαντικές επιπτώσεις στους εθνικούς προϋπολογισμούς και στις εθνικές διοικήσεις;</p>
<p>Θα υπάρξει επίπτωση στους εθνικούς προϋπολογισμούς και στις εθνικές διοικήσεις: βραχυπρόθεσμα και μεσοπρόθεσμα αναμένεται εκτιμώμενη αύξηση κατά περίπου 20-30 % των πόρων.</p>
<p>Θα υπάρξουν άλλες σημαντικές επιπτώσεις;</p>
<p>Δεν αναμένονται άλλες σημαντικές αρνητικές επιπτώσεις. Η προτιμώμενη επιλογή πολιτικής αναμένεται να οδηγήσει σε αρτιότερες ικανότητες κυβερνοασφάλειας και, κατά συνέπεια, θα έχει ουσιαστικότερες μετριαστικές επιπτώσεις στον αριθμό και τη σοβαρότητα των περιστατικών, συμπεριλαμβανομένων των παραβιάσεων δεδομένων. Είναι επίσης πιθανό η πρόταση να έχει θετικές επιπτώσεις στη διασφάλιση</p>

ισότιμων όρων ανταγωνισμού σε όλα τα κράτη μέλη για όλες τις οντότητες που καλύπτονται από το πεδίο εφαρμογής της οδηγίας NIS και να μειώσει τις ασυμμετρίες πληροφόρησης στον τομέα της κυβερνοασφάλειας.

Αναλογικότητα;

Η προτιμώμενη επιλογή δεν υπερβαίνει τα αναγκαία για την ικανοποιητική επίτευξη των ειδικών στόχων. Η προβλεπόμενη ευθυγράμμιση και ο προβλεπόμενος εξορθολογισμός των μέτρων ασφαλείας και των υποχρεώσεων υποβολής εκθέσεων σχετίζονται με τα αιτήματα των κρατών μελών και των επιχειρήσεων για βελτίωση του ισχύοντος πλαισίου.

Δ. Παρακολούθηση

Πότε θα επανεξεταστεί η πολιτική;

Η πρώτη επανεξέταση θα πραγματοποιηθεί 54 μήνες μετά την έναρξη ισχύος της νομικής πράξης. Η Επιτροπή θα υποβάλει έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο σχετικά με την επανεξέτασή της. Η επανεξέταση θα εκπονηθεί με την υποστήριξη του ENISA και της ομάδας συνεργασίας.