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»

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

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 τον 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) αριθ. 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 κ-μ 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 κλπ.), γ) την τήρηση της αρχής της ίσης μεταχείρισης μεταξύ προσώπων και μεταξύ επιχειρήσεων, δ) τον 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 I ως και v της Οδηγίας), 17 άρθρα και 2 Παραρτήματα (I και II αντίστοιχα των II και III της Οδηγίας). Τα Κεφάλαια του νόμου Α΄,Β΄,Γ΄,Δ΄,Ε΄ αντιστοιχούν στα Κεφάλαια της Οδηγίας I,II,IV,V,VI-VII. Το Κεφάλαιο III 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

Πίνακας 1 : Αντιστοιχία άρθρων Οδηγίας με άρθρα του νόμου

Επίσης τα Παραρτήματα I και II του νόμου αντιστοιχούν στα Παραρτήματα II και III της Οδηγίας διότι το Παράρτημα I αυτής έχει ενσωματωθεί στο άρθρο 7 του παρόντος νόμου. Στα Παραρτήματα I και II παρατίθενται δύο πίνακες εκ των οποίων ο πρώτος (Παράρτημα I) 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 II) 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 (§ 1).

Με την § 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 ΕΚΑ) και οι βασικές αρμοδιότητές τους, οι οποίες με λεπτομέρεια ορίζονται στα οικεία άρθρα.

Με την § 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) 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) αριθ. 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 υπολοίπων 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 (§ 1). Ακολούθως προσδιορίζεται ο τρόπος εργασίας και συνεργασίας των εμπλεκομένων μερών (§ 2), τα γενικά κριτήρια χαρακτηρισμού (§ 3), η περίπτωση προσφοράς διασυνοριακών υπηρεσιών από φορέα (§ 4) και ο τρόπος υποβολής στην Επιτροπή ανά διετία των στοιχείων που απαιτούνται για την αξιολόγηση της εφαρμογής της Οδηγίας (§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 (§ 1). Ακολούθως, παρατίθενται παράγοντες που πρέπει να ληφθούν υπόψη κατά τον προσδιορισμό της σοβαρότητας της διατάραξης (§ 2) και λαμβάνεται ειδική μέριμνα (κριτήριο § 2 ζ), 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 ελαχίστου επιπέδου εναρμόνισης ενώ στο άρθρο 6 § 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. (§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 (§4) ή και εκτός αυτής, όσο και ως προς τις εθνικές αρχές και φορείς (§ 2), ενώ λαμβάνεται μέριμνα για την υλική και θεσμική υποστήριξη του ρόλου αυτού (§ 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 (§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 (§ 1). Ακολούθως ορίζονται οι παράμετροι για τον προσδιορισμό αντικτύπου ενός συμβάντος (§ 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 (§ 3), επαφιέμενης 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 (§ 4) και προβλέπεται η δυνατότητα της αρχής να εκδίδει εξειδικευμένες συστάσεις για την κοινοποίηση συμβάντων ανάλογα με τις περιστάσεις, λαμβανομένων υπόψη των παραμέτρων της § 2 (§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 επιβάλλει 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 (§1). επίσης, εξουσιοδοτείται η ΕΑΚ να εκδώσει υποχρεωτικές για τους ΦΕΒΥ οδηγίες συμμόρφωσης μετά την αξιολόγηση των ανωτέρω πληροφοριών (§2), ενώ για θέματα παραβίασης προσωπικών δεδομένων συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (§3). Η Εθνική Αρχή Κυβερνοασφάλειας εισηγείται την έκδοση υπουργικής απόφασης για την εξειδίκευση των ανωτέρω κριτηρίων και της μεθοδολογίας αξιολόγησης (§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 (§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 (§ 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 (§ 3). Για διασυνοριακά συμβάντα ακολουθούνται οι ίδιες αρχές όπως στην περίπτωση των ΦΕΒΥ ως προς την ενημέρωση των άλλων κρατών (§4) και του κοινού (§ 5). Ειδικά για τους ΠΨΥ δεν επιβάλλονται επιπλέον υποχρεώσεις ασφάλειας ή κοινοποίησης (§ 6), ενώ εξαιρούνται από το νόμο οι πολύ μικρές και οι μικρές επιχειρήσεις κατά την σύσταση 2003/361/ΕΚ της Επιτροπής (§ 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 (§ 1). Σε περίπτωση παροχής υπηρεσιών σε πολλά κράτη μέλη οι αρμόδιες αρχές συνεργάζονται (§ 2) ανταλλάσοντας 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 (§ 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 (§ 2). Παρά τον ορισμό αντιπροσώπου προβλέπεται ρητά ότι δεν μεταβάλλονται οι υποχρεώσεις γενικά του ΠΨΥ έναντι της διεθνούς νομοθεσίας ή των εθνικών νομικών τάξεων (§ 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 (§ 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 (§ 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 (§ 1). Για λόγους χρηστής διοίκησης ενημερώνεται ο ενδιαφερόμενος, τουλάχιστον 5 μέρες 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 (§ 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 σε ΦΕΚ εκτός των διατάξεων που ρητά αναφέρεται σε αυτές άλλη ημερομηνία έναρξης ισχύος.

Αθήνα 12 Νοεμβρίου 2018

ΟΙ ΥΠΟΥΡΓΟΙ

ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΕΝΗΜΕΡΩΣΗΣ

ΝΙΚΟΛΑΟΣ ΠΑΠΠΑΣ

ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ

ΠΑΝΑΓΙΩΤΗΣ ΚΑΜΜΕΝΟΣ

ΔΙΚΑΙΟΣΥΝΗΣ, ΔΙΑΦΑΝΕΙΑΣ
ΚΑΙ ΑΝΘΡΩΠΙΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

ΜΙΧΑΗΛ ΚΑΛΟΓΗΡΟΥ