**ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ**

***στο σχέδιο νόμου «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση»***

Προς τη Βουλή των Ελλήνων

*Α. Γενικό μέρος*

Με τον παρόντα νόμο εναρμονίζεται το εθνικό δίκαιο με τις διατάξεις της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (στο εξής «Οδηγία NIS» ή «Οδηγία») ενσωματώνοντας την Οδηγία αυτή στο εθνικό δίκαιο. Σκοπός της Οδηγίας NIS, είναι η θέσπιση μέτρων για την επίτευξη ενός κοινού ελάχιστου επιπέδου ως προς την ασφάλεια συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση.

Η Ένωση, λαμβάνοντας υπ' όψιν το ζωτικό ρόλο που διαδραματίζουν για την κοινωνία και την οικονομία τα συστήματα δικτύου και πληροφοριών και εκτιμώντας την σοβαρότητα της βλάβης που προκαλείται από σκόπιμες επιζήμιες ενέργειες στην οικονομία της Ένωσης και γενικότερα στην κοινωνία, θεσπίζει κοινό πλαίσιο κανόνων για όλα τα κράτη-μέλη, ώστε να επιτευχθεί ένα ελάχιστο κοινό επίπεδο ασφάλειας και ενθαρρύνει τη συνεργασία με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών («ENISA»), ώστε να υπάρχει και ενιαία στρατηγική αντιμετώπισης των κινδύνων. Ο ορισμός της έννοιας των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) και των Παρόχων Ψηφιακών Υπηρεσιών (ΠΨΥ) μετά τη διαπίστωση ότι, υπάρχει διαφοροποίηση εντός της Ένωσης στο επίπεδο προστασίας καταναλωτών και επιχειρήσεων, θεσπίζεται με κοινό τρόπο, με το σαφή προσδιορισμό για ορισμένες κοινές παραμέτρους και αφήνοντας τα κράτη-μέλη να ορίσουν τις συγκεκριμένες τιμές τους σε εθνικό επίπεδο, χωρίς να αποκλείεται η θέσπιση και επιπλέον παραμέτρων από τα κράτη-μέλη ή επιπλέον κανόνων ασφάλειας. Οι κανόνες μπορεί να οριστούν τόσο από τους ΦΕΒΥ και τους ΠΨΥ όσο και από τα κράτη-μέλη.

Η εφαρμογή της Οδηγίας 2016/1148/ΕΕ δεν αναιρεί άλλες αυστηρότερες διατάξεις ή ειδικότερους κανόνες που θεσπίστηκαν ήδη, ή θα θεσπιστούν στο μέλλον, ως τομεακές πράξεις της Ένωσης, όπως η Οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Ούτε θα πρέπει οι διατάξεις της να εφαρμόζονται σε παρόχους υπηρεσιών εμπιστοσύνης κατά την έννοια του κανονισμού (ΕΕ) αριθμ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Η αυστηρότερη νομοθεσία στο συγκεκριμένο πεδίο είναι εκείνη που ορίζει τα μέτρα που πρέπει να ληφθούν. Παράλληλα λαμβάνει υπόψη σημαντικά κανονιστικά κείμενα στο πλαίσιο αυτό, όπως η απόφαση 2013/488/ΕΕ του Συμβουλίου και οι συμφωνίες εμπιστευτικότητας ή οι ανεπίσημες συμφωνίες εμπιστευτικότητας, όπως το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light Protocol» και είναι σύμφωνη με το άρθρο 346 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ).

Ο παρών νόμος αποσκοπεί στο να αποτελέσει ένα ελάχιστο μέσο εναρμόνισης της Ελλάδας με τα υπόλοιπα κράτη-μέλη της Ε.Ε., όσον αφορά στην εφαρμογή της Οδηγίας NIS, στον τομέα της ασφάλειας συστημάτων δικτύων και πληροφοριών. Παρέχει δε, τη δυνατότητα να λαμβάνονται όλα τα αναγκαία μέτρα για τη διαφύλαξη της δημόσιας τάξης και ασφάλειας, καθώς και για τη διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων. Οι υφιστάμενοι ή μέλλοντες να ισχύσουν ρυθμιστικοί κανόνες για τομείς της οικονομίας, μέσω εθνικών-τομεακών νομικών πράξεων, εφαρμόζονται αντί του παρόντος νόμου, εάν και εφόσον οι υποχρεώσεις που προβλέπουν είναι τουλάχιστον ισοδύναμες με τις απορρέουσες από τον παρόντα νόμο.

Για σκοπούς παρακολούθησης και εφαρμογής του παρόντος νόμου ορίζεται η Εθνική Αρμόδια Αρχή (εφεξής «Εθνική Αρχή Κυβερνοασφάλειας»), η οποία θα λειτουργεί και ως «Ενιαίο Κέντρο Επαφής» (ΕΚΕ), για τη διευκόλυνση της διασυνοριακής συνεργασίας, εφοδιασμένη με τους κατάλληλους τεχνικούς, οικονομικούς και ανθρώπινους πόρους για την επίτευξη των σκοπών της. Η Εθνική Αρχή Κυβερνοασφάλειας θα έχει συντονιστικό ρόλο επί όλων των σχετικών θεμάτων. Παράλληλα, ορίζεται και η Αρμόδια Ομάδα Απόκρισης σε Συμβάντα («Computer Security Incident Response Team — CSIRT» ή και «Computer Emergency Response Team - CERT»), η οποία και θα λαμβάνει άμεσα την κοινοποίησή τους, θα φροντίζει για την αντιμετώπισή τους και θα ενημερώνει σχετικά και όποτε απαιτείται το ΕΚΕ. Το ΕΚΕ υποβάλλει τακτική συνοπτική και ανωνυμοποιημένη (για λόγους επιχειρηματικού απορρήτου ή και προσωπικών δεδομένων) έκθεση, στο αρμόδιο ευρωπαϊκό όργανο («Ομάδα Συνεργασίας - Cooperation Group»), η οποία περιλαμβάνει στοιχεία για το πλήθος των παραβιάσεων, το είδος και τη σοβαρότητά τους. Λαμβάνεται μέριμνα για τον εφοδιασμό της Αρμόδιας Ομάδας Απόκρισης σε Συμβάντα με κατάλληλους πόρους (τεχνικούς, οικονομικούς και ανθρώπινους). Σε κάθε περίπτωση η ευθύνη συμμόρφωσης βαρύνει τους ΦΕΒΥ και τους ΠΨΥ που θα προσδιοριστούν βάσει του παρόντος νόμου.

Συνοπτικά και εν κατακλείδι, ο παρών νόμος επιλαμβάνεται των θεμάτων ασφάλειας συστημάτων δικτύου και πληροφοριών μόνο για τους τομείς που ρητά αναφέρονται σε αυτόν, λαμβάνοντας μέριμνα για:

α) την αποφυγή συγκρούσεων της εθνικής νομοθεσίας με τομεακές πράξεις της Ένωσης (εφαρμόζεται η αυστηρότερη ρύθμιση),

β) την πρόβλεψη εξαιρέσεων λόγω ειδικών συνθηκών (εθνική ασφάλεια κ.λπ.),

γ) την τήρηση της αρχής της ίσης μεταχείρισης μεταξύ προσώπων και μεταξύ επιχειρήσεων,

δ) το σεβασμό των ατομικών δικαιωμάτων και της επιχειρηματικής ελευθερίας,

ε) τη συνεπή συνεργασία με τα όργανα της Ένωσης, αλλά και

στ) την εξειδίκευση και προσαρμογή των κανόνων του παρόντος προς τις διατάξεις της Οδηγίας.

*Β. Ειδικό μέρος*

Ο νόμος αποτελείται από 5 Κεφάλαια (Κεφάλαια Α΄ ως και Ε΄ αντίστοιχα των Ι ως και ν της Οδηγίας), 17 άρθρα και 2 Παραρτήματα (Ι και ΙΙ αντίστοιχα των ΙΙ και ΙΙΙ της Οδηγίας). Τα Κεφάλαια του νόμου Α΄,Β΄,Γ΄,Δ΄,Ε΄ αντιστοιχούν στα Κεφάλαια της Οδηγίας I,II,IV,V,VI-VII. Το Κεφάλαιο ΙΙΙ της Οδηγίας δεν απαιτείται να ενσωματωθεί, ενώ το Κεφάλαιο Ε΄ του παρόντος περιλαμβάνει τις διατάξεις των Κεφαλαίων VI και VII της Οδηγίας, μαζί. Τα άρθρα 1 ως και 17 του νόμου αντιστοιχούν στα άρθρα της Οδηγίας, σύμφωνα με τον ακόλουθο Πίνακα 1.

| Άρθρο Οδηγίας | Άρθρο νόμου |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 4 § ζ |
| 4 | 3 |
| 5 | 4 |
| 6 | 5 |
| 7 | 6 |
| 8 | 7 |
| 9 | 8 |
| 10 | Δεν απαιτείται ενσωμάτωση |
| 11 | Δεν απαιτείται ενσωμάτωση |
| 12 | Δεν απαιτείται ενσωμάτωση |
| 13 | Δεν απαιτείται ενσωμάτωση |
| 14 | 9 |
| 15 | 10 |
| 16 | 11 |
| 17 | 12 |
| 18 | 13 |
| 19 | Δεν απαιτείται ενσωμάτωση |
| 20 | 14 |
| 21 | 15 |
| 22 | Δεν απαιτείται ενσωμάτωση |
| 23 | Δεν απαιτείται ενσωμάτωση |
| 24 | Δεν απαιτείται ενσωμάτωση |
| 25 | Δεν απαιτείται ενσωμάτωση |
| 26 | Δεν απαιτείται ενσωμάτωση |
| 27 | Δεν απαιτείται ενσωμάτωση |

Επίσης τα Παραρτήματα Ι και ΙΙ του νόμου αντιστοιχούν στα Παραρτήματα ΙΙ και ΙΙΙ της Οδηγίας διότι το Παράρτημα Ι αυτής έχει ενσωματωθεί στο άρθρο 7 του παρόντος νόμου. Στα Παραρτήματα Ι και ΙΙ παρατίθενται δύο πίνακες εκ των οποίων ο πρώτος (Παράρτημα Ι) αφορά τους τομείς δραστηριότητας και υποτομείς υπηρεσιών επί των οποίων έχει εφαρμογή ο νόμος (τηρουμένων των προβλεπομένων εξαιρέσεων ή περιορισμών κατά περίπτωση), ο δε δεύτερος (Παράρτημα ΙΙ) αφορά τους τομείς παροχής ψηφιακών υπηρεσιών από τους φορείς που ασκούν ανάλογες δραστηριότητες εντός της χώρας. Τα παραρτήματα αποτελούν βασικό και αναπόσπαστο μέρος του νόμου επειδή προσδιορίζουν το πεδίο εφαρμογής του. Στο Κεφάλαιο Α΄ (άρθρα 1, 2, 3, 4) περιγράφονται οι γενικές αρχές για την εφαρμογή του νόμου, όπως το αντικείμενο και πεδίο εφαρμογής του νόμου, οι εξαιρέσεις ή και η σχέση με διατάξεις από άλλες νομικές πράξης της Ένωσης, οι ορισμοί των εννοιών και ο τρόπος χαρακτηρισμού των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών με αναφορά στα Παραρτήματα και τέλος οι παράμετροι χαρακτηρισμού των συμβάντων ως σοβαρών διαταράξεων της ασφάλειας. Στο Κεφάλαιο Β΄ (άρθρα 5, 6 και 7) περιγράφεται το εθνικό πλαίσιο για την ασφάλεια συστημάτων δικτύων και πληροφοριών, στο οποίο περιλαμβάνεται η γενική στρατηγική («Εθνική Στρατηγική Κυβερνοασφάλειας» - ΕΣΚ) και οι δύο κύριες αρχές που μεριμνούν η μεν πρώτη («Εθνική Αρχή Κυβερνοασφάλειας» - ΕΑΚ) για την στρατηγική και το γενικό σχεδιασμό σε εθνικό επίπεδο ενώ η δεύτερη («Ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών» - CSIRT) για την άμεση ανταπόκριση σε συμβάντα ασφάλειας σε εθνικό επίπεδο. Στο Κεφάλαιο Γ΄ και στο Κεφάλαιο Δ΄ περιγράφονται οι υποχρεώσεις των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) και των Παρόχων Ψηφιακών Υπηρεσιών (ΠΨΥ) αντίστοιχα. Οι υποχρεώσεις αυτές αφορούν κυρίως τόσο την αποστολή πληροφοριών και την εφαρμογή υποδείξεων διόρθωσης ελλείψεών τους όσο και τη συνεργασία κατά τους ελέγχους. Στο Κεφάλαιο Ε΄ των τελικών διατάξεων, περιλαμβάνονται προβλέψεις για τους φορείς που μπορούν και θέλουν να προβούν σε εθελούσιες κοινοποιήσεις συμβάντων και καθορίζονται οι κυρώσεις για τους παραβάτες του νόμου, ως προς τα γενικά όρια. Οι κυρώσεις μπορούν να εξειδικευθούν με ειδικότερη πράξη ή πράξεις ανά τομέα και εφαρμόζονται αυτοτελώς ανεξαρτήτως άλλων κυρώσεων για τις ίδιες παραβάσεις.

*Γ. Επί των άρθρων*

Άρθρο 1
Αντικείμενο και πεδίο εφαρμογής

Με το άρθρο 1 του νόμου (άρθρο 1 της Οδηγίας) καθορίζεται το αντικείμενο και το πεδίο εφαρμογής του νόμου. Αναφέρεται ρητά η ενσωμάτωση της Οδηγίας αλλά και το γεγονός ότι όλα τα θεσπιζόμενα μέτρα, εκείνα που ρητά προβλέπονται από την Οδηγία αλλά και κάθε επιπλέον μέτρο, αποσκοπούν στην επίτευξη υψηλού επιπέδου ασφάλειας σε εθνικό επίπεδο στα συστήματα δικτύου και πληροφοριών (παράγραφος 1).

Με την παράγραφο 2 αποτυπώνονται με σαφήνεια οι τρεις αρχές (Εθνικής Αρχή Κυβερνοασφάλειας ή ΕΑΚ, Εθνική αρχή για την απόκριση σε συμβάντα ασφάλειας CSIRT ή CERT, και το εθνικό Ενιαίο Κέντρο Επαφής ή Ε-ΚΑ) και οι βασικές αρμοδιότητές τους, οι οποίες με λεπτομέρεια ορίζονται στα οικεία άρθρα.

Με την παράγραφο 3 αποσαφηνίζεται η εξαίρεση των περιπτώσεων επιχειρήσεων που εμπίπτουν στις προβλέψεις του άρθρου 33 παρ. 1 του ν. 4070/2012 ή σε παρόχους υπηρεσιών εμπιστοσύνης που υπόκεινται στις απαιτήσεις του άρθρου 19 του Κανονισμού (ΕΕ) υπ' αριθ. 910/2014. Η αποσαφήνιση αυτή κρίνεται αναγκαία λόγω της φύσης των υπηρεσιών που προσφέρουν ιδιωτικοί και δημόσιοι φορείς οι οποίοι συχνά εμπίπτουν σε περισσότερους από έναν κανόνες εθνικού ή ενωσιακού δικαίου και, όπως έχει προαναφερθεί στο γενικό μέρος, εφαρμόζεται η Οδηγία μόνο εάν δεν υπάρχει ειδικότερος κανόνας ή άλλος αυστηρότερος κανόνας δικαίου που να ρυθμίζει το ίδιο θέμα.

Η ίδια αρχή, της εφαρμογής του αυστηρότερου κανόνα δικαίου μεταξύ των διατάξεων της Οδηγίας ή του άλλου κανόνα, εάν ήδη αυτός υπάρχει σε ειδική διάταξη ή σε τομεακή πράξη, εφαρμόζεται μέσω των παραγράφων 4, 5, 6, 7, 8 και σε ό, τι αφορά τις διατάξεις της Οδηγίας 2008/114/ΕΚ του Συμβουλίου και των Οδηγιών 2011/93/ΕΕ και 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, του Κανονισμού (ΕΚ) αριθμ. 2016/679 (GDPR) και τον ν. 2472/1997. Με την επιφύλαξη του άρθρου 346 της Συνθήκης Λειτουργίας της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), προστατεύεται το δικαίωμα του κράτους-μέλους να χειρίζεται με ειδικό τρόπο απόρρητες πληροφορίες που αφορούν θέματα εθνικής ασφάλειας και επιχειρηματικού απορρήτου των ΦΕΒΥ, των ΠΨΥ και γενικότερα, ώστε να μεταβιβάζονται μόνο όσες είναι απολύτως απαραίτητες από τον παρόντα νόμο επί τη βάσει των αρχών της συνάφειας και αναλογικότητας οι οποίες διέπουν το σύνολο του παρόντος νόμου, προκειμένου να αποφεύγονται οι συγκρούσεις νόμων και να μην αντίκεινται σε τομεακές ενωσιακές νομικές πράξεις που επιφέρουν τουλάχιστον ισοδύναμα αποτελέσματα στο ίδιο πεδίο. Ο παρών νόμος λειτουργεί συμπληρωματικά και επικουρικά σε ό, τι έχει ήδη ρυθμιστεί ειδικά ή τομεακά.

Άρθρο 2

Με το άρθρο 2 (άρθρο 2 της Οδηγίας) λαμβάνεται μέριμνα για την Προστασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μη θίγονται οι διατάξεις του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ, GDPR), Κανονισμός (ΕΚ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (ΕΕ L 119) και το ν. 2472/1997 (Α΄ 50).

Άρθρο 3
Ορισμοί

Με το άρθρο 3 (άρθρο 4 της Οδηγίας) δίδονται ορισμοί των εννοιών που αναφέρονται στην Οδηγία και στην εθνική νομοθεσία, όπως της έννοιας «σύστημα δικτύου και πληροφοριών», της ασφάλειας αυτών και της εθνικής στρατηγικής για την επίτευξη αυτής της ασφάλειας,

των ΦΕΒΥ, των ψηφιακών υπηρεσιών και των παρόχων τους, των συμβάντων ασφάλειας, του χειρισμού αυτών και των κινδύνων από αυτά, των αντιπροσώπων φορέων, των προτύπων και τεχνικών προδιαγραφών, του σημείου ανταλλαγής κίνησης διαδικτύου (IXP), συστήματος ονομάτων χώρου (DNS), των παρόχων αυτής της υπηρεσίας και των μητρώων αυτής, επιγραμμικής αγοράς και μηχανής αναζήτησης και νεφοϋπολογιστικής. Η παράθεση των ορισμών στο συγκεκριμένο σημείο κρίνεται σκόπιμη τόσο για την ευχέρεια της παρουσίασης των υπόλοιπων άρθρων, όσο και προς αποσαφήνιση του νοήματος κάθε όρου, χωρίς περιττές διευρύνσεις ή εσφαλμένες παραλείψεις κάποιων από αυτούς.

Άρθρο 4
Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών

Με το άρθρο 4 (άρθρο 5 της Οδηγίας) ορίζεται ποιος, σε ποιο πεδίο ευθύνης και με ποιου είδους πράξη δικαίου θα διενεργήσει τον προσδιορισμό των ΦΕΒΥ (παράγραφος 1). Ακολούθως προσδιορίζεται ο τρόπος εργασίας και συνεργασίας των εμπλεκόμενων μερών (παράγραφος 2), τα γενικά κριτήρια χαρακτηρισμού (παράγραφος 3), η περίπτωση προσφοράς διασυνοριακών υπηρεσιών από φορέα (παράγραφος 4) και ο τρόπος υποβολής στην Επιτροπή ανά διετία των στοιχείων που απαιτούνται για την αξιολόγηση της εφαρμογής της Οδηγίας (παράγραφος 5).

Άρθρο 5
Σοβαρή διατάραξη

Με το άρθρο 5 (άρθρο 6 της Οδηγίας) ορίζεται ποιος, σε ποιο πεδίο ευθύνης και με ποιου είδους πράξη δικαίου θα καθορίσει τα κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρή διατάραξη (παράγραφος 1). Ακολούθως, παρατίθενται παράγοντες που πρέπει να ληφθούν υπόψη κατά τον προσδιορισμό της σοβαρότητας της διατάραξης (παράγραφος 2) και λαμβάνεται ειδική μέριμνα (κριτήριο παράγραφος 2ζ), ώστε να μπορούν να προστεθούν και έτερα επιπλέον ειδικά κριτήρια ανά τομέα, όπως προβλέπει άλλωστε και η Οδηγία στο άρθρο 3 αυτής. Σκοπός του νόμου είναι η επίτευξη ενός ελάχιστου επιπέδου εναρμόνισης ενώ στο άρθρο 6 παράγραφος 2 της Οδηγίας ρητά αναφέρεται ότι επαφίεται στην εθνική νομοθεσία η θέσπιση ειδικών κριτηρίων ανά τομέα.

Άρθρο 6
Εθνική στρατηγική Κυβερνοασφάλειας

Με το άρθρο 6 (άρθρο 7 της Οδηγίας) ορίζεται ρητά η Εθνική Αρχή Κυβερνοασφάλειας ως ο φορέας που επικαιροποιεί την Εθνική Στρατηγική Κυβερνοασφάλειας (ΕΣΚ) και προσδιορίζεται γενικά το περιεχόμενό της, το οποίο περιλαμβάνει, τουλάχιστον, τη στοχοθεσία, τα μέτρα πρόληψης, απόκρισης και αποκατάστασης από περιστατικά και τα προγράμματα εκπαίδευσης. Με την ανωτέρω διατύπωση του νόμου καλύπτονται οι απαιτήσεις της Οδηγίας, οι οποίες αφορούν τους τομείς των Παραρτημάτων ΙΙ και ΙΙΙ αυτής, για τους ΦΕΒΥ και ΠΨΥ αντίστοιχα, επιτρέποντας μια ολοκληρωμένη αντιμετώπιση των προβλημάτων του κυβερνοχώρου.

Άρθρο 7
Εθνική Αρχή Κυβερνοασφάλειας

Με το άρθρο 7 (άρθρο 8 της Οδηγίας) ορίζεται ότι η υπηρεσία που αναλαμβάνει τις αρμοδιότητες της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ) είναι η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης (παράγραφος 1). Ακολούθως ορίζεται η ΕΑΚ, ως ο φορέας εφαρμογής του νόμου και αναλαμβάνει και τις αρμοδιότητες του εθνικού Ενιαίου Κέντρου Επαφής (ΕΚΕ), οι οποίες ορίζονται με σαφήνεια τόσο ως προς την επικοινωνία με τους διεθνείς φορείς και αρχές, εντός Ευρωπαϊκής Ένωσης (παράγραφος 4) ή και εκτός αυτής, όσο και ως προς τις εθνικές αρχές και φορείς (παράγραφος 2), ενώ λαμβάνεται μέριμνα για την υλική και θεσμική υποστήριξη του ρόλου αυτού (παράγραφος 3).

Άρθρο 8
Ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)

Με το άρθρο 8 (άρθρο 9 της Οδηγίας) προβλέπεται η αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT ή CERT), τα καθήκοντα, οι αρμοδιότητες και οι υποχρεώσεις της, όπως και ο εφοδιασμός της με τους κατάλληλους πόρους για την επιτέλεση του έργου της. Δεν αποκλείεται από την Οδηγία η παράλληλη άσκηση άλλων καθηκόντων ούτε προβλέπεται υποχρεωτικά ότι είναι μία μόνο αρχή που θα ασκεί αυτές τις αρμοδιότητες, πρόβλεψη που τηρείται και στο νόμο, ο οποίος δεν προβλέπει ασυμβίβαστο με άλλες αρμοδιότητες. Ως αρμόδια ομάδα απόκρισης ορίζεται η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ. Παράλληλα ενσωματώνεται το Παράρτημα Ι της Οδηγίας που περιγράφει τις αρμοδιότητες αυτές (παράγραφοι 2, 3, 4 του παρόντος άρθρου).

Άρθρο 9
Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων

Με το άρθρο 9 (άρθρο 14 της Οδηγίας) καθορίζεται ποια είναι η αρχή που αξιολογεί τα λαμβανόμενα από τους ΦΕΒΥ μέτρα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους (παράγραφος 1). Ακολούθως ορίζονται οι παράμετροι για τον προσδιορισμό αντικτύπου ενός συμβάντος (παράγραφος 2) και η υποχρέωση διασυνοριακών κοινοποιήσεων για συμβάντα που αφορούν και άλλα κράτη-μέλη, αλλά και γενικότερα για την ανταλλαγή πληροφοριών με την επιφύλαξη θεμάτων εθνικού και επιχειρηματικού απορρήτου (παράγραφος 3), επαφιεμένης της ενημέρωσης του ΦΕΒΥ στη διακριτική ευχέρεια της αρχής, ανάλογα με την περίπτωση και τις περιστάσεις. Με ανάλογο σκεπτικό και μετά από διαβούλευση με τον ΦΕΒΥ ενημερώνεται το κοινό, αν είναι αναγκαίο για την πρόληψη ή καταστολή συμβάντος (παράγραφος 4) και προβλέπεται η δυνατότητα της αρχής να εκδίδει εξειδικευμένες συστάσεις για την κοινοποίηση συμβάντων ανάλογα με τις περιστάσεις, λαμβανομένων υπόψη των παραμέτρων της παραγράφου 2 (παράγραφος 5).

Άρθρο 10
Εφαρμογή και επιβολή

Με το άρθρο 10 του νόμου (άρθρο 15 της Οδηγίας) εξουσιοδοτείται η Εθνική Αρχή Κυβερνοασφάλειας να εφαρμόσει και να επιβάλει το νόμο μέσω της αξιολόγησης της συμμόρφωσης των ΦΕΒΥ στις απαιτήσεις του παρόντος νόμου και μέσω της απαίτησης παροχής συγκεκριμένων πληροφοριών ως προς το επίπεδο ασφάλειάς τους, αλλά και ως προς τα αποτελέσματα των επιθεωρήσεων που διενεργήθηκαν από τα αρμόδια όργανα (παράγραφος 1). Επίσης, εξουσιοδοτείται η ΕΑΚ να εκδώσει υποχρεωτικές για τους ΦΕΒΥ οδηγίες συμμόρφωσης μετά την αξιολόγηση των ανωτέρω πληροφοριών (παράγραφος 2), ενώ για θέματα παραβίασης προσωπικών δεδομένων συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (παράγραφος 3). Η Εθνική Αρχή Κυβερνοασφάλειας εισηγείται την έκδοση υπουργικής απόφασης για την εξειδίκευση των ανωτέρω κριτηρίων και της μεθοδολογίας αξιολόγησης (παράγραφος 4).

Άρθρο 11
Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων

Με το άρθρο 11 (άρθρο 16 της Οδηγίας) καθορίζεται η αρμόδια αρχή, η οποία θα αξιολογεί τα λαμβανόμενα από τους ΠΨΥ μέτρα για τη διαχείριση κινδύνων όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους, ο τρόπος διενέργειας για αυτές τις διαδικασίες αξιολόγησης αλλά και κοινοποίησης σοβαρών περιστατικών ασφαλείας (παράγραφος 1). Ακολούθως ορίζονται οι παράμετροι για τον προσδιορισμό του επιπέδου μείωσης των επιπτώσεων από κινδύνους και επιπλέον εξουσιοδοτείται η ΕΑΚ να ελέγχει τα μέτρα που λαμβάνονται προς αυτή την κατεύθυνση. Η αξιολόγηση της σοβαρότητας συμβάντος προβλέπεται να διενεργείται μέσω των παραμέτρων που ορίστηκαν και για τους ΦΕΒΥ (πλήθος επηρεαζόμενων χρηστών, διάρκεια και γεωγραφικό εύρος) με δυο επιπλέον παραμέτρους για τους ΠΨΥ που αφορούν το μέγεθος διατάραξης της υπηρεσίας του ΠΨΥ και τις οικονομικές επιπτώσεις. Η υποχρεωτικότητα κοινοποίησης εξαρτάται από το εάν και κατά πόσον έχουν πρόσβαση στις απαιτούμενες πληροφορίες οι ΠΨΥ (παράγραφος 2). Σε περίπτωση εξάρτησης ενός ΠΨΥ από τρίτο φορέα για την παροχή υπηρεσίας του, κοινοποιείται από τον τρίτο φορέα το συμβάν που διαταράσσει την παροχή υπηρεσίας. Οι κοινοποιήσεις πάντα αφορούν περιπτώσεις όπου επηρεάζονται τομείς του Παραρτήματος ΙΙ (παράγραφος 3). Για διασυνοριακά συμβάντα ακολουθούνται οι ίδιες αρχές, όπως στην περίπτωση των ΦΕΒΥ ως προς την ενημέρωση των άλλων κρατών (παράγραφος 4) και του κοινού (παράγραφος 5). Ειδικά για τους ΠΨΥ δεν επιβάλλονται επιπλέον υποχρεώσεις ασφάλειας ή κοινοποίησης (παράγραφος 6), ενώ εξαιρούνται από το νόμο οι πολύ μικρές και οι μικρές επιχειρήσεις κατά την σύσταση 2003/361/ΕΚ της Επιτροπής (παράγραφος 7).

Άρθρο 12
Εφαρμογή και επιβολή

Με το άρθρο 12 του νόμου (άρθρο 17 της Οδηγίας) εξουσιοδοτείται η ΕΑΚ να εφαρμόσει και επιβάλλει το νόμο μέσω της λήψης εποπτικών μέτρων επί ενός ΠΨΥ, όταν ληφθεί πληροφορία περί μη συμμόρφωσής του στις απαιτήσεις του άρθρου 10 και να απαιτήσει τις σχετικές πληροφορίες και τη διόρθωση ελλείψεων (παράγραφος 1). Σε περίπτωση παροχής υπηρεσιών σε πολλά κράτημέλη οι αρμόδιες αρχές συνεργάζονται (παράγραφος 2) ανταλλάσσοντας πληροφορίες. Επίσης, καθορίζεται η κανονιστική πράξη με την οποία θα ορισθούν οι αναγκαίες λεπτομέρειες για την εφαρμογή των ανωτέρω (υπουργική πράξη με εισήγηση της ΕΑΚ).

Άρθρο 13
Δικαιοδοσία και εδαφικότητα

Με το άρθρο 13 (άρθρο 18 της Οδηγίας) ρυθμίζονται θέματα δικαιοδοσίας και εδαφικότητας για τους ΠΨΥ, ώστε να αποσαφηνίζονται πλήρως οι περιπτώσεις στις οποίες οι ελληνικές αρχές έχουν αρμοδιότητα ως προς τα αντικείμενα του παρόντος νόμου. Ορίζεται ότι ως κύρια εγκατάστασή φορέα ΠΨΥ θεωρείται η έδρα του και η αρμοδιότητα ανήκει στις αρχές του κράτους-μέλους εντός του οποίου αυτή βρίσκεται. Κατά συνέπεια οι ΠΨΥ που έχουν έδρα στην Ελλάδα θεωρείται ότι έχουν την κύρια εγκατάστασή τους στη χώρα και αρμόδιες αρχές είναι οι ελληνικές (παράγραφος 1). Ένας ΠΨΥ που δεν είναι εγκατεστημένος στην Ένωση αλλά προσφέρει υπηρεσίες του Παραρτήματος ΙΙ του νόμου (Παράρτημα ΙΙΙ της Οδηγίας) εντός αυτής, ορίζει υποχρεωτικά αντιπρόσωπο, ο οποίος πρέπει να βρίσκεται οπωσδήποτε σε κάποιο κράτος-μέλος από εκείνα στα οποία προσφέρει υπηρεσίες, υποκείμενος στη δικαιοδοσία αυτού του κράτους-μέλους (παράγραφος 2). Παρά τον ορισμό αντιπροσώπου προβλέπεται ρητά ότι δεν μεταβάλλονται οι υποχρεώσεις γενικά του ΠΨΥ έναντι της διεθνούς νομοθεσίας ή των εθνικών νομικών τάξεων (παράγραφος 3).

Άρθρο 14
Εθελούσια κοινοποίηση

Με το άρθρο 14 (άρθρο 20 της Οδηγίας) προβλέπεται η δυνατότητα εθελούσιας κοινοποίησης συμβάντων ασφάλειας από φορείς οι οποίοι δεν έχουν χαρακτηριστεί ως ΦΕΒΥ ούτε ως ΠΨΥ, προκειμένου να διευκολυνθούν οι αρμόδιες υπηρεσίες στο έργο τους για την πρόληψη και καταστολή γενικότερων κινδύνων (παράγραφος 1). Η επεξεργασία όμως των πληροφοριών αυτών προτεραιοποιείται ανάλογα με το φόρτο εργασίας της αρμόδιας υπηρεσίας και με την αξιολόγηση της σοβαρότητας του περιστατικού από αυτή, διαθέτοντας τη διακριτική ευχέρεια πρόταξης των υποχρεωτικών κοινοποιήσεων. Επιπλέον ρητά αναφέρεται ότι η επεξεργασία των εθελούσιων κοινοποιήσεων δεν είναι υποχρεωτική αν συνιστά δυσανάλογη ή υπέρμετρη επιβάρυνση για τους κρατικούς φορείς (παράγραφος 2).

Άρθρο 15
Κυρώσεις

Με το άρθρο 15 (άρθρο 21 της Οδηγίας) ορίζεται το γενικό πλαίσιο επιβολής κυρώσεων για τους σκοπούς του παρόντος νόμου, λαμβανομένης υπόψη της αρχής της αναλογικότητας. Ειδικότερα ορίζεται η αρχή που επιβάλλει τις κυρώσεις (Υπουργός Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης μετά από εισήγηση

της ΕΑΚ) σε φυσικό ή νομικό πρόσωπο, για παραβάσεις του νόμου από ΦΕΒΥ ή ΠΨΥ. Οι κυρώσεις αφορούν τόσο τη μη έγκαιρη κοινοποίηση συμβάντων ασφάλειας και τη λήψη μέτρων όσο και την παροχή πληροφοριών κατά τους ελέγχους. Είναι κλιμακούμενες ώστε να ενθαρρύνεται ο παραβάτης να συμμορφώνεται με τις υποδείξεις των αρμοδίων αρχών και ορίζονται μέχρι τις 15.000 ευρώ, ενώ φτάνουν έως και τα 200.000 ευρώ σε περίπτωση υποτροπής ή υποτροπών, σε ό, τι αφορά την υποχρέωση κοινοποίησης. Για τη μη λήψη κατάλληλων μέτρων ή για τη μη παροχή πληροφοριών ανέρχονται μέχρι του ποσού των 50.000 ευρώ, ενώ φτάνουν έως και τα 200.000 ευρώ σε περίπτωση υποτροπής ή υποτροπών (παράγραφος 1). Για λόγους χρηστής διοίκησης ενημερώνεται ο ενδιαφερόμενος, τουλάχιστον πέντε (5) ημέρες πριν την επιβολή, ώστε να αντιτάξει τους ισχυρισμούς του. Η απόφαση πρέπει να είναι γραπτή και αιτιολογημένη, ενώ αναρτάται στον ιστότοπο της ΕΑΚ για λόγους διαφάνειας και κοινοποιείται στον ενδιαφερόμενο. Τα ποσά θα εισπράττονται μέσω των διατάξεων του Κώδικα Είσπραξης Δημοσίων Εσόδων (ΚΕΔΕ) για λογαριασμό του Δημοσίου (παράγραφος 2).

Άρθρο 16

Με το άρθρο 16 διασφαλίζεται η συνεκτικότητα του νόμου με τα Παραρτήματα Ι και ΙΙ που τον συνοδεύουν τα οποία είναι απαραίτητα για την εφαρμογή του.

Άρθρο 17
Έναρξη ισχύος

Με το άρθρο 17 ορίζεται η έναρξη ισχύος του νόμου από τη δημοσίευση στην Εφημερίδα της Κυβερνήσεως, εκτός των διατάξεων που ρητά αναφέρεται σε αυτές άλλη ημερομηνία έναρξης ισχύος.

Αθήνα, 12 Νοεμβρίου 2018

ΟΙ ΥΠΟΥΡΓΟΙ

| | |
|---|---|
| ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ | ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ |
| Ν. Παππάς | Π. Καμμένος |

ΔΙΚΑΙΟΣΥΝΗΣ, ΔΙΑΦΑΝΕΙΑΣ
ΚΑΙ ΑΝΘΡΩΠΙΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Μ. Καλογήρου

**ΣΧΕΔΙΟ ΝΟΜΟΥ**

***Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση***

**ΚΕΦΑΛΑΙΟ Α΄**
**ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ**

**Άρθρο 1**
**Αντικείμενο και πεδίο εφαρμογής**
**(άρθρο 1 παράγραφοι 1, 3, 4, 5, 6, 7 της Οδηγίας 2016/1148/ΕΕ)**

1. Σκοπός του παρόντος είναι η ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194), με την οποία θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

2. Οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται στον παρόντα νόμο δεν εφαρμόζονται σε επιχειρήσεις που πληρούν τις προϋποθέσεις της παρ. 1 του άρθρου 33 του ν. 4070/2012 (Α΄ 82) ή σε παρόχους υπηρεσιών εμπιστοσύνης που εμπίπτουν στο άρθρο 19 του Κανονισμού (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 (ΕΕ L 257).

3. Ο παρών νόμος εφαρμόζεται με την επιφύλαξη των διατάξεων του π.δ. 39/2011 (Α΄ 104) και των νόμων 4267/2014 (Α΄ 137) και 4360/2016 (Α΄ 9).

4. Με την επιφύλαξη του άρθρου 346 της Συνθήκης Λειτουργίας της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), πληροφορίες που είναι απόρρητες σύμφωνα με ενωσιακούς και εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές, μόνον εφόσον η ανταλλαγή αυτή είναι αναγκαία για την εφαρμογή του παρόντος. Οι πληροφορίες, που ανταλλάσσονται, περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς το σκοπό της ανταλλαγής αυτής. Η εν λόγω ανταλλαγή πληροφοριών διαφυλάσσει το απόρρητο αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών.

5. Με τον παρόντα δεν θίγονται τα μέτρα που λαμβάνει η χώρα μας για τη διαφύλαξη των ουσιωδών κρατικών λειτουργιών και ιδίως για τη διαφύλαξη της εθνικής ασφάλειας, συμπεριλαμβανομένων των μέτρων για την προστασία πληροφοριών, των οποίων η διάδοση θεωρείται αντίθετη προς τα ουσιώδη συμφέροντα ασφάλειας, καθώς και για τη διατήρηση του νόμου και της τάξης και ιδίως για τη διευκόλυνση της διερεύνησης, της ανίχνευσης και της δίωξης ποινικών αδικημάτων.

6. Αν μία τομεακή νομική πράξη της Ευρωπαϊκής Ένωσης απαιτεί από τους φορείς εκμετάλλευσης βασικών υ-

πηρεσιών ή τους παρόχους ψηφιακών υπηρεσιών είτε να εξασφαλίζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους είτε να κοινοποιούν συμβάντα, εφαρμόζονται οι διατάξεις της εν λόγω τομεακής νομικής πράξης, υπό την προϋπόθεση ότι οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που θεσπίζονται στον παρόντα νόμο.

**Άρθρο 2**
**(Άρθρο 2 της Οδηγίας 2016/1148/ΕΕ)**

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, που γίνεται κατά τον παρόντα νόμο, διενεργείται σύμφωνα με τον Κανονισμό (ΕΚ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (ΕΕ L 119) και το ν. 2472/1997 (Α΄ 50).

**Άρθρο 3**
**Ορισμοί**
**(Άρθρο 4 της Οδηγίας 2016/1148/ΕΕ)**

Για τους σκοπούς του παρόντος νόμου, ισχύουν οι εξής ορισμοί:

1) «σύστημα δικτύου και πληροφοριών»:

α) ένα δίκτυο ηλεκτρονικών επικοινωνιών, σύμφωνα με την περίπτωση ιζ΄ της Ενότητας Α΄παράγραφος του άρθρου 2 του ν. 4070/2012,

β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων,

γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στις περιπτώσεις α΄ και β΄ για τους σκοπούς της λειτουργίας, της χρήσης, της προστασίας και της συντήρησής τους,

2) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, με δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών,

3) «εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών»: πλαίσιο το οποίο παρέχει στρατηγικούς στόχους και προτεραιότητες για την ασφάλεια συστημάτων δικτύου και πληροφοριών σε εθνικό επίπεδο,

4) «φορέας εκμετάλλευσης βασικών υπηρεσιών»: δημόσια ή ιδιωτική οντότητα είδους αναφερόμενου στο Παράρτημα Ι, η οποία πληροί τα κριτήρια που ορίζονται στην παράγραφο 2 του άρθρου 4,

5) «ψηφιακή υπηρεσία»: υπηρεσία σύμφωνα με την περίπτωση β΄ της παρ. 1 του άρθρου 2 του π.δ. 81/2018 (Α΄151), η οποία είναι είδος αναφερόμενο στο Παράρτημα ΙΙ,

6) «πάροχος ψηφιακών υπηρεσιών»: νομικό πρόσωπο που παρέχει ψηφιακή υπηρεσία,

7) «συμβάν»: κάθε γεγονός που έχει στην πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών,

8) «χειρισμός συμβάντων»: το σύνολο των διαδικασιών που υποστηρίζουν τον εντοπισμό, την ανάλυση και την ανάσχεση ενός συμβάντος, καθώς και την παρέμβαση για την αντιμετώπισή του,

9) «κίνδυνος»: κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός με ενδεχομένως δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών,

10) «αντιπρόσωπος»: κάθε φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ευρωπαϊκή Ένωση, που ρητώς έχει οριστεί να ενεργεί εξ ονόματος παρόχου ψηφιακών υπηρεσιών μη εγκατεστημένου στην Ευρωπαϊκή Ένωση, στο οποίο μπορεί να απευθύνεται η εθνική αρμόδια αρχή ή η Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT) του άρθρου 8 παράγραφος 1 αντί του παρόχου ψηφιακών υπηρεσιών, όσον αφορά τις υποχρεώσεις αυτού σύμφωνα με τον παρόντα νόμο,

11) «πρότυπο»: πρότυπο σύμφωνα με το σημείο 1 του άρθρου 2 του Κανονισμού (ΕΕ) 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2012 (ΕΕ L 316),

12) «προδιαγραφή»: τεχνική προδιαγραφή σύμφωνα με το σημείο 4 του άρθρου 2 του Κανονισμού (ΕΕ) 1025/2012,

13) «σημείο ανταλλαγής κίνησης διαδικτύου (Internet Exchange Point - IXP)»: δικτυακή υποδομή που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων αυτόνομων συστημάτων, κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης διαδικτύου, και η οποία διασυνδέει μόνον αυτόνομα συστήματα. Το IXP δεν αναγκάζει την κίνηση διαδικτύου που διέρχεται μεταξύ ζεύγους συμμετεχόντων αυτόνομων συστημάτων να διέλθει από τρίτο αυτόνομο σύστημα ούτε την τροποποιεί ούτε παρεμβαίνει με άλλον τρόπο σε αυτήν,

14) «σύστημα ονομάτων χώρου (Domain Name System - DNS)»: ιεραρχικά κατανεμημένο σύστημα ονοματοδοσίας εντός ενός δικτύου, το οποίο εκτελεί παραπομπές αιτημάτων για ονόματα τομέων,

15) «πάροχος υπηρεσιών συστήματος ονομάτων χώρου»: οντότητα που παρέχει υπηρεσίες συστήματος ονομάτων χώρου στο διαδίκτυο,

16) «μητρώο ονομάτων χώρου ανώτατου επιπέδου» (top-level domain name registry): οντότητα που διαχειρίζεται και εκμεταλλεύεται την καταχώριση ονομάτων διαδικτυακών χώρων εντός συγκεκριμένου χώρου ανώτατου επιπέδου (TLD),

17) «επιγραμμική αγορά» (online marketplace): ψηφιακή υπηρεσία που επιτρέπει σε καταναλωτές ή και εμπόρους, όπως ορίζονται στις περιπτώσεις α΄ και β΄ της παρ. 1 του άρθρου 4 της 70330οικ./30.6.2015 κοινής απόφασης των Υπουργών Οικονομίας, Υποδομών, Ναυτιλίας και Τουρισμού και Δικαιοσύνης, Διαφάνειας και Ανθρώπινων Δικαιωμάτων (Β΄ 1421), να συνάπτουν επιγραμμικές συμβάσεις πώλησης ή παροχής υπηρεσιών με εμπόρους είτε στον ιστοχώρο της επιγραμμικής αγοράς είτε σε ιστοχώρο εμπόρου που χρησιμοποιεί υπηρεσίες υπολογιστικής παρεχόμενες από την επιγραμμική αγορά,

18) «επιγραμμική μηχανή αναζήτησης» (online search engine): ψηφιακή υπηρεσία που επιτρέπει στους χρήστες να εκτελούν αναζητήσεις καταρχήν σε όλους τους ιστοχώρους ή σε ιστοχώρους συγκεκριμένης γλώσσας βάσει ερωτήματος για οποιοδήποτε θέμα, με τη μορφή λέξης-κλειδιού, φράσης ή άλλων δεδομένων, και επιστρέφει

ως αποτέλεσμα συνδέσμους όπου μπορεί κανείς να βρει πληροφορίες σχετικές με το περιεχόμενο που έχει ζητηθεί,

19) «υπηρεσία νεφοϋπολογιστικής»: ψηφιακή υπηρεσία που επιτρέπει την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων.

**Άρθρο 4**
**Φορείς εκμετάλλευσης βασικών υπηρεσιών**
**(Άρθρο 5 της Οδηγίας 2016/1148/ΕΕ)**

1. Η Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7, σε συνεργασία με τις ανά τομέα βασικής υπηρεσίας αρμόδιες ρυθμιστικές/εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς, προσδιορίζει, για κάθε τομέα και υποτομέα του Παραρτήματος Ι, τους φορείς εκμετάλλευσης βασικών υπηρεσιών που είναι εγκατεστημένοι στην Ελληνική Επικράτεια.

Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, ορίζονται οι φορείς εκμετάλλευσης βασικών υπηρεσιών.

2. Τα κριτήρια για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών της περίπτωσης 4 του άρθρου 3 είναι τα εξής:

α) ο φορέας να παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών ή και οικονομικών δραστηριοτήτων,

β) η παροχή της υπηρεσίας αυτής να στηρίζεται σε συστήματα δικτύου και πληροφοριών και

γ) η πρόκληση σοβαρής διατάραξης της παροχής της εν λόγω υπηρεσίας, κατά τα οριζόμενα στο άρθρο 5, από τυχόν συμβάν.

3. Για τους σκοπούς της παραγράφου 1, η Εθνική Αρχή Κυβερνοασφάλειας καταρτίζει κατάλογο τόσο των βασικών υπηρεσιών όσο και των φορέων εκμετάλλευσής τους. Οι κατάλογοι αυτοί επανεξετάζονται σε τακτική βάση, τουλάχιστον ανά διετία και, εφόσον κριθεί αναγκαίο, επικαιροποιούνται.

4. Για τους σκοπούς της παραγράφου 1, όταν φορέας εκμετάλλευσης βασικών υπηρεσιών παρέχει και σε άλλο ή άλλα κράτη-μέλη της ΕΕ υπηρεσία που αναφέρεται στην παράγραφο 2, η Εθνική Αρχή Κυβερνοασφάλειας διαβουλεύεται με τις αντίστοιχες αρχές του ή των άλλων κρατών-μελών πριν από τη λήψη απόφασης για τον προσδιορισμό του.

5. Η Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7 υποβάλλει στην Επιτροπή ανά διετία τις πληροφορίες που είναι αναγκαίες για την αξιολόγηση της εφαρμογής της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο. Στις πληροφορίες αυτές περιλαμβάνονται τουλάχιστον τα εξής:

α) τα εθνικά κριτήρια βάσει των οποίων προσδιορίζονται οι φορείς εκμετάλλευσης βασικών υπηρεσιών,

β) ο κατάλογος των υπηρεσιών που αναφέρεται στην παράγραφο 3,

γ) ο αριθμός των φορέων εκμετάλλευσης βασικών υπηρεσιών που έχουν προσδιοριστεί για κάθε τομέα του Παραρτήματος Ι και αναφορά της σημασίας τους σε σχέση με τον εν λόγω τομέα,

δ) τα κατώτατα όρια, εφόσον υπάρχουν, για τον προσδιορισμό του σχετικού επιπέδου παροχής υπηρεσιών με αναφορά στον αριθμό των χρηστών που εξαρτώνται από την υπηρεσία αυτή, όπως αναφέρεται στην περίπτωση α΄ της παραγράφου 2 του άρθρου 5, ή της σημασίας του συγκεκριμένου φορέα εκμετάλλευσης βασικών υπηρεσιών, όπως αναφέρεται στην περίπτωση στ΄ της παραγράφου 2 του άρθρου 5.

**Άρθρο 5**
**Σοβαρή διατάραξη**
**(Άρθρο 6 της Οδηγίας 2016/1148/ΕΕ)**

1. Η Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7 σε συνεργασία με τις, ανά τομέα βασικής υπηρεσίας, αρμόδιες ρυθμιστικές ή εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς, καθορίζει τα κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης.

2. Κατά τον προσδιορισμό της σοβαρότητας της διατάραξης που αναφέρεται στην περίπτωση γ΄ της παραγράφου 2 του άρθρου 4 λαμβάνονται υπόψη τουλάχιστον οι εξής παράγοντες:

α) ο αριθμός των χρηστών που εξαρτώνται από την υπηρεσία, η οποία παρέχεται από τον οικείο φορέα εκμετάλλευσης,

β) η εξάρτηση άλλων τομέων που αναφέρονται στο Παράρτημα Ι από την υπηρεσία που παρέχεται από τον εν λόγω φορέα εκμετάλλευσης,

γ) ο αντίκτυπος που θα μπορούσαν να έχουν τα συγκεκριμένα περιστατικά διατάραξης, από άποψη βαθμού και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες ή στη δημόσια ασφάλεια,

δ) το μερίδιο αγοράς του οικείου φορέα εκμετάλλευσης,

ε) το γεωγραφικό εύρος της περιοχής που θα μπορούσε να επηρεαστεί από ένα περιστατικό,

στ) η σημασία του εν λόγω φορέα για τη διατήρηση επαρκούς επιπέδου της υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω υπηρεσίας,

ζ) οι ειδικότεροι παράγοντες που αφορούν το συγκεκριμένο τομέα.

**ΚΕΦΑΛΑΙΟ Β΄**
**ΕΘΝΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ**

**Άρθρο 6**
**Εθνική Στρατηγική Κυβερνοασφάλειας**
**(Άρθρο 7 της Οδηγίας 2016/1148/ΕΕ)**

1. Η Εθνική Αρχή Κυβερνοασφάλειας επικαιροποιεί την «Εθνική Στρατηγική Κυβερνοασφάλειας» που έχει εγκριθεί με την υ.α. 3218/2018 του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω) και την κοινοποιεί στην Επιτροπή μέσα σε τρεις (3) μήνες από την έγκρισή της από τον Υπουργό Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης.

Από την κοινοποίηση αυτή εξαιρούνται στοιχεία της στρατηγικής που συνδέονται με την εθνική ασφάλεια. Η

Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο των αρμοδιοτήτων της και για τις ανάγκες της παραγράφου αυτής, μπορεί να συνεργάζεται με τις αρμόδιες ρυθμιστικές/εποπτικές αρχές και τους λοιπούς εμπλεκόμενους εθνικούς φορείς.

2. Η Εθνική Στρατηγική Κυβερνοασφάλειας, η οποία αποτελεί την εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών, περιλαμβάνει τα εξής:

α) τους στόχους και τις προτεραιότητες της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών,

β) το πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύων και πληροφοριών, συμπεριλαμβανομένων του ρόλου και των αρμοδιοτήτων των κυβερνητικών οργάνων και των λοιπών αρμόδιων φορέων,

γ) τον προσδιορισμό των μέτρων ετοιμότητας, απόκρισης και αποκατάστασης, συμπεριλαμβανομένης της συνεργασίας ανάμεσα στο δημόσιο και ιδιωτικό τομέα,

δ) αναφορά των προγραμμάτων εκπαίδευσης, ευαισθητοποίησης και κατάρτισης σε σχέση με την εθνική στρατηγική ασφάλειας δικτύων και συστημάτων πληροφοριών,

ε) αναφορά των σχεδίων έρευνας και ανάπτυξης σχετικά με την εθνική στρατηγική ασφάλειας συστημάτων δικτύου και πληροφοριών,

στ) σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό κινδύνων,

ζ) κατάλογο των διαφόρων φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας συστημάτων δικτύου και πληροφοριών.

**Άρθρο 7**
**Εθνική Αρχή Κυβερνοασφάλειας**
**(Άρθρο 8 της Οδηγίας 2016/1148/ΕΕ)**

1. Ως Εθνική Αρμόδια Αρχή για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, εφεξής «Αρμόδια Αρχή» ή «Εθνική Αρχή Κυβερνοασφάλειας», ορίζεται η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (άρθρο 15 του π.δ. 82/2017, Α΄ 117). Η Εθνική Αρχή καλύπτει τους τομείς που αναφέρονται στο Παράρτημα Ι και τις υπηρεσίες που αναφέρονται στο Παράρτημα ΙΙ.

2. Η Εθνική Αρχή Κυβερνοασφάλειας:

α) παρακολουθεί την εφαρμογή του παρόντος,

β) ορίζεται ως το εθνικό ενιαίο κέντρο επαφής, εφεξής «Ενιαίο Κέντρο Επαφής», για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ασκώντας καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών-μελών, καθώς και με τις Αρμόδιες Αρχές άλλων κρατών-μελών στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται στα άρθρα 11 και 12 της Οδηγίας που ενσωματώνεται με τον παρόντα,

γ) ως ενιαίο κέντρο επαφής υποβάλλει ετησίως στην ομάδα συνεργασίας του άρθρου 11 της ανωτέρω Οδηγίας, συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει, συμπεριλαμβανομένου του αριθμού των κοινοποιήσεων και της φύσης των κοινοποιημένων συμβάντων, καθώς και τα μέτρα που έχουν ληφθεί σύμφωνα με τα άρθρα 9 και 11,

δ) συνεργάζεται με την αρμόδια CSIRT της παραγράφου 1 του άρθρου 8, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του παρόντος νόμου,

ε) διαβουλεύεται και συνεργάζεται με τις Αρμόδιες Εθνικές Αρχές επιβολής του νόμου, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), καθώς και τις λοιπές αρμόδιες ρυθμιστικές ή εποπτικές αρχές και τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τα θέματα που άπτονται της εφαρμογής του παρόντος,

στ) συνεργάζεται με τις Αρμόδιες Αρχές των λοιπών κρατών-μελών, στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται στα άρθρα 11 και 12 της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο,

ζ) συμμετέχει στην ομάδα συνεργασίας του άρθρου 11 της ως άνω Οδηγίας, ορίζει τους εθνικούς αντιπροσώπους της χώρας σ΄ αυτήν και ενημερώνει τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τις εργασίες και τις αποφάσεις που λαμβάνονται στο πλαίσιο αυτής,

η) συνεργάζεται με σχετικούς με θέματα κυβερνοασφάλειας και προστασίας κρίσιμων υποδομών διεθνείς οργανισμούς και όργανα ή υπηρεσίες της Ευρωπαϊκής Ένωσης ή άλλων κρατών και συμμετέχει στις αντίστοιχες συναντήσεις συναφών με τα ανωτέρω, επιτροπών και ομάδων εργασίας.

3. Ο ορισμός της Αρμόδιας Αρχής και του ενιαίου κέντρου επαφής, τα καθήκοντά τους, καθώς και κάθε μεταγενέστερη σχετική τροποποίηση δημοσιοποιούνται και κοινοποιούνται, χωρίς καθυστέρηση, στην Επιτροπή.

**Άρθρο 8**
**Ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)**
**(Άρθρο 9 της Οδηγίας 2016/1148/ΕΕ)**

1. Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team – CSIRT εφεξής «αρμόδια CSIRT»), η οποία καλύπτει τους τομείς του Παραρτήματος Ι και τις υπηρεσίες του Παραρτήματος ΙΙ του παρόντος, και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, είναι η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ.

2. Η αρμόδια CSIRT:

α) εξασφαλίζει υψηλό επίπεδο διαθεσιμότητας των υπηρεσιών επικοινωνιών της, αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτει διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. Επιπλέον, οι δίαυλοι επικοινωνίας είναι σαφώς προσδιορισμένοι και ευρύτερα γνωστοί στα μέλη της περιοχής ευθύνης και τους συνεργαζόμενους εταίρους,

β) τα γραφεία της και τα υποστηρικτικά συστήματα πληροφοριών εγκαθίστανται σε ασφαλείς χώρους,

γ) αναφορικά με τη συνέχεια της επιχειρησιακής δραστηριότητάς της, η αρμόδια CSIRT:

αα) είναι εφοδιασμένη με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, προκειμένου να διευκολύνεται η παράδοση καθηκόντων,

ββ) είναι επαρκώς στελεχωμένη ώστε να εξασφαλίζεται η διαθεσιμότητα ανά πάσα στιγμή,

γγ) βασίζεται σε υποδομή, η συνέχεια της οποίας είναι

διασφαλισμένη. Για τον σκοπό αυτό, διατίθενται πλεονάζοντα συστήματα και εφεδρικοί χώροι εργασίας,

δ) συμμετέχει σε διεθνή δίκτυα συνεργασίας.

3. Οι αρμοδιότητες της αρμόδιας CSIRT είναι οι εξής:

α) η παρακολούθηση συμβάντων σε εθνικό επίπεδο,

β) η παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων επαγρύπνησης και ανακοινώσεων, καθώς και η διάδοση πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους και συμβάντα,

γ) η παρέμβαση σε περίπτωση συμβάντος,

δ) η παροχή δυναμικής ανάλυσης κινδύνων και συμβάντων, καθώς και η επίγνωση της κατάστασης,

ε) η συμμετοχή στο δίκτυο CSIRT και η συνεργασία με τις αντίστοιχες υπηρεσίες των υπόλοιπων κρατών – μελών στο πλαίσιο του δικτύου CSIRT του άρθρου 12 της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο,

στ) η λήψη των κοινοποιήσεων συμβάντων που υποβάλλονται σύμφωνα με τον παρόντα νόμο,

ζ) η ενημέρωση του Εθνικού Ενιαίου Κέντρου Επαφής της περίπτωσης β΄ της παραγράφου 2 του άρθρου 7, σχετικά με τις κοινοποιήσεις των συμβάντων που υποβάλλονται σύμφωνα με τον παρόντα νόμο,

η) η εγκαθίδρυση σχέσεων συνεργασίας με τον ιδιωτικό τομέα,

θ ) η προώθηση, η υιοθέτηση και η χρήση κοινών ή τυποποιημένων πρακτικών για:

αα) τις διαδικασίες χειρισμού συμβάντων και κινδύνων,

ββ) τα συστήματα ταξινόμησης συμβάντων, κινδύνων και πληροφοριών.

4. Συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του παρόντος.

## ΚΕΦΑΛΑΙΟ Γ΄
## ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΩΝ ΦΟΡΕΩΝ ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΒΑΣΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

### Άρθρο 9
### Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων (Άρθρο 14 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς, ανά τομέα βασικής υπηρεσίας, εμπλεκόμενους φορείς:

α) αξιολογεί τα τεχνικά και οργανωτικά μέτρα που λαμβάνουν οι φορείς εκμετάλλευσης βασικών υπηρεσιών για τη διαχείριση των κινδύνων που αφορούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους, ως προς την καταλληλότητα και την αναλογικότητά τους,

β) αξιολογεί την καταλληλότητα των μέτρων που λαμβάνουν οι φορείς εκμετάλλευσης βασικών υπηρεσιών για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειάς τους,

γ) καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν οι φορείς εκμετάλλευσης βασικών υπηρεσιών, προκειμένου να κοινοποιήσουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT συμβάντα με σοβαρές επιπτώσεις στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών που αυτοί παρέχουν. Οι ανωτέρω κοινοποιήσεις εκ μέρους των φορέων εκμετάλλευσης βασικών υπηρεσιών πρέπει να πραγματοποιούνται χωρίς αδικαιολόγητη καθυστέρηση και να περιλαμβάνουν πληροφορίες που να επιτρέπουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT να προσδιορίσουν τόσο τη σοβαρότητα όσο και τις διασυνοριακές επιπτώσεις, λόγω του κοινοποιούμενου περιστατικού. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα.

2. Για να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος, λαμβάνονται υπόψη ειδικότερα οι εξής παράμετροι:

α) ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας,

β) η διάρκεια του συμβάντος,

γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν.

3. Βάσει των πληροφοριών που παρέχονται στην κοινοποίηση από το φορέα εκμετάλλευσης βασικών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας ενημερώνει το ή τα άλλα επηρεαζόμενα κράτη-μέλη, εφόσον το κοινοποιούμενο συμβάν έχει σοβαρό αντίκτυπο στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών στο εν λόγω κράτος-μέλος. Στο πλαίσιο της ανωτέρω ενημέρωσης, διαφυλάσσεται, σύμφωνα με το ενωσιακό δίκαιο ή με την εθνική νομοθεσία, η ασφάλεια και τα εμπορικά συμφέροντα του κοινοποιούντος φορέα εκμετάλλευσης βασικών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί στην κοινοποίησή του.

Όταν οι περιστάσεις το επιτρέπουν, η Εθνική Αρχή Κυβερνοασφάλειας ή η αρμόδια CSIRT παρέχει στον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών πληροφορίες όσον αφορά τις ενέργειες που έλαβαν χώρα σε συνέχεια της κοινοποίησής του, όπως πληροφορίες που θα μπορούσαν να υποστηρίξουν την αποτελεσματική διαχείριση του περιστατικού.

Μετά από αίτηση της αρμόδιας αρχής ή του CSIRT, το ενιαίο κέντρο επαφής διαβιβάζει τις κοινοποιήσεις συμβάντων που αναφέρονται στο πρώτο εδάφιο της παρούσας στα ενιαία κέντρα επαφής των άλλων επηρεαζόμενων κρατών-μελών.

4. Ύστερα από διαβούλευση με τον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να ενημερώνει το κοινό σχετικά με μεμονωμένα συμβάντα, αν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη μελλοντικού συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη.

5. Η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να καταρτίζει και να εκδίδει κατευθυντήριες γραμμές σχετικά με τις περιστάσεις υπό τις οποίες οι φορείς εκμετάλλευσης βασικών υπηρεσιών είναι υποχρεωμένοι να κοινοποιούν συμβάντα, συμπεριλαμβανομένων μεταξύ άλλων των παραμέτρων που προσδιορίζουν τη σοβαρότητα των επιπτώσεων ενός συμβάντος, όπως αυτές αναφέρονται στην παράγραφο 2.

**Άρθρο 10**
**Εφαρμογή και επιβολή**
**(Άρθρο 15 της Οδηγίας 2016/1148/ΕΕ)**

1. Η Εθνική Αρχή Κυβερνοασφάλειας:

α) αξιολογεί τη συμμόρφωση των φορέων εκμετάλλευσης βασικών υπηρεσιών προς τις υποχρεώσεις τους, σύμφωνα με το άρθρο 9 και των επιπτώσεών τους στην ασφάλεια των συστημάτων δικτύου και πληροφοριών,

β) απαιτεί από τους φορείς εκμετάλλευσης βασικών υπηρεσιών να παρέχουν:

αα) τις απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων δικτύου και των πληροφοριών τους, συμπεριλαμβανομένων, μεταξύ άλλων, τεκμηριωμένων και εγκεκριμένων πολιτικών ασφάλειας,

ββ) στοιχεία που να αποδεικνύουν την ουσιαστική εφαρμογή πολιτικών ασφάλειας, όπως τα αποτελέσματα επιθεώρησης ασφάλειας που έχει διενεργηθεί είτε από την Εθνική Αρχή Κυβερνοασφάλειας είτε από εξουσιοδοτημένο από αυτήν όργανο και, στη δεύτερη αυτή περίπτωση, να θέτουν τα αποτελέσματά τους, καθώς και όλα τα σχετικά στοιχεία στη διάθεση της Εθνικής Αρχής Κυβερνοασφάλειας.

Όταν ζητούνται αυτές οι πληροφορίες ή τα στοιχεία, η Εθνική Αρχή Κυβερνοασφάλειας δηλώνει τον σκοπό του αιτήματος και προσδιορίζει τις ειδικότερες πληροφορίες που ζητούνται.

2. Μετά την αξιολόγηση των πληροφοριών ή των αποτελεσμάτων των επιθεωρήσεων ασφάλειας που αναφέρονται στην περίπτωση β΄ της παραγράφου 1, η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να εκδίδει δεσμευτικές οδηγίες προς τους φορείς εκμετάλλευσης βασικών υπηρεσιών για την αποκατάσταση των εντοπισμένων ελλείψεων.

3. Κατά την αντιμετώπιση συμβάντων που οδηγούν σε παραβιάσεις προσωπικών δεδομένων, συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

4. Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας καθορίζονται η μεθοδολογία αξιολόγησης της περίπτωσης α΄ και η διαδικασία παροχής πληροφοριών της περίπτωσης β΄ της παραγράφου 1.

## ΚΕΦΑΛΑΙΟ Δ΄
## ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΩΝ ΠΑΡΟΧΩΝ ΨΗΦΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

**Άρθρο 11**
**Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων**
**(Άρθρο 16 της Οδηγίας 2016/1148/ΕΕ)**

1. Η Εθνική Αρχή Κυβερνοασφάλειας σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς εμπλεκόμενους φορείς:

α) αξιολογεί τα τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που πρέπει να λάβουν οι πάροχοι ψηφιακών υπηρεσιών, όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στο πλαίσιο της παροχής, εντός της Ευρωπαϊκής Ένωσης, των υπηρεσιών του Παραρτήματος ΙΙ. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο και να συνεκτιμούν ιδίως τα εξής στοιχεία:

αα) την ασφάλεια των συστημάτων και των εγκαταστάσεων,

ββ) τη διαχείριση συμβάντων,

γγ) τη διαχείριση της επιχειρησιακής συνέχειας,

δδ) την παρακολούθηση, τους ελέγχους και τις δοκιμές δικτύων και πληροφοριακών συστημάτων,

εε) τη συμμόρφωση με διεθνή πρότυπα,

β) αξιολογεί τα μέτρα για την αποτροπή και την ελαχιστοποίηση των επιπτώσεων συμβάντων, τα οποία πρέπει να λάβουν οι πάροχοι ψηφιακών υπηρεσιών και επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν σε σχέση με τις υπηρεσίες του Παραρτήματος ΙΙ, οι οποίες προσφέρονται εντός της Ευρωπαϊκής Ένωσης, με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειάς τους,

γ) καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν οι πάροχοι ψηφιακών υπηρεσιών, προκειμένου να κοινοποιούν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT, χωρίς αδικαιολόγητη καθυστέρηση, κάθε συμβάν που έχει σημαντικές επιπτώσεις στην παροχή της υπηρεσίας, η οποία υπάγεται σε κατηγορία υπηρεσιών που αναφέρεται στο Παράρτημα ΙΙ και παρέχεται από αυτούς εντός της Ευρωπαϊκής Ένωσης. Οι ανωτέρω κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT να προσδιορίσουν τόσο τη σοβαρότητα του συμβάντος όσο και τις διασυνοριακές επιπτώσεις. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα πάροχο.

2. Για να προσδιοριστεί αν οι επιπτώσεις ενός συμβάντος είναι σημαντικές, λαμβάνονται υπόψη ειδικότερα οι εξής παράμετροι:

α) ο αριθμός των χρηστών που επηρεάζονται από το συμβάν, ιδίως αυτών που εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών,

β) η διάρκεια του συμβάντος,

γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν,

δ) το μέγεθος της διατάραξης της λειτουργίας της υπηρεσίας,

ε) η έκταση των επιπτώσεων στις οικονομικές και κοινωνικές δραστηριότητες.

Η υποχρέωση κοινοποίησης συμβάντος εφαρμόζεται μόνο αν ο πάροχος ψηφιακών υπηρεσιών έχει πρόσβαση στις πληροφορίες που απαιτούνται για να εκτιμηθεί ο αντίκτυπος του συμβάντος έναντι των παραμέτρων που αναφέρονται στις περιτπώσεις α΄ έως ε΄.

3. Όταν ένας φορέας εκμετάλλευσης βασικών υπηρεσιών εξαρτάται από τρίτο φορέα παροχής ψηφιακών υπηρεσιών για την παροχή υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων οικονομικών και κοινωνικών δραστηριοτήτων, κοινοποιείται από τον εν λόγω φορέα κάθε σοβαρή επίπτωση επί της συνέχειας των βασικών υπηρεσιών που οφείλεται σε συμβάν το οποίο επηρεάζει τον πάροχο ψηφιακών υπηρεσιών.

4. Κατά περίπτωση, και συγκεκριμένα αν το συμβάν με σημαντικές επιπτώσεις που αναφέρεται στην περίπτωση γ΄ της παραγράφου 1 αφορά δύο (2) ή περισσότερα κράτη-μέλη, η Εθνική Αρχή Κυβερνοασφάλειας ενημερώνει τα άλλα κράτη-μέλη που επηρεάζονται από το συμβάν. Στο πλαίσιο της ενημέρωσης αυτής, το ενιαίο κέντρο ε-

παφής σε συνεργασία με την αρμόδια CSIRT πρέπει, σύμφωνα με το ενωσιακό δίκαιο και την εθνική νομοθεσία που είναι σύμφωνη προς το ενωσιακό δίκαιο, να διαφυλάσσουν την ασφάλεια και τα εμπορικά συμφέροντα του παρόχου ψηφιακών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που ο τελευταίος έχει παράσχει. Το εθνικό ενιαίο κέντρο επαφής διαβιβάζει τις κοινοποιήσεις συμβάντων που αναφέρονται στο πρώτο εδάφιο της παρούσας στα ενιαία κέντρα επαφής των άλλων επηρεαζόμενων κρατών-μελών.

5. Ύστερα από διαβούλευση με τον ενδιαφερόμενο πάροχο ψηφιακών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT, και, κατά περίπτωση, οι αρμόδιες αρχές ή τα αρμόδια CSIRT άλλων ενδιαφερόμενων κρατών-μελών μπορούν να ενημερώνουν το κοινό σχετικά με μεμονωμένα συμβάντα ή να απαιτούν από τον πάροχο ψηφιακών υπηρεσιών να το πράξει, όταν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη ή αν η αποκάλυψη του συμβάντος εξυπηρετεί το δημόσιο συμφέρον.

6. Με την επιφύλαξη της παραγράφου 5 του άρθρου 1, δεν επιβάλλονται οποιεσδήποτε περαιτέρω υποχρεώσεις ασφάλειας ή κοινοποίησης στους παρόχους ψηφιακών υπηρεσιών.

7. Τα άρθρα 11 έως 13 δεν εφαρμόζονται σε πολύ μικρές και μικρές επιχειρήσεις, όπως αυτές ορίζονται στη σύσταση 2003/361/ΕΚ της Επιτροπής της 6ης Μαΐου 2003 (ΕΕ L 124).

### Άρθρο 12
### Εφαρμογή και επιβολή
### (Άρθρο 17 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας:

α) αξιολογεί και αναλαμβάνει δράση επιβάλλοντας τα απαραίτητα εποπτικά μέτρα, όταν της παρέχονται στοιχεία που αποδεικνύουν ότι πάροχος ψηφιακών υπηρεσιών δεν πληροί τις απαιτήσεις που ορίζονται στο άρθρο 11. Τα εν λόγω αποδεικτικά στοιχεία μπορεί να υποβάλλονται από μια αρμόδια αρχή άλλου κράτους-μέλους, στο οποίο παρέχεται η υπηρεσία,

β) απαιτεί από τους παρόχους ψηφιακών υπηρεσιών:

αα) να παρέχουν τις απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων δικτύου και των πληροφοριών τους, συμπεριλαμβανομένων τεκμηριωμένων και εγκεκριμένων πολιτικών ασφάλειας,

ββ) να διορθώνουν οποιαδήποτε παράλειψη συμμόρφωσης προς τις απαιτήσεις που ορίζονται στο άρθρο 11.

2. Αν ένας πάροχος ψηφιακών υπηρεσιών έχει την κύρια εγκατάστασή του ή αντιπρόσωπο σε ένα κράτος-μέλος, αλλά τα συστήματα δικτύου και πληροφοριών του βρίσκονται σε ένα ή περισσότερα άλλα κράτη-μέλη, η αρμόδια αρχή του κράτους-μέλους της κύριας εγκατάστασης ή του αντιπροσώπου και οι αρμόδιες αρχές των άλλων κρατών-μελών συνεργάζονται και παρέχουν αμοιβαία συνδρομή, εφόσον απαιτείται. Η συνδρομή και η συνεργασία μπορεί να καλύπτουν ανταλλαγές πληροφοριών μεταξύ των σχετικών αρμόδιων αρχών και αιτήματα για τη λήψη των ανωτέρω αναφερόμενων εποπτικών μέτρων.

3. Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, καθορίζονται τα μέτρα της περίπτωσης α΄ και η διαδικασία παροχής πληροφοριών της περίπτωσης β΄ της παραγράφου 1.

### Άρθρο 13
### Δικαιοδοσία και εδαφικότητα
### (Άρθρο 18 της Οδηγίας 2016/1148/ΕΕ)

1. Ο πάροχος ψηφιακών υπηρεσιών υπόκειται στη δικαιοδοσία των Ελληνικών αρχών όταν έχει την κύρια εγκατάστασή του στην Ελληνική Επικράτεια. Ο πάροχος ψηφιακών υπηρεσιών θεωρείται ότι έχει την κύρια εγκατάστασή του στην Ελληνική Επικράτεια όταν έχει την έδρα του σε αυτήν.

2. Ο πάροχος ψηφιακών υπηρεσιών που δεν είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση αλλά προσφέρει, εντός της Ευρωπαϊκής Ένωσης, υπηρεσίες που αναφέρονται στο Παράρτημα ΙΙ ορίζει αντιπρόσωπο στην Ένωση. Ο αντιπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη-μέλη στα οποία προσφέρονται οι υπηρεσίες. Ο πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτου- μέλους στο οποίο είναι εγκατεστημένος ο αντιπρόσωπος.

3. Ο ορισμός αντιπροσώπου από τον πάροχο ψηφιακών υπηρεσιών δεν θίγει τις νομικές ενέργειες που μπορεί να αναληφθούν κατά του ίδιου του παρόχου ψηφιακών υπηρεσιών.

## ΚΕΦΑΛΑΙΟ Ε΄
## ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

### Άρθρο 14
### Εθελούσια κοινοποίηση
### (Άρθρο 20 της Οδηγίας 2016/1148/ΕΕ)

1. Οντότητες που δεν έχουν προσδιοριστεί ως φορείς εκμετάλλευσης βασικών υπηρεσιών και δεν είναι πάροχοι ψηφιακών υπηρεσιών μπορεί να κοινοποιούν σε εθελούσια βάση συμβάντα με σοβαρές επιπτώσεις στη επιχειρησιακή συνέχεια των υπηρεσιών που παρέχουν.

2. Κατά την επεξεργασία των κοινοποιήσεων, οι αρμόδιες αρχές ενεργούν σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 9. Οι αρμόδιες αρχές μπορεί να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων. Οι εθελούσιες κοινοποιήσεις υποβάλλονται σε επεξεργασία μόνον εφόσον η επεξεργασία αυτή δεν συνιστά δυσανάλογη ή περιττή επιβάρυνση για τα οικεία κράτη-μέλη.

Η εθελούσια κοινοποίηση δεν συνεπάγεται την επιβολή στην κοινοποιούσα οντότητα υποχρεώσεων τις οποίες δεν θα είχε αν δεν προέβαινε στην εν λόγω κοινοποίηση.

### Άρθρο 15
### Κυρώσεις
### (Άρθρο 21 της Οδηγίας 2016/1148/ΕΕ)

1. Ο Υπουργός Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, επιβάλλει κυρώσεις σε φυσικό ή νομικό πρόσωπο, σε περίπτωση παραβίασης των διατάξεων του παρόντος νόμου, ως εξής:

α) Αν διαπιστωθεί ότι φορέας εκμετάλλευσης βασικών υπηρεσιών ή φορέας παροχής ψηφιακών υπηρεσιών δεν κοινοποιεί ή κοινοποιεί με αδικαιολόγητη καθυστέρηση

συμβάν με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών του, επιβάλλεται:

αα) πρόστιμο μέχρι του ποσού των δεκαπέντε χιλιάδων (15.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων,

ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.

β) Αν διαπιστωθεί ότι φορέας εκμετάλλευσης βασικών υπηρεσιών ή φορέας παροχής ψηφιακών υπηρεσιών δεν λαμβάνει κατάλληλα και αναλογικά, τεχνικά και οργανωτικά, προληπτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των δικτύων και των συστημάτων πληροφοριών που χρησιμοποιεί για τις υπηρεσίες αυτές, επιβάλλεται:

αα) πρόστιμο μέχρι του ποσού των πενήντα χιλιάδων (50.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων,

ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.

γ) Αν διαπιστωθεί ότι φυσικό ή νομικό πρόσωπο δεν παρέχει ή παρέχει με αδικαιολόγητη καθυστέρηση οποιαδήποτε σχετική πληροφορία που ζητείται κατά τη διενέργεια ελέγχου ή τη διερεύνηση περιστατικού, επιβάλλεται:

αα) πρόστιμο μέχρι του ποσού των πενήντα χιλιάδων (50.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων,

ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.

2. Πριν από την επιβολή κυρώσεων, η Εθνική Αρχή Κυβερνοασφάλειας ειδοποιεί εγγράφως το ενδιαφερόμενο φυσικό ή νομικό πρόσωπο, παρέχοντας σε αυτό το δικαίωμα ακρόασης και παροχής εξηγήσεων σε ημερομηνία, που απέχει πέντε (5) τουλάχιστον εργάσιμες ημέρες από την κοινοποίηση της ειδοποίησης.

Οι κυρώσεις επιβάλλονται με γραπτή και αιτιολογημένη απόφαση, η οποία κοινοποιείται στο ενδιαφερόμενο φυσικό ή νομικό πρόσωπο και στην οποία προσδιορίζεται η παράβαση. Οι κυρώσεις που επιβάλλονται στις ανωτέρω περιπτώσεις αναρτώνται στην επίσημη ιστοσελίδα της Εθνικής Αρχής Κυβερνοασφάλειας.

**Άρθρο 16**

Προσαρτώνται στο παρόντα νόμο και αποτελούν αναπόσπαστο τμήμα αυτού τα Παραρτήματα Ι και ΙΙ.

**Άρθρο 17**
**Έναρξη ισχύος**

Η ισχύς του παρόντος νόμου αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως, εκτός αν άλλως ορίζεται στις επιμέρους διατάξεις.

ΠΑΡΑΡΤΗΜΑ Ι
ΕΙΔΟΣ ΟΝΤΟΤΗΤΩΝ ΓΙΑ ΤΟΥΣ ΣΚΟΠΟΥΣ ΤΟΥ ΑΡΘΡΟΥ 3 ΠΑΡΑΓΡΑΦΟΣ 4

| Τομέας | Υποτομέας | Είδος οντότητας |
|---|---|---|
| 1. Ενέργεια | α) Ηλεκτρική ενέργεια | — Επιχειρήσεις ηλεκτρικής ενέργειας, όπως ορίζονται στην περίπτ. ιη΄ της παρ. 3 του άρθρου 2 του ν. 4001/2011 (Α΄ 179), οι οποίες ασκούν τη δραστηριότητα «προμήθεια», όπως ορίζεται στην περίπτ. κα΄ της παρ. 1 του άρθρου 2 του ανωτέρω νόμου |
| | | — Διαχειριστές δικτύου διανομής, όπως ορίζονται στην περίπτ. στ΄ της παρ. 1 του άρθρου 2 του ν. 4001/2011 |
| | | — Διαχειριστές συστήματος μεταφοράς, όπως ορίζονται στην περίπτ. ια΄ της παρ. 3 του άρθρου 2 του ν. 4001/2011 |
| | β) Πετρέλαιο | — Διαχειριστές αγωγών μεταφοράς πετρελαίου |
| | | — Διαχειριστές παραγωγής πετρελαίου, εγκαταστάσεων διύλισης και επεξεργασίας, αποθήκευσης και μεταφοράς πετρελαίου |
| | γ) Αέριο | — Επιχειρήσεις προμήθειας, όπως ορίζονται στην περίπτ. κβ΄ της παρ. 1 και στην περίπτ. κβ΄ της παρ. 2 του άρθρου 2 του ν. 4001/2011 |
| | | — Διαχειριστές δικτύου διανομής, όπως ορίζονται στην περίπτ. στ΄ της παρ. 1 του άρθρου 2 του ν. 4001/2011 |
| | | — Διαχειριστές συστήματος μεταφοράς, όπως ορίζονται στα άρθρα 61, 62, στην περίπτ. α΄ της παρ. 1, στις περίπτ.στ΄, ζ΄ και η΄ της παρ. 2 του άρθρου 2 του ν. 4001/2011 |
| | | — Διαχειριστές συστήματος αποθήκευσης, όπως ορίζονται στο άρθρο 2 σημείο 10 της Οδηγίας 2009/73/ΕΚ |
| | | — Διαχειριστές συστήματος ΥΦΑ, όπως ορίζονται στο άρθρο 2 σημείο 12 της Οδηγίας 2009/73/ΕΚ |
| | | — Επιχειρήσεις φυσικού αερίου, όπως ορίζονται στην περίπτ. ιδ΄ της παρ. 2 του άρθρου 2 του ν. 4001/2011 |
| | | — Διαχειριστές εγκαταστάσεων διύλισης και επεξεργασίας φυσικού αερίου |
| 2. Μεταφορές | α) Αεροπορικές μεταφορές | — Αερομεταφορείς, όπως ορίζονται στο σημείο 4 του άρθρου 3 του Κανονισμού (ΕΚ) 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαρτίου 2008 (ΕΕ L 97) |
| | | — Φορείς διαχείρισης αερολιμένα, όπως ορίζονται στην περίπτ. β΄ της παρ. 1 του άρθρου 2 του π.δ. 52/2012 (Α΄ 102), αερολιμένες, όπως ορίζονται στην περίπτ. α΄ της παρ. 1 του άρθρου 2 του ίδιου π.δ., συμπεριλαμβανομένων των κεντρικών αερολιμένων που απαριθμούνται στο τμήμα 2 του Παραρτήματος ΙΙ του Κανονισμού (ΕΕ) 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Δεκεμβρίου |

| | | |
|---|---|---|
| | | 2013 (ΕΕ L 348), και φορείς εκμετάλλευσης βοηθητικών εγκαταστάσεων που βρίσκονται εντός των αερολιμένων |
| | | — Φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας που παρέχουν υπηρεσίες ελέγχου εναέριας κυκλοφορίας όπως ορίζονται στο σημείο 1 του άρθρου 2 του Κανονισμού (ΕΚ) 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Μαρτίου 2004 (ΕΕ L 96) |
| | β). Σιδηροδρομικές μεταφορές | — Διαχειριστές της υποδομής, όπως ορίζονται στην παρ. 2 του άρθρου 3 του ν. 4408/2016 (Α΄ 135) |
| | | — Σιδηροδρομικές επιχειρήσεις, όπως ορίζονται στην παρ. 1 του άρθρου 3 του ν. 4408/2016, συμπεριλαμβανομένων των φορέων εκμετάλλευσης εγκαταστάσεων για την παροχή υπηρεσιών, όπως ορίζονται στην παρ. 12 του άρθρου 3 του ιδίου νόμου |
| | γ) Πλωτές μεταφορές | — Εσωτερικές πλωτές, θαλάσσιες και ακτοπλοϊκές εταιρείες μεταφοράς επιβατών και εμπορευμάτων, όπως ορίζονται για τις θαλάσσιες μεταφορές στο Παράρτημα Ι του Κανονισμού (ΕΚ) 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 31ης Μαρτίου 2004 (ΕΕ L 129), μη συμπεριλαμβανομένων των μεμονωμένων πλοίων που χρησιμοποιούνται από τις εταιρείες αυτές |
| | | — Διαχειριστικοί φορείς των λιμένων, όπως ορίζονται στην παρ. 11 του άρθρου 2 του ν. 3622/2007 (Α΄ 281), συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων όπως ορίζονται στο σημείο 11 του άρθρου 2 του Κανονισμού (ΕΚ) 725/2004, και φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός των λιμένων |
| | | — Φορείς εκμετάλλευσης υπηρεσιών εξυπηρέτησης κυκλοφορίας πλοίων (VTS), όπως ορίζονται στην περίπτ. κ΄ του άρθρου 3 του π.δ. 49/2005 (Α΄ 66) |
| | δ) Οδικές μεταφορές | — Οδικές αρχές, όπως ορίζονται στο σημείο 12 του άρθρου 2 του κατ' εξουσιοδότηση Κανονισμού (ΕΕ) 2015/962 της Επιτροπής της 18ης Δεκεμβρίου 2015 (ΕΕ L 157) που είναι υπεύθυνες για τον έλεγχο διαχείρισης της κυκλοφορίας |
| | | — Φορείς εκμετάλλευσης συστημάτων ευφυών μεταφορών (ITS), όπως ορίζονται στην παρ. 1 του άρθρου 4 του π.δ. 50/2012 (Α΄ 100) |
| 3. Τράπεζες | | Πιστωτικά ιδρύματα, όπως ορίζονται στο σημείο 1 του άρθρου 4 του Κανονισμού (ΕΕ) 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Ιουνίου 2013 (ΕΕ L 176) |
| 4. Υποδομές χρηματοπιστωτικών αγορών | | — Φορείς εκμετάλλευσης τόπων διαπραγμάτευσης, όπως ορίζονται στην παρ. 24 του άρθρου 4 του ν. 4514/2018 (Α΄ 14) |
| | | — Κεντρικοί αντισυμβαλλόμενοι (CCP), όπως ορίζονται στο σημείο 1 του άρθρου 2 του Κανονισμού |

| | | |
|---|---|---|
| | | (ΕΕ) 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 4ης Ιουλίου 2012 (ΕΕ L 201) |
| 5. Τομέας της υγείας | Περιβάλλοντα υγειονομικής περίθαλψης (μεταξύ άλλων νοσοκομεία και ιδιωτικές κλινικές) | Πάροχοι υγειονομικής περίθαλψης, όπως ορίζονται στην περίπτ. ζ΄ του άρθρου 3 του ν. 4213/2013 (Α΄ 261) |
| 6. Προμήθεια και διανομή πόσιμου νερού | | Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης, όπως ορίζονται στην περίπτ. α΄ της παρ. 1 του άρθρου 2 της Γ1(δ)/ΓΠ οικ.67322 κοινής απόφασης των Υπουργών Εσωτερικών, Οικονομίας και Ανάπτυξης, Υγείας, Περιβάλλοντος και Ενέργειας (Β΄ 3282), αλλά εξαιρουμένων των διανομέων για τους οποίους η διανομή νερού ανθρώπινης κατανάλωσης αποτελεί μόνο μέρος της γενικής τους δραστηριότητας διανομής λοιπών προϊόντων και αγαθών που δεν θεωρούνται βασικές υπηρεσίες |
| 7. Ψηφιακή υποδομή | | — Σημεία ανταλλαγής κίνησης διαδικτύου (IXP) |
| | | — Πάροχοι υπηρεσιών συστήματος ονομάτων χώρου (DNS) |
| | | — Μητρώα ονομάτων χώρου ανώτατου επιπέδου (TLD) |

ΠΑΡΑΡΤΗΜΑ ΙΙ
ΕΙΔΗ ΨΗΦΙΑΚΩΝ ΥΠ[ΗΡΕΣΙΩΝ ΓΙΑ ΤΟΥΣ ΣΚΟΠΟΥΣ ΤΟΥ ΑΡΘΡΟΥ 3 ΠΑΡΑΓΡΑΦΟΣ 5

1. Επιγραμμική αγορά
2. Επιγραμμική μηχανή αναζήτησης
3. Υπηρεσία νεφοϋπολογιστικής

Αθήνα, 12 Νοεμβρίου 2018

ΟΙ ΥΠΟΥΡΓΟΙ

ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ

ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

Ν. Παππάς

Π. Καμμένος

ΔΙΚΑΙΟΣΥΝΗΣ, ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΑΝΘΡΩΠΙΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Μ. Καλογήρου

Αριθμ. 301/8/2018

**ΕΚΘΕΣΗ**
**Γενικού Λογιστηρίου του Κράτους**
*(άρθρο 75 παρ.1 του Συντάγματος)*

***στο σχέδιο νόμου του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση»***

Α. Με το υπόψη σχέδιο νόμου, ενσωματώνεται στην ελληνική νομοθεσία η Οδηγία 2016/1148/ΕΕ, σχετικά με τη θέσπιση μέτρων επίτευξης υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών. Ειδικότερα:

1.α. Προσδιορίζονται το αντικείμενο και το πεδίο εφαρμογής των προτεινόμενων ρυθμίσεων, με τις προβλεπόμενες εξαιρέσεις για τη μη εφαρμογή των οριζόμενων απαιτήσεων ασφάλειας και κοινοποίησης στις μνημονευόμενες επιχειρήσεις ή στους αναφερόμενους παρόχους, καθώς και με τις σχετικές επιφυλάξεις (ανταλλαγή αναγκαίων πληροφοριών με διαφύλαξη του απορρήτου αυτών, προστασία των συμφερόντων ασφαλείας και εμπορικών συμφερόντων των εμπλεκόμενων φορέων κ.λπ.).

β. Διασφαλίζεται η εφαρμογή της ισχύουσας ελληνικής και ενωσιακής νομοθεσίας για τη διενέργεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται κατ' εφαρμογή του υπό ψήφιση νόμου.

γ. Δίδονται οι έννοιες των όρων, που αναφέρονται στις προτεινόμενες διατάξεις για την εκπλήρωση των σκοπών του υπό ψήφιση νόμου. *(άρθρα 1-3)*

2.α. Οι φορείς εκμετάλλευσης βασικών υπηρεσιών, που είναι εγκατεστημένοι στην ελληνική επικράτεια, προσδιορίζονται, για κάθε τομέα και υποτομέα, από την Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με τις αρμόδιες ρυθμιστικές/εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς.

Οι ανωτέρω φορείς ορίζονται με υπουργική απόφαση και προσδιορίζονται σύμφωνα με τα προβλεπόμενα κριτήρια.

β. Για την εφαρμογή των ανωτέρω, η Εθνική Αρχή Κυβερνοασφάλειας προβαίνει στις μνημονευόμενες ενέργειες (κατάρτιση σχετικών καταλόγων, διαβουλεύσεις με αντίστοιχες αρχές άλλων κρατών μελών, υποβολή, ανά διετία, πληροφοριών στην Επιτροπή με το οριζόμενο περιεχόμενο).

γ. Η Εθνική Αρχή Κυβερνοασφάλειας καθορίζει, επίσης, σε συνεργασία με τις κατά περίπτωση αρμόδιες ρυθμιστικές/εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς, τα κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης, λαμβάνοντας υπόψη τους μνημονευόμενους παράγοντες. *(άρθρα 4-5)*

3.α. Ορίζεται ότι, η Εθνική Αρχή Κυβερνοασφάλειας επικαιροποιεί την Εθνική Στρατηγική Κυβερνοασφάλειας και την κοινοποιεί στην Επιτροπή εντός της οριζόμενης προθεσμίας.

β. Η Εθνική Στρατηγική Κυβερνοασφάλειας αποτελεί την εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών και περιλαμβάνει, μεταξύ άλλων, τους στόχους και τις προτεραιότητες αυτής, τον προσδιορισμό των μέτρων ετοιμότητας, απόκρισης και αποκατάστασης με συνεργασία δημόσιου και ιδιωτικού τομέα, προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης, σχέδια έρευνας και ανάπτυξης και εκτίμησης κινδύνου κ.λπ.. *(άρθρο 6)*

4.α. Ορίζεται η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης ως Εθνική Αρμόδια Αρχή για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (εφεξής, Αρμόδια Αρχή ή Εθνική Αρχή Κυβερνοασφάλειας).

β. Προσδιορίζονται οι αρμοδιότητες της ανωτέρω Αρχής, μεταξύ των οποίων περιλαμβάνονται η συνεργασία με τις οριζόμενες εθνικές αρχές και φορείς και τις αρμόδιες αρχές λοιπών κρατών-μελών, η διεξαγωγή σχετικών διαβουλεύσεων, συμμετοχή σε μνημονευόμενες ομάδες εργασίας, καθώς και η συμμετοχή στην Ομάδα Συνεργασίας «Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)» με τον ορισμό εθνικών αντιπροσώπων.

γ. Η Εθνική Αρχή Κυβερνοασφάλειας ορίζεται ως το εθνικό κέντρο επαφής (εφεξής, Εθνικό Κέντρο Επαφής), για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, που ασκεί καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών-μελών, με την υποχρέωση υποβολής, ετησίως, στην αρμόδια ομάδα συνεργασίας, έκθεσης με τα συμβάντα και τα μέτρα που έχουν ληφθεί, κατά τα ειδικότερα οριζόμενα.

δ. Προβλέπεται η υποχρέωση δημοσιοποίησης και κοινοποίησης στην Επιτροπή της Αρμόδιας Αρχής, του Εθνικού Κέντρου Επαφής και των καθηκόντων αυτών. *(άρθρο 7)*

5.α. Η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ ορίζεται ως Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών [Computer Security Incident Response Team (CSIRT)], η οποία καλύπτει τους μνημονευόμενους τομείς και τις υπηρεσίες, είναι δε υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας.

β. Η ανωτέρω Υπηρεσία, στο πλαίσιο άσκησης των καθηκόντων της, μεταξύ άλλων, οφείλει να εξασφαλίζει υψηλό επίπεδο διαθεσιμότητας των υπηρεσιών επικοινωνιών και εγκατάσταση των γραφείων της σε ασφαλείς χώρους. Σχετικά δε με τη συνέχεια της επιχειρησιακής της δραστηριότητας, πρέπει να είναι εφοδιασμένη με τις κατάλληλες υποδομές και επαρκώς στελεχωμένη, συμμετέχει δε σε διεθνή δίκτυα συνεργασίας.

γ. Περαιτέρω, προσδιορίζονται οι αρμοδιότητες της CSIRT (παρέμβαση σε περίπτωση συμβάντος, παροχή δυναμικής ανάλυσης κινδύνων και συμβάντων, συνεργασία με την Εθνική Αρχή Κυβερνοασφάλειας για την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας κ.λπ.).

*(άρθρο 8, σε συνδυασμό με τα Παραρτήματα Ι και ΙΙ)*

6.α. Για την ασφάλεια των συστημάτων δικτύου και πληροφοριών των φορέων εκμετάλλευσης βασικών υπηρεσιών, καθώς και των παρόχων ψηφιακών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς, κατά περίπτωση, εμπλεκόμενους φορείς:

- αξιολογεί τα τεχνικά και οργανωτικά μέτρα που λαμβάνουν οι ανωτέρω φορείς εκμετάλλευσης βασικών υπηρεσιών και οι πάροχοι ψηφιακών υπηρεσιών, για τη διαχείριση των κινδύνων σχετικά με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται στις δραστηριότητές τους,

- αξιολογεί την καταλληλότητα των προαναφερόμενων μέτρων, για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύων και πληροφοριών,

- καθορίζει τις σχετικές διαδικασίες κοινοποίησης, που πρέπει να τηρούνται από τους ανωτέρω φορείς και παρόχους, κατά τα ειδικότερα οριζόμενα.

β. Περαιτέρω, καθορίζονται οι παράμετροι που λαμβάνονται υπόψη για τον προσδιορισμό της σοβαρότητας του αντίκτυπου ενός συμβάντος (αριθμός χρηστών, διάρκεια συμβάντος κ.λπ.).

γ. Ρυθμίζονται θέματα σχετικά με την ενημέρωση από την Εθνική Αρχή Κυβερνοασφάλειας των επηρεαζόμενων από συμβάν με σοβαρό αντίκτυπο κρατών-μελών.

δ. Προσδιορίζονται οι ενέργειες στις οποίες προβαίνει η Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο της εφαρμογής και επιβολής από τους προαναφερόμενους φορείς και παρόχους των ανωτέρω υποχρεώσεων και συγκεκριμένα:

- αξιολογεί τη συμμόρφωση των φορέων εκμετάλλευσης βασικών υπηρεσιών προς τις κατά τα ανωτέρω υποχρεώσεις τους και απαιτεί από τους εν λόγω φορείς την παροχή απαραίτητων πληροφοριών και στοιχείων σχετικά με την εφαρμογή των διατάξεων του υπό ψήφιση νόμου, σύμφωνα με τα οριζόμενα.

Με υπουργική απόφαση καθορίζονται η μεθοδολογία της προαναφερόμενης αξιολόγησης και η διαδικασία παροχής των αναγκαίων πληροφοριών.

Επιπλέον, η ανωτέρω Αρχή μπορεί να εκδίδει δεσμευτικές οδηγίες προς τους εν λόγω φορείς για την αποκατάσταση των εντοπισμένων ελλείψεων και να συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στις περιπτώσεις συμβάντων όπου παρατηρούνται παραβιάσεις προσωπικών δεδομένων.

Επίσης, αξιολογεί και επιβάλλει τα απαραίτητα εποπτικά μέτρα στους παρόχους ψηφιακών υπηρεσιών, στις περιπτώσεις που αυτοί δεν πληρούν τα οριζόμενα στον υπό ψήφιση νόμο και απαιτεί από αυτούς την παροχή των αναγκαίων πληροφοριών για την εκτίμηση της ασφάλειας των συστημάτων δικτύου και των πληροφοριών αυτών, καθώς και τη διόρθωση οποιασδήποτε παράλειψης συμμόρφωσης των εν λόγω παρόχων.

Με υπουργική απόφαση καθορίζονται τα προαναφερόμενα εποπτικά μέτρα και η διαδικασία παροχής των αναγκαίων πληροφοριών.

Προβλέπεται, επίσης, η συνεργασία και παροχή αμοιβαίας συνδρομής μεταξύ των αρμόδιων αρχών, στην περίπτωση παρόχου ψηφιακών υπηρεσιών, με κύρια εγκατάσταση ή αντιπρόσωπο σε ένα κράτος-μέλος και συστήματα δικτύου και πληροφοριών του βρίσκονται σε άλλο ή άλλα κράτη-μέλη. *(άρθρα 9-12)*

7.α. Ρυθμίζονται θέματα δικαιοδοσίας και εδαφικότητας για τους παρόχους ψηφιακών υπηρεσιών και συγκεκριμένα ορίζεται ότι, στην περίπτωση που έχουν την κύρια εγκατάστασή τους στην ελληνική επικράτεια, υπάγονται στο δίκαιο των ελληνικών αρχών, ενώ όταν δεν είναι εγκατεστημένοι στην Ευρωπαϊκή Ένωση ορίζεται αντιπρόσωπος αυτών στην Ένωση.

β. Παρέχεται η δυνατότητα σε οντότητες που δεν έχουν προσδιορισθεί ως φορείς εκμετάλλευσης βασικών υπηρεσιών και δεν είναι πάροχοι ψηφιακών υπηρεσιών, να κοινοποιούν σε εθελούσια βάση συμβάντα με σοβαρές επιπτώσεις στην επιχειρησιακή συνέχεια των υπηρεσιών που παρέχουν.

Οι αρμόδιες αρχές, κατά την επεξεργασία των κοινοποιήσεων, μπορεί να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελουσίων κοινοποιήσεων.

Οι εθελούσιες κοινοποιήσεις δεν συνεπάγονται την επιβολή υποχρεώσεων, υποβάλλονται δε σε επεξεργασία μόνον εφόσον αυτό δεν συνιστά δυσανάλογη ή περιττή επιβάρυνση για τα οικεία κράτη-μέλη. *(άρθρα 13, 14)*

8. Προβλέπεται η επιβολή κυρώσεων, από τον Υπουργό Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, σύμφωνα με την οριζόμενη διαδικασία, σε φυσικά ή νομικά πρόσωπα που είναι φορείς εκμετάλλευσης βασικών υπηρεσιών ή φορείς παροχής ψηφιακών υπηρεσιών και παραβιάζουν τις προτεινόμενες ρυθμίσεις. Ειδικότερα, επιβάλλεται πρόστιμο:

- έως 15.000 ευρώ, με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων, σε περίπτωση μη κοινοποίησης ή κοινοποίησης σοβαρού συμβάντος με αδικαιολόγητη καθυστέρηση,

- έως 50.000 ευρώ, με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων, σε περίπτωση που: i) δεν λαμβάνουν τα κατάλληλα, κατά περίπτωση, μέτρα για τη διαχείριση των κινδύνων ασφάλειας των δικτύων και των συστημάτων πληροφοριών που χρησιμοποιούν, ii) δεν παρέχονται ή παρέχονται με αδικαιολόγητη καθυστέρηση οι πληροφορίες που ζητούνται κατά τη διενέργεια ελέγχου ή τη διερεύνηση περιστατικού.

Τα ανωτέρω πρόστιμα, σε περίπτωση υποτροπής, μπορεί να ανέλθουν μέχρι το ποσό των 200.000 ευρώ.

*(άρθρο 15)*

9. Προσαρτώνται στον υπό ψήφιση νόμο και αποτελούν αναπόσπαστο τμήμα αυτού τα Παραρτήματα Ι και ΙΙ, όπου προσδιορίζονται οι οντότητες (τομείς) και τα είδη των ψηφιακών υπηρεσιών που καλύπτει η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ, ως Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών. *(άρθρο 16)*

Β. Από τις προτεινόμενες διατάξεις προκαλούνται, επί του Κρατικού Προϋπολογισμού, τα ακόλουθα οικονομικά αποτελέσματα:

1. Ενδεχόμενη δαπάνη, από τυχόν λήψη μέτρων για την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας (μέτρα ετοιμότητας, προγράμματα εκπαίδευσης και κατάρτισης, εφοδιασμό της αρμόδιας υπηρεσίας (CSIRT) με τις κατάλληλες υποδομές, εξοπλισμό και προσωπικό κ.λπ.), η οποία εξαρτάται από πραγματικά γεγονότα. *(άρθρα 6, 7 και 8)*

2. Ενδεχόμενη αύξηση των δημοσίων εσόδων, από την είσπραξη των προστίμων που επιβάλλονται, με υπουργική απόφαση, σε φορείς εκμετάλλευσης βασικών υπηρεσιών ή φορείς παροχής ψηφιακών υπηρεσιών, σε περίπτωση που παραβιάζουν τις προτεινόμενες ρυθμίσεις. *(άρθρο 15)*

Η εν λόγω αύξηση εξαρτάται από πραγματικά γεγονότα (είδος και αριθμός παραβάσεων, περιπτώσεις υποτροπής κ.λπ.).

Αθήνα, 9 Νοεμβρίου 2018

Η Γενική Διευθύντρια

Ιουλία Γ. Αρμάγου

**ΕΙΔΙΚΗ ΕΚΘΕΣΗ**

*(άρθρο 75 παρ. 3 του Συντάγματος)*

***στο σχέδιο νόμου «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση»***

Από τις διατάξεις του προτεινόμενου σχεδίου νόμου προκαλείται, σε βάρος του Κρατικού Προϋπολογισμού, ενδεχόμενη δαπάνη, από τυχόν λήψη μέτρων για την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας (μέτρα ετοιμότητας, προγράμματα εκπαίδευσης και κατάρτισης, εφοδιασμό της αρμόδιας υπηρεσίας (CSIRT) με τις κατάλληλες υποδομές, εξοπλισμό και προσωπικό κ.λπ.). *(άρθρα 6, 7 και 8)*

Η εν λόγω δαπάνη, η οποία εξαρτάται από πραγματικά γεγονότα, θα αντιμετωπίζεται από τις πιστώσεις του Κρατικού Προϋπολογισμού.

Αθήνα, 12 Νοεμβρίου 2018

ΟΙ ΥΠΟΥΡΓΟΙ

| ΟΙΚΟΝΟΜΙΚΩΝ | ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ |
|---|---|
| Ευκλ. Τσακαλώτος | Ν. Παππάς |

**ΕΚΘΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΣΥΝΕΠΕΙΩΝ ΡΥΘΜΙΣΕΩΝ**

**ΥΠΟΥΡΓΕΙΟ:** ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ
**ΥΠΕΥΘΥΝΟΣ ΕΠΙΚΟΙΝΩΝΙΑΣ: Μαγλαράς Λέανδρος**
**ΥΠΗΡΕΣΙΑ: Γενική Γραμματεία Ψηφιακής Πολιτικής**
**ΘΕΣΗ / ΕΙΔΙΚΟΤΗΤΑ: Αναπλ. Προϊστάμενος Διεύθυνσης Κυβερνοασφάλειας/ ΠΕ Πληροφορικής**
**ΤΗΛΕΦΩΝΟ: 210 9098275**
**E-MAIL: l.maglaras@gsdp.gr**

**ΤΙΤΛΟΣ ΠΡΟΤΕΙΝΟΜΕΝΟΥ ΣΧΕΔΙΟΥ ΝΟΜΟΥ:**
Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ
του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194/19.7.2016)

**ΠΕΡΙΛΗΠΤΙΚΗ ΑΝΑΦΟΡΑ**
**ΣΤΟ ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΚΥΡΙΑΣ ΑΞΙΟΛΟΓΟΥΜΕΝΗΣ ΡΥΘΜΙΣΗΣ:**

Περιεχόμενο της κύριας αξιολογούμενης ρύθμισης αποτελεί η ενσωμάτωση στην ελληνική έννομη τάξη της Οδηγίας 2016/1148/ΕΕ του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194/19.7.2016) σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση

**1. Αναγκαιότητα**

Με τις ρυθμίσεις του παρόντος σχεδίου νόμου θεσπίζονται τα μέτρα που απαιτούνται για την επίτευξη υψηλού επιπέδου ασφάλειας ίσο ή ανώτερο με το κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση. Η θέσπιση τέτοιων μέτρων κρίνεται απαραίτητη προϋπόθεση για την εύρυθμη λειτουργία κρίσιμων υπηρεσιών, για την προστασία των δεδομένων πολιτών και επιχειρήσεων εντός της Ένωσης (κατά συνέπεια και της Ελλάδας) και για την προστασία των θεμελιωδών δικαιωμάτων των πολιτών και των επιχειρήσεων σε ότι αφορά την αδιάλειπτη, αξιόπιστη και αποδοτική παροχή υπηρεσιών και βασικών αγαθών ζωτικής σημασίας για την κοινωνία, στους τομείς της ενέργειας, των μεταφορών, της τραπεζικής και χρηματοπιστωτικής αγοράς, της υγείας, του πόσιμου ύδατος, των ψηφιακών υποδομών, των επιγραμμικών υπηρεσιών αγοράς και μηχανών αναζήτησης καθώς και ψηφιακών υπηρεσιών νεφοϋπολογιστικής.

**2. Καταλληλότητα**

Τα συστήματα και οι υπηρεσίες δικτύων και πληροφοριών διαδραματίζουν ζωτικό ρόλο στην κοινωνία. Η αξιοπιστία και η ασφάλειά τους είναι ουσιώδους σημασίας για τις οικονομικές και κοινωνικές δραστηριότητες, και ιδίως για τη λειτουργία της εσωτερικής αγοράς ενώ τα περιστατικά ασφάλειας βαίνουν αυξανόμενα σε συχνότητα και σοβαρότητα θέτοντας σε κίνδυνο την ομαλή κυκλοφορία υπηρεσιών, αγαθών και προσώπων στην Ένωση. Σε συνέχεια της σημαντικής προόδου που έχει σημειωθεί στην κατάρτιση κοινών πολιτικών σε διάφορούς τομείς η θέσπιση κανόνων και αρχών για την επίτευξη κοινού ελάχιστου επιπέδου ασφάλειας στο τομέα των συστημάτων δικτύων και επικοινωνιών μέσω της εθνικής νομοθεσίας αποτελεί την κατάλληλη αντιμετώπιση, διότι ενισχύει την ενοποιημένη προσέγγιση στην Ένωση των σχετικών ζητημάτων προς όφελος των πολιτών και της οικονομίας. Παράλληλα αναγνωρίζεται η σημασία των τομεακών πολιτικών ή και των ειδικών ρυθμίσεων για συγκεκριμένους λόγους, σε εθνικό επίπεδο, οι οποίες δεν θίγονται καθώς το κριτήριο υπαγωγής στον παρόντα νόμο είναι η αυστηρότητα των κανόνων,

η οποία οφείλει να είναι τουλάχιστον ίση με την προβλεπόμενη από τον παρόντα νόμο για να εξαιρεθεί από την εφαρμογή του κάποιο πεδίο, τομέας ή φορέας. Οι εφαρμοζόμενες πολιτικές εξειδικεύονται από την εθνική νομοθεσία με τον τρόπο που επιλέγει το κράτος μέλος, το οποίο και ορίζει τις τελικές λεπτομέρειες εντός του πλαισίου της ενωσιακής νομοθεσίας. Με αυτή την διαβαθμισμένη προσέγγιση επιτυγχάνεται η ενίσχυση της συνοχής μεταξύ των πολιτικών της Ένωσης, αλλά και ως προς την εδαφική δικαιοδοσία η διασυνοριακή ομοιομορφία στις εφαρμοζόμενες αρχές και πολιτικές ενώ διατηρεί ο εθνικός νομοθέτης τις εξουσίες που επιτρέπουν θέσπιση αυστηρότερων ή πρόσθετων κανόνων για ειδικούς λόγους (εθνική ασφάλεια, δημόσια τάξη κλπ).

**3. Συνέπειες στην Οικονομία**

Από την ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194/19.7.2016) σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση δεν προκαλείται πρόσθετη δαπάνη στον προϋπολογισμό του Υπουργείου Ψηφιακής Πολιτικής Επικοινωνιών και Ενημέρωσης.

**4. Συνέπειες στην κοινωνία και στους πολίτες**

Η παρούσα Οδηγία προστατεύει τα δικαιώματα των πολιτών και των επιχειρήσεων στην παροχή αξιόπιστων και αδιάλειπτων κατά το δυνατό υπηρεσιών και αγαθών, στους τομείς που έχουν προαναφερθεί, με αποτέλεσμα τόσο την ομογενοποίηση του βιοτικού επιπέδου στην Ένωση, προς όφελος των πολιτών, όσο και την ομογενοποίηση των υποχρεώσεων των φορέων που εμπλέκονται, προς όφελος του ανταγωνισμού των επιχειρήσεων στην Ένωση προσφέροντας ασφαλέστερο, υγιέστερο και ισχυρότερο οικονομικό περιβάλλον σε αυτές, το οποίο συμβάλλει στην οικονομική ανάπτυξη αλλά και στην παροχή καλύτερων υπηρεσιών στους πολίτες της Ένωσης.

**5. Συνέπειες στο φυσικό και πολιτιστικό περιβάλλον**

Οι συνέπειες για το φυσικό περιβάλλον είναι ευνοϊκές καθώς οι τομείς (π.χ. της ενέργειας, του πόσιμου ύδατος, κα) που συνδέονται άμεσα με το εν λόγω σχέδιο νόμου, καθίστανται ασφαλέστεροι λόγω της υποχρέωσης των φορέων να λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων από ηλεκτρονικές απειλές. Ως αποτέλεσμα ελαχιστοποιείται ο κίνδυνος επιβάρυνσης του περιβάλλοντος, λόγω τεχνολογικών καταστροφών κρίσιμων υποδομών, οι οποίες οφείλονται σε ηλεκτρονικές απειλές ενώ η έγκαιρη και αποτελεσματική αντιμετώπισή τους προκαλεί σχετική οικονομία πόρων.

Στο πολιτιστικό περιβάλλον ομοίως οι συνέπειες είναι ευνοϊκές διότι τα συστήματα δικτύου και πληροφοριών τα οποία συνδέονται άμεσα με την αναζήτηση και μετάδοση χρήσιμης πληροφορίας, μέρος της οποίας αφορά το ίδιο το πολιτιστικό γίγνεσθαι και το ιστορικό πολιτιστικό περιβάλλον, καθίστανται ανθεκτικότερα και με αυξημένες δυνατότητες αδιάλειπτης παροχής υπηρεσιών.

**6. Συνέπειες στη Δημόσια Διοίκηση και την απονομή της Δικαιοσύνης**

Ευνοϊκές είναι οι συνέπειες και στους τομείς της Δημόσιας Διοίκησης αλλά και της απονομής Δικαιοσύνης η οποία όμως δεν επηρεάζεται άμεσα. Η άμεση επιρροή στη Δημόσια Διοίκηση οφείλεται στη μεθοδολογία που πρέπει να υιοθετηθεί, να προσαρμοστεί ή να αναπτυχθεί για την εφαρμογή των προβλέψεων της παρούσας νομοθεσίας η οποία θα επιφέρει συνεπέστερη λειτουργία σε ορισμένους τομείς που πλέον θα υποχρεούνται να τηρούν πιο αυστηρούς κανόνες (πχ. μεταφορές, πόσιμο ύδωρ, ψηφιακές υπηρεσίες κλπ.). Έμμεσα λόγω της εφαρμογής της παρούσας νομοθεσίας η απόδοση δικαιοσύνης βελτιώνεται λόγω της συνεπέστερης λειτουργίας των ψηφιακών υπηρεσιών.

**7. Νομιμότητα**

Η ενσωμάτωση της Οδηγίας αποτελεί δικαίωμα και υποχρέωση των κρατών μελών μετά την παροχή ενός διαστήματος μεταβατικής περιόδου κατά την οποία τα κράτη μέλη προσαρμόζουν τη νομοθεσία τους και προετοιμάζονται για την πλήρη ενσωμάτωση.

**8. Αρμοδιότητα**

Αρμόδιο Υπουργείο για την υλοποίηση του παρόντος σχεδίου νόμου είναι το Υπουργείο Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης (ΥΨΗΠΤΕ). Για τη σύνταξη του σχεδίου νόμου συνεργάστηκαν υπηρεσίες του ΥΨΗΠΤΕ με ομόλογους φορείς άλλων υπουργείων.

**9. Τήρηση Νομοτεχνικών Κανόνων και Κωδικοποίηση**

Το παρόν σχέδιο νόμου διαμορφώθηκε κατόπιν των παρατηρήσεων και οδηγιών της ΚΕΝΕ.

**10. Διαφάνεια - Κοινωνική συμμετοχή**

Το παρόν σχέδιο νόμου διαμορφώθηκε κατόπιν διαβούλευσης με φορείς άλλων υπουργείων, σχετικούς με το εξειδικευμένο πεδίο της Κυβερνοασφάλειας και της προστασίας συστημάτων δικτύων και πληροφοριών.