

**ΕΚΤΕΛΕΣΤΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2018/151 ΤΗΣ ΕΠΙΤΡΟΠΗΣ**

της 30ής Ιανουαρίου 2018

που θεσπίζει κανόνες για την εφαρμογή της οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, όσον αφορά τον περαιτέρω προσδιορισμό των στοιχείων που πρέπει να λαμβάνονται υπόψη από τους παρόχους ψηφιακών υπηρεσιών για τη διαχείριση κινδύνων που απειλούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών, καθώς και των παραμέτρων βάσει των οποίων καθορίζεται κατά πόσον ο αντίκτυπος συμβάντος είναι σημαντικός

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη την οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση <sup>(1)</sup>, και ιδίως το άρθρο 16 παράγραφος 8,

Εκτιμώντας τα ακόλουθα:

- (1) Σύμφωνα με την οδηγία (ΕΕ) 2016/1148, οι πάροχοι ψηφιακών υπηρεσιών έχουν τη δυνατότητα να λαμβάνουν τεχνικά και οργανωτικά μέτρα που θεωρούν κατάλληλα και αναλογικά για τη διαχείριση του κινδύνου που απειλεί την ασφάλεια των συστημάτων δικτύου και πληροφοριών, εφόσον τα μέτρα αυτά διασφαλίζουν κατάλληλο επίπεδο ασφάλειας και λαμβάνουν υπόψη τα στοιχεία που προβλέπει η εν λόγω οδηγία.
- (2) Κατά τον προσδιορισμό των κατάλληλων και αναλογικών τεχνικών και οργανωτικών μέτρων, ο πάροχος ψηφιακών υπηρεσιών θα πρέπει να υιοθετεί συστηματική προσέγγιση της ασφάλειας των πληροφοριών, χρησιμοποιώντας προσέγγιση βάσει κινδύνου.
- (3) Προκειμένου να κατοχυρωθεί η ασφάλεια συστημάτων και εγκαταστάσεων, οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να εκτελούν διαδικασίες αξιολόγησης και ανάλυσης. Οι δραστηριότητες αυτές θα πρέπει να αφορούν τη συστηματική διαχείριση των συστημάτων δικτύου και πληροφοριών, την υλική και περιβαλλοντική ασφάλεια, την ασφάλεια εφοδιασμού και τους ελέγχους πρόσβασης.
- (4) Κατά την ανάλυση κινδύνου στο πλαίσιο της συστηματικής διαχείρισης των συστημάτων δικτύου και πληροφοριών, οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να ενθαρρύνονται να προσδιορίζουν ειδικούς κινδύνους και να εκφράζουν ποσοτικά τη σημασία τους, για παράδειγμα εντοπίζοντας απειλές κατά περιουσιακών στοιχείων κρίσιμης σημασίας, καθώς και τον τρόπο με τον οποίο αυτές μπορούν να επηρεάσουν τις λειτουργίες, και προσδιορίζοντας ποιος είναι ο καλύτερος τρόπος αντιμετώπισης αυτών των απειλών με βάση τις υπάρχουσες ικανότητες και τους απαιτούμενους πόρους.
- (5) Οι πολιτικές για τους ανθρώπινους πόρους θα μπορούσαν να αναφέρονται σε διαχείριση δεξιοτήτων, συμπεριλαμβανομένων πτυχών που σχετίζονται με την ανάπτυξη δεξιοτήτων σχετικών με την ασφάλεια και την ευαισθητοποίηση. Κατά τη λήψη απόφασης σχετικά με την ενδεδειγμένη δέσμη πολιτικών για την ασφάλεια λειτουργίας, οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη πτυχές της διαχείρισης των αλλαγών, διαχείρισης τρωτών σημείων, τυποποίησης των επιχειρησιακών και διοικητικών πρακτικών και χαρτογράφησης του συστήματος.
- (6) Στις πολιτικές για την αρχιτεκτονική ασφάλειας θα μπορούσε να περιλαμβάνεται ιδίως ο διαχωρισμός των δικτύων και των συστημάτων, καθώς και ειδικά μέτρα ασφάλειας για κρίσιμες λειτουργίες όπως οι λειτουργίες διαχείρισης. Ο διαχωρισμός των δικτύων και των συστημάτων θα μπορούσε να επιτρέπει σε πάροχο ψηφιακών υπηρεσιών να διακρίνει ανάμεσα σε στοιχεία, όπως ροές δεδομένων και υπολογιστικούς πόρους, που ανήκουν σε πελάτες, σε ομάδα πελατών, στον πάροχο ψηφιακών υπηρεσιών ή σε τρίτα μέρη.
- (7) Τα μέτρα που έχουν ληφθεί όσον αφορά την υλική και περιβαλλοντική ασφάλεια θα πρέπει να εγγυώνται την ασφάλεια των συστημάτων δικτύου και πληροφοριών του οργανισμού από ζημία η οποία προκαλείται από συμβάντα όπως κλοπή, πυρκαγιά, πλημμύρα ή άλλα καιρικά φαινόμενα, διακοπές τηλεπικοινωνιών ή ηλεκτρικής ενέργειας.
- (8) Στην ασφάλεια του εφοδιασμού με ηλεκτρική ενέργεια, καύσιμα ή ψύξη θα μπορούσε να συγκαταλέγεται η ασφάλεια της αλυσίδας εφοδιασμού, στην οποία περιλαμβάνεται, ειδικότερα, η ασφάλεια τρίτων αντισυμβαλλόμενων και υπεργολάβων και η διαχείρισή τους. Η ιχνηλασιμότητα των κρίσιμων προμηθειών αναφέρεται στην ικανότητα του παρόχου ψηφιακών υπηρεσιών να προσδιορίζει και να καταγράφει τις πηγές αυτών των προμηθειών.
- (9) Στους χρήστες ψηφιακών υπηρεσιών θα πρέπει να συγκαταλέγονται τα φυσικά και νομικά πρόσωπα που είναι πελάτες ή συνδρομητές διαδικτυακής αγοράς ή υπηρεσίας υπολογιστικού νέφους, ή που επισκέπτονται ιστότοπο μηχανής αναζήτησης προκειμένου να πραγματοποιήσουν αναζήτηση με λέξεις-κλειδιά.

<sup>(1)</sup> ΕΕ L 194 της 19.7.2016, σ. 1.

- (10) Όταν προσδιορίζεται η σημασία του αντικτύπου ενός συμβάντος, οι περιπτώσεις που προβλέπονται στον παρόντα κανονισμό θα πρέπει να θεωρείται ότι δεν αποτελούν εξαντλητικό κατάλογο σημαντικών συμβάντων. Διδάγματα μπορούν να αντληθούν από την εφαρμογή του παρόντος κανονισμού και από τις εργασίες της ομάδας συνεργασίας σχετικά με τη συλλογή πληροφοριών για τις βέλτιστες πρακτικές για κινδύνους και συμβάντα, καθώς και από συζητήσεις σχετικά με τις λεπτομέρειες για την υποβολή κοινοποιήσεων συμβάντων που προβλέπονται στο άρθρο 11 παράγραφος 3 σημεία θ) και ιγ) της οδηγίας (ΕΕ) 2016/1148. Ως αποτέλεσμα θα μπορούσαν να προκύψουν ολοκληρωμένες κατευθυντήριες γραμμές σχετικά με ποσοτικά κατώτατα όρια των παραμέτρων κοινοποίησης που ενδέχεται να ενεργοποιούν την υποχρέωση κοινοποίησης για τους παρόχους ψηφιακών υπηρεσιών σύμφωνα με το άρθρο 16 παράγραφος 3 της οδηγίας (ΕΕ) 2016/1148. Όπου ενδείκνυται, η Επιτροπή θα μπορούσε επίσης να εξετάσει το ενδεχόμενο αναθεώρησης των κατώτατων ορίων που προβλέπονται σήμερα στον παρόντα κανονισμό.
- (11) Για να μπορούν οι αρμόδιες αρχές να ενημερώνονται σχετικά με δυνητικούς νέους κινδύνους, οι πάροχοι ψηφιακών υπηρεσιών θα πρέπει να ενθαρρύνονται να αναφέρουν αυτοβούλως κάθε συμβάν τα χαρακτηριστικά του οποίου αγνοούσαν προηγουμένως, όπως νέα προγράμματα εκμετάλλευσης ατελειών, διανύσματα επιθέσεων ή παράγοντες απειλής, τρωτά σημεία και κινδύνους.
- (12) Ο παρών κανονισμός θα πρέπει να αρχίσει να εφαρμόζεται την επόμενη ημέρα από τη λήξη της προθεσμίας μεταφοράς της οδηγίας (ΕΕ) 2016/1148 στο εθνικό δίκαιο.
- (13) Τα μέτρα που προβλέπει ο παρών κανονισμός είναι σύμφωνα με τη γνώμη της επιτροπής για την ασφάλεια συστημάτων δικτύου και πληροφοριών, που αναφέρεται στο άρθρο 22 της οδηγίας (ΕΕ) 2016/1148,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

#### Άρθρο 1

#### Αντικείμενο

Με τον παρόντα κανονισμό προσδιορίζονται περαιτέρω τα στοιχεία τα οποία πρέπει να λαμβάνονται υπόψη από τους παρόχους ψηφιακών υπηρεσιών κατά τον προσδιορισμό και τη λήψη μέτρων για την εξασφάλιση υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών τα οποία χρησιμοποιούν στο πλαίσιο της παροχής υπηρεσιών που αναφέρονται στο παράρτημα ΙΙΙ της οδηγίας (ΕΕ) 2016/1148 και προσδιορίζονται περαιτέρω οι παράμετροι που πρέπει να λαμβάνονται υπόψη για να κρίνεται κατά πόσον συμβάν έχει σημαντικό αντίκτυπο στην παροχή των εν λόγω υπηρεσιών.

#### Άρθρο 2

#### Στοιχεία ασφάλειας

1. Ως ασφάλεια των συστημάτων και των εγκαταστάσεων που αναφέρεται στο άρθρο 16 παράγραφος 1 στοιχείο α) της οδηγίας (ΕΕ) 2016/1148 νοείται η ασφάλεια των συστημάτων δικτύου και πληροφοριών και του φυσικού τους περιβάλλοντος· περιλαμβάνει τα ακόλουθα στοιχεία:

- α) συστηματική διαχείριση των συστημάτων δικτύου και πληροφοριών: χαρτογράφηση των συστημάτων πληροφοριών και θέσπιση δέσμης κατάλληλων πολιτικών για τη διαχείριση της ασφάλειας των πληροφοριών, στην οποία συμπεριλαμβάνεται η ανάλυση των κινδύνων, οι ανθρώπινοι πόροι, η ασφάλεια των λειτουργιών, η αρχιτεκτονική ασφάλειας, η ασφάλεια της διαχείρισης του κύκλου ζωής των δεδομένων και του συστήματος και, κατά περίπτωση, η κρυπτογράφηση και η διαχείρισή της.
- β) υλική και περιβαλλοντική ασφάλεια: η ύπαρξη δέσμης μέτρων για την προστασία της ασφάλειας των συστημάτων δικτύου και πληροφοριών των παρόχων ψηφιακών υπηρεσιών από ζημία με χρήση προσέγγισης βασισμένης στην επικινδυνότητα όλων των πιθανών κινδύνων, η οποία καλύπτει, για παράδειγμα, βλάβες του συστήματος, ανθρώπινα σφάλματα, κακόβουλες ενέργειες ή φυσικά φαινόμενα·
- γ) ασφάλεια προμηθειών: η δημιουργία και συντήρηση των κατάλληλων πολιτικών που διασφαλίζουν την προσβασιμότητα και, κατά περίπτωση, την ιχνηλασιμότητα των κρίσιμων προμηθειών που χρησιμοποιούνται για την παροχή των υπηρεσιών·
- δ) ελέγχους πρόσβασης στα συστήματα δικτύου και πληροφοριών: η ύπαρξη δέσμης μέτρων με τα οποία εξασφαλίζεται η φυσική και λογική πρόσβαση σε συστήματα δικτύων και πληροφοριών, συμπεριλαμβανομένης της ασφάλειας διαχείρισης των συστημάτων δικτύου και πληροφοριών, παρέχεται με εξουσιοδοτήσεις και περιορισμούς βάσει απαιτήσεων εμπορικής λειτουργίας και ασφάλειας.

2. Σε ό, τι αφορά τη διαχείριση συμβάντων που αναφέρεται στο άρθρο 16 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2016/1148, τα μέτρα που λαμβάνονται από τον πάροχο ψηφιακών υπηρεσιών περιλαμβάνουν:

- α) διεργασίες και διαδικασίες ανίχνευσης που συντηρούνται και ελέγχονται προκειμένου να εξασφαλιστεί έγκαιρη και κατάλληλη ενημέρωση για μη φυσιολογικά συμβάντα·
- β) διαδικασίες και πολιτικές για την υποβολή εκθέσεων σχετικά με συμβάντα και τον εντοπισμό αδυναμιών και τρωτών σημείων των οικείων συστημάτων πληροφοριών·

- γ) αντίδραση σύμφωνα με καθιερωμένες διαδικασίες και υποβολή εκθέσεων σχετικά με τα αποτελέσματα του ληφθέντος μέτρου·
- δ) αξιολόγηση της σοβαρότητας του συμβάντος, τεκμηρίωση των γνώσεων που αποκομίστηκαν από την ανάλυση των συμβάντων και συλλογή των σχετικών πληροφοριών που μπορούν να χρησιμεύσουν ως αποδεικτικά στοιχεία και να στηρίξουν μια διαδικασία συνεχούς βελτίωσης.
3. Ως διαχείριση της επιχειρησιακής συνέχειας που αναφέρεται στο άρθρο 16 παράγραφος 1 στοιχείο γ) της οδηγίας (ΕΕ) 2016/1148 νοείται η ικανότητα ενός οργανισμού να διατηρεί ή, κατά περίπτωση, να αποκαθιστά την παροχή των υπηρεσιών σε αποδεκτά προκαθορισμένα επίπεδα μετά από συμβάν που διαταράσσει την παροχή των υπηρεσιών, και περιλαμβάνει:
- α) την εγκατάσταση και τη χρήση σχεδίων έκτακτης ανάγκης βασισμένων σε ανάλυση του επιχειρηματικού αντίκτυπου για τη διασφάλιση της συνέχειας των υπηρεσιών που παρέχουν οι πάροχοι ψηφιακών υπηρεσιών που αξιολογούνται και ελέγχονται σε τακτική βάση, για παράδειγμα, μέσω ασκήσεων·
- β) ικανότητες ανάκαμψης μετά από καταστροφές που αξιολογούνται και ελέγχονται σε τακτική βάση, για παράδειγμα, μέσω ασκήσεων.
4. Η παρακολούθηση, οι επιθεωρήσεις και οι δοκιμές που αναφέρονται στο άρθρο 16 παράγραφος 1 στοιχείο δ) της οδηγίας (ΕΕ) 2016/1148 περιλαμβάνουν τη δημιουργία και συντήρηση των πολιτικών για:
- α) την εκτέλεση σχεδιασμένης αλληλουχίας παρατηρήσεων ή μετρήσεων με τις οποίες αξιολογείται κατά πόσον τα συστήματα δικτύου και πληροφοριών λειτουργούν όπως προβλέπεται·
- β) την επιθεώρηση και την επαλήθευση ότι πρότυπο ή σειρά κατευθυντήριων γραμμών τηρείται, ότι τα πρακτικά είναι ακριβή και ότι επιτυγχάνονται οι στόχοι σχετικά με την αποδοτικότητα και την αποτελεσματικότητα·
- γ) τη διαδικασία που προορίζεται να αποκαλύψει ελλείψεις στο πλαίσιο των μηχανισμών ασφάλειας των συστημάτων δικτύου και πληροφοριών που προστατεύουν τα δεδομένα και διατηρούν τις λειτουργικές δυνατότητες όπως προβλέπεται. Η διαδικασία αυτή περιλαμβάνει τεχνικές διαδικασίες και το προσωπικό που απασχολείται στη ροή λειτουργίας.
5. Ως διεθνή πρότυπα που αναφέρονται στο άρθρο 16 παράγραφος 1 στοιχείο ε) της οδηγίας (ΕΕ) 2016/1148 νοούνται τα πρότυπα που έχουν εκδοθεί από διεθνή φορέα τυποποίησης, όπως αναφέρεται στο άρθρο 2 παράγραφος 1 στοιχείο α) του κανονισμού (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου<sup>(1)</sup>. Σύμφωνα με το άρθρο 19 της οδηγίας (ΕΕ) 2016/1148, μπορούν επίσης να χρησιμοποιηθούν ευρωπαϊκά ή διεθνή αποδεκτά πρότυπα και προδιαγραφές για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένων υφιστάμενων εθνικών προτύπων.
6. Οι πάροχοι ψηφιακών υπηρεσιών διασφαλίζουν ότι διαθέτουν κατάλληλη τεκμηρίωση ώστε να παρέχεται στην αρμόδια αρχή η δυνατότητα να επαληθεύει τη συμμόρφωση με τα στοιχεία ασφάλειας που ορίζονται στις παραγράφους 1, 2, 3, 4 και 5.

### Άρθρο 3

#### **Παράμετροι που πρέπει να λαμβάνονται υπόψη για να προσδιορίζεται κατά πόσον ο αντίκτυπος ενός συμβάντος είναι σημαντικός**

1. Όσον αφορά τον αριθμό των χρηστών που επηρεάζονται από συμβάν, ιδίως των χρηστών που εξαρτώνται από την υπηρεσία για την παροχή δικών τους υπηρεσιών, που αναφέρεται στο άρθρο 16 παράγραφος 4 στοιχείο α) της οδηγίας (ΕΕ) 2016/1148, ο πάροχος ψηφιακών υπηρεσιών είναι σε θέση να εκτιμήσει ένα από τα εξής:
- α) τον αριθμό των πληγέντων φυσικών και νομικών προσώπων με τα οποία έχει συναφθεί σύμβαση για την παροχή της υπηρεσίας· ή
- β) τον αριθμό των διγόμενων χρηστών που έχουν χρησιμοποιήσει την υπηρεσία ιδίως με βάση προηγούμενα δεδομένα κίνησης.
2. Ως διάρκεια του συμβάντος που αναφέρεται στο άρθρο 16 παράγραφος 4 στοιχείο β) νοείται η χρονική περίοδος από τη διατάραξη της κατάλληλης παροχής της υπηρεσίας, όσον αφορά τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα, μέχρι τον χρόνο της αποκατάστασης.
3. Όσον αφορά το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν που αναφέρεται στο άρθρο 16 παράγραφος 4 στοιχείο γ) της οδηγίας (ΕΕ) 2016/1148, ο πάροχος ψηφιακών υπηρεσιών είναι σε θέση να προσδιορίσει κατά πόσον το συμβάν επηρεάζει την παροχή των υπηρεσιών του σε συγκεκριμένα κράτη μέλη.
4. Η έκταση της διατάραξης της λειτουργίας της υπηρεσίας που αναφέρεται στο άρθρο 16 παράγραφος 4 στοιχείο δ) της οδηγίας (ΕΕ) 2016/1148 μετράται με βάση ένα ή περισσότερα από τα ακόλουθα χαρακτηριστικά που επηρεάζονται δυσμενώς από συμβάν: τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή την εμπιστευτικότητα των δεδομένων ή των συναφών υπηρεσιών.

<sup>(1)</sup> Κανονισμός (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών του Συμβουλίου 89/686/ΕΟΚ και 93/15/ΕΟΚ και των οδηγιών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ L 316 της 14.11.2012, σ. 12).

5. Όσον αφορά την έκταση του αντίκτυπου στις οικονομικές και κοινωνικές δραστηριότητες που αναφέρεται στο άρθρο 16 παράγραφος 4 στοιχείο ε) της οδηγίας (ΕΕ) 2016/1148, ο πάροχος ψηφιακών υπηρεσιών είναι σε θέση να συμπεράνει, βάσει ενδείξεων όπως η φύση των συμβατικών του σχέσεων με τον πελάτη ή, κατά περίπτωση, ο δυνητικός αριθμός των επηρεαζόμενων χρηστών, κατά πόσον το συμβάν έχει προκαλέσει σημαντικές υλικές ή μη υλικές ζημιές για τους χρήστες, όπως σε σχέση με την υγεία, την ασφάλεια ή την περιουσιακή ζημία.

6. Για τους σκοπούς των παραγράφων 1, 2, 3, 4 και 5, οι πάροχοι ψηφιακών υπηρεσιών δεν απαιτείται να συλλέγουν πρόσθετες πληροφορίες στις οποίες δεν έχουν πρόσβαση.

#### Άρθρο 4

##### Σημαντικός αντίκτυπος συμβάντος

1. Συμβάν θεωρείται ότι έχει σημαντικό αντίκτυπο όταν έχει συμβεί τουλάχιστον μία από τις ακόλουθες καταστάσεις:
  - α) η υπηρεσία που παρέχεται από πάροχο ψηφιακών υπηρεσιών δεν ήταν διαθέσιμη για περισσότερες από 5 000 000 χρηστούρες· ο όρος χρηστούρα αναφέρεται στο πλήθος των θιγόμενων χρηστών στην Ένωση επί χρονικό διάστημα εξήντα λεπτών·
  - β) το συμβάν είχε ως αποτέλεσμα την απώλεια της ακεραιότητας, της αυθεντικότητας, ή της εμπιστευτικότητας των αποθηκευμένων ή μεταδοθέντων ή των επεξεργασμένων δεδομένων ή τις συναφείς υπηρεσίες που προσφέρονται ή είναι προσβάσιμες μέσω συστήματος δικτύου και πληροφοριών του παρόχου ψηφιακών υπηρεσιών, επηρεάζοντας περισσότερους από 100 000 χρήστες εντός της Ένωσης·
  - γ) το συμβάν προκάλεσε κίνδυνο για τη δημόσια ασφάλεια, τη δημόσια προστασία ή κίνδυνο απώλειας ανθρώπινων ζωών·
  - δ) το συμβάν έχει προκαλέσει υλικές ζημιές σε τουλάχιστον έναν χρήστη στην Ένωση, εφόσον η ζημία που προκλήθηκε στον εν λόγω χρήστη υπερβαίνει το 1 000 000 EUR.
2. Στηριζόμενη στις βέλτιστες πρακτικές που συγκεντρώθηκαν από την ομάδα συνεργασίας κατά την εκτέλεση των καθηκόντων της δυνάμει του άρθρου 11 παράγραφος 3 της οδηγίας (ΕΕ) 2016/1148 και από τις συζητήσεις δυνάμει του άρθρου 11 παράγραφος 3 στοιχείο ιγ) του εν λόγω κανονισμού, η Επιτροπή δύναται να αναθεωρήσει τα κατώτατα όρια που καθορίζονται στην παράγραφο 1.

#### Άρθρο 5

##### Έναρξη ισχύος

1. Ο παρών κανονισμός αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή του στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.
2. Εφαρμόζεται από την 10η Μαΐου 2018.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 30 Ιανουαρίου 2018.

Για την Επιτροπή  
Ο Πρόεδρος  
Jean-Claude JUNCKER