Ε.Ε. Παρ. III(I)
Αρ. 5353, 11.9.2020

Κ.Δ.Π. 408/2020

Αριθμός 408

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ ΤΟΥ 2020

Απόφαση δυνάμει των άρθρων 17(ιη), (ιθ), (κβ), (κγ), και (λα), 20(1)(γ) και (4), 40, 43 και 46

Προοίμιο.
89(I) του 2020.

Η Αρχή Ψηφιακής Ασφάλειας (στο εξής "η Αρχή"), ασκώντας τις εξουσίες που της παρέχονται από τα άρθρα 17(ιη), (ιθ), (κβ), (κγ), (λα), 20(1)(γ),40, 43 και 46 του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020, αποφάσισε να εκδώσει την παρούσα Απόφαση με την οποία καθορίζεται το πλαίσιο μέτρων ψηφιακής ασφάλειας δικτύων και συστημάτων πληροφοριών στον τομέα των Δικτύων και Επικοινωνιών Πέμπτης Γενιάς (5G) στην Κύπρο.

Η Αρχή εκδίδει την παρούσα Απόφαση αφού έλαβε, μεταξύ άλλων, υπόψη:

Επίσημη Εφημερίδα της Ε.Ε: L194, 19.7.2016, σ.1.

(α) τις πρόνοιες της Οδηγίας (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση,

Επίσημη Εφημερίδα της Ε.Ε: L 321, 17.12.2018, σ.36.

(β) τις πρόνοιες της Οδηγίας (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Δεκεμβρίου του 2018, σχετικά με την θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών,

Επίσημη Εφημερίδα. Παράρτημα Τρίτο (Ι): 01.07.2011.

(γ) τις πρόνοιες του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020 (Ν.89(Ι)/2020),

(δ) το περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011 (Κ.Δ.Π. 253/2011),

(ε) το περί της Κοινοποίησης των Παραβιάσεων Ασφαλείας ή Απώλειας Ακεραιότητας Δικτύων ή και Υπηρεσιών Διάταγμα του 2013 (Κ.Δ.Π. 371/2013),

(στ) την Απόφαση Υπουργικού Συμβουλίου με αρ. 86.094 και ημερομηνίας. 01/11/2018,

Επίσημη Εφημερίδα. Παράρτημα Τρίτο (Ι): 25.10.2013.

(ζ) την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 (Κ.Δ.Π. 218/2019),

Επίσημη Εφημερίδα. Παράρτημα Τρίτο (Ι): 28.06.2019.

(η) την περί Ασφάλειας Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020 (Κ.Δ.Π. 389/2020),

Επίσημη Εφημερίδα. Παράρτημα Τρίτο (Ι): 21.08.2020.

(θ) την Εθνική Στρατηγική για την ασφάλεια δικτύων και συστημάτων πληροφοριών και την κυβερνοασφάλεια,

(ι) την Κυβερνοασφάλεια των Δικτύων και Επικοινωνιών Πέμπτης Γενιάς (5G) - Εργαλειοθήκη της ΕΕ για μέτρα μετριασμού των κινδύνων, Ομάδα Συνεργασίας NIS, ημερ. Ιανουαρίου 2020. Στην Απόφαση δεν περιλαμβάνονται οι πρόνοιες της Ευρωπαϊκής Εργαλειοθήκης για την επιβολή περιορισμών ή και αποκλεισμών στη βάση πολιτικών κριτηρίων (βλ. στρατηγικό μέτρο SM03 και σχετική παραπομπή στην παράγραφο 2.37 της συντονισμένης από την ΕΕ εκτίμηση επικινδυνότητας όπου προσδιορίζονται διάφοροι παράγοντες κινδύνου για την αξιολόγηση του προφίλ κινδύνου των προμηθευτών),

(ια) την Ανακοίνωση της Επιτροπής ημερ. 29 Ιανουαρίου 2020 προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Ασφαλής εγκατάστασης των δικτύων 5G στην ΕΕ - Εφαρμογή της εργαλειοθήκης της ΕΕ, και

(ιβ) το Πεδίο Απειλών για τα Δίκτυα 5G του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), Νοέμβριος 2019.

ΜΕΡΟΣ Ι

Εισαγωγικές Διατάξεις

Συνοπτικός τίτλος.

1. Η παρούσα Απόφαση θα αναφέρεται ως η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κυβερνοασφάλεια Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς 5G) Απόφαση του 2020.

Ερμηνεία.

2. (1) Στην παρούσα Απόφαση, εκτός αν από το κείμενο προκύπτει διαφορετική έννοια –

Κ.Δ.Π. 218/2019.

"Απόφαση κοινοποίησης συμβάντων του 2019" σημαίνει την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Κοινοποίηση Συμβάντων) Απόφαση του 2019 και περιλαμβάνει κάθε απόφαση που την τροποποιεί ή την αντικαθιστά·

Κ.Δ.Π.389/2020. "Απόφαση Μέτρων Ασφαλείας του 2020" σημαίνει την περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020 και περιλαμβάνει κάθε απόφαση που την τροποποιεί ή την αντικαθιστά·

"βασικά πάγια στοιχεία δικτύου 5G" σημαίνει τα κρίσιμης σημασίας και ευαίσθητα πάγια στοιχεία δικτύου 5G και περιλαμβάνει τουλάχιστον τις λειτουργίες δικτύου πυρήνα (core network), λειτουργίες διαχείρισης και ενορχήστρωσης δικτύου (network orchestration and management) και λειτουργίες δικτύου πρόσβασης 5G υπεύθυνες για την κατανομή πόρων, διαχείριση προσβάσεων, επικοινωνίες καθώς επίσης και την ασφάλεια δικτύου (ακεραιότητα, εμπιστευτικότητα, αυθεντικότητα και διαθεσιμότητα), όπως ορίζονται στο Παράρτημα ΙΙΙ·

Παράρτημα ΙΙΙ.

Κ.Δ.Π. 253/2011. "Διάταγμα Ασφάλειας Δικτύων" σημαίνει το περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011 και περιλαμβάνει κάθε απόφαση που το τροποποιεί ή το αντικαθιστά·

"δίκτυο 5G" σημαίνει το δίκτυο κινητών επικοινωνιών πέμπτης γενιάς (5^{th} Generation)·

"κατευθυντήριες γραμμές" σημαίνει τις Αποφάσεις οι οποίες εκδίδονται από την Αρχή δυνάμει του άρθρου 46 του Νόμου και οι οποίες αποσκοπούν στην αποσαφήνιση και ρύθμιση διαδικασιών, μεθόδων και χρονοδιαγραμμάτων της παρούσας Απόφασης·

89(Ι) του 2020. "Νόμος" σημαίνει τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο του 2020 και περιλαμβάνει κάθε νόμο που τον τροποποιεί ή τον αντικαθιστά·

"Οδηγία (ΕΕ) 2016/1148" σημαίνει την Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση·

"Οδηγία (ΕΕ) 2018/1972" σημαίνει την Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Δεκεμβρίου του 2018, σχετικά με την θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών·

"παροχείς διαχειριζόμενων υπηρεσιών (Managed Service Providers)" σημαίνει τους παροχείς υπηρεσιών στους οποίους ανατίθεται η παρακολούθηση δικτύων, η διαχείριση περιστατικών ασφαλείας, η διαχείριση πόρων και αλλαγών καθώς επίσης και λογαριασμών χρηστών και υπηρεσιών. Οι υπηρεσίες αυτές παρέχονται δυνάμει συμφωνιών παροχής υπηρεσιών μεταξύ των παροχέων ηλεκτρονικών επικοινωνιών και των παροχέων διαχειριζόμενων υπηρεσιών·

"παροχείς ηλεκτρονικών επικοινωνιών" ή “παροχείς” σημαίνει τους παροχείς δικτύου ηλεκτρονικών επικοινωνιών και τους παροχείς υπηρεσιών ηλεκτρονικών επικοινωνιών·

"προμηθευτής" σημαίνει τον κατασκευαστή τηλεπικοινωνιακού εξοπλισμού και περιλαμβάνει τρίτους προμηθευτές όπως παροχείς υπηρεσιών νεφοϋπολογιστικής και υπεργολάβους ασφάλειας και συντήρησης.

“συνδεδεμένες εταιρίες’’ σημαίνει οποιεσδήποτε δύο ή περισσότερες εταιρίες ενός συγκροτήματος εταιριών.

‘’συγκρότημα εταιριών’’ σημαίνει το σύνολο εταιριών το οποίο αποτελείται από τη μητρική και τη θυγατρική ή τις θυγατρικές.

(2) Όροι που χρησιμοποιούνται στην παρούσα Απόφαση και δεν ορίζονται διαφορετικά , έχουν την έννοια που αποδίδει σε αυτούς ο Νόμος ή η Οδηγία (ΕΕ) 2016/1148 ή η Οδηγία (ΕΕ) 2018/1972.

Σκοπός. 3. (1) Ο σκοπός της παρούσας Απόφασης είναι η εισαγωγή ελάχιστων απαιτήσεων ασφαλείας ικανών να μετριάσουν τους κύριους κινδύνους που αφορούν την ασφάλεια των Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Πέμπτης Γενιάς (5G).

(2) Με την επιφύλαξη των μέτρων που καθορίζονται στην Απόφαση Μέτρων Ασφάλειας του 2020 (Κ.Δ.Π. 389/2020) και στο Διάταγμα του 2011 (Κ.Δ.Π. 253/2011) όσον αφορά το δίκτυο και την υπηρεσία ηλεκτρονικών επικοινωνιών Πέμπτης Γενιάς (5G), η παρούσα απόφαση καθορίζει επιπρόσθετα ειδικότερα μέτρα.

ΜΕΡΟΣ ΙΙ

Εξουσίες Αρχής και Υποχρεώσεις Παροχέων

Εξουσίες Αρχής. 4. (1) Για τους σκοπούς της παρούσας Απόφασης, η Αρχή ασκεί τις εξουσίες που της χορηγούνται από τα άρθρα 17(ιη), (ιθ), (κβ), (κγ), και (λα), 20(1)(γ) και (4), 40, 43 και 46 του Νόμου, το Διάταγμα Ασφάλειας Δικτύων, την Απόφαση Κοινοποίησης Συμβάντων του 2019 και την Απόφαση Μέτρων Ασφαλείας του 2020.

(2) Χωρίς επηρεασμό των όσων αναφέρονται στο εδάφιο (1) ανωτέρω και τηρουμένων των διατάξεων του εδαφίου (3) του άρθρου 15 και του άρθρου 18 του Νόμου και του πλαισίου γενικής πολιτικής σε σχέση με την ψηφιακή ασφάλεια που εκδίδεται από τον Υφυπουργό δυνάμει του άρθρου 16 του Νόμου, η Αρχή δύναται:

(α) να απαιτεί από τους παροχείς ηλεκτρονικών επικοινωνιών την παροχή τεχνικών, οικονομικών και άλλων πληροφοριών και εγγράφων αναφορικά με την ασφάλεια και λειτουργεία των δικτύων και επικοινωνιών Πέμπτης Γενιάς 5G,

(β) να επιβάλλει περιορισμούς, απαγορεύσεις, ενισχυμένες διατάξεις ασφαλείας και συγκεκριμένες απαιτήσεις στους παροχείς ηλεκτρονικών επικοινωνιών όσον αφορά τους προμηθευτές τους

συμπεριλαμβανομένων των προμηθευτών υψηλού κινδύνου και τους παροχείς διαχειριζόμενων υπηρεσιών, σύμφωνα με τις διατάξεις του Μέρους VI της παρούσας Απόφασης,

(γ) να διενεργεί έρευνες και ελέγχους στους παροχείς ηλεκτρονικών επικοινωνιών για να διασφαλίζει ότι τηρούν τους απαραίτητους ελέγχους ασφαλείας στην αλυσίδα εφοδιασμού των δικτύων κινητών επικοινωνιών,

(δ) να επιβάλλει πρόσθετα μέτρα καθώς και να διενεργεί ελέγχους στις πολιτικές ασφάλειας πληροφοριών και τα βασικά και ειδικά μέτρα ασφάλειας των δικτύων κινητών επικοινωνιών που εφαρμόζουν οι παροχείς ηλεκτρονικών επικοινωνιών,

(ε) να επιβάλλει διοικητικά πρόστιμα σε παροχείς ηλεκτρονικών επικοινωνιών για παράβαση των διατάξεων της παρούσας Απόφασης, σύμφωνα με τις διατάξεις του Νόμου,

(στ) να υποχρεώνει τους παροχείς ηλεκτρονικών επικοινωνιών όπως, τηρουμένων των προνοιών των άρθρων 2(2), 2(3), 17 και 19 του Νόμου και εφόσον η Αρχή κρίνει σκόπιμο κατόπιν αιτήματος της Αστυνομίας, να διαθέτουν πληροφορίες προς την Αστυνομία, για σκοπούς Δημόσιας Τάξεως και Εθνικής Ασφάλειας της Δημοκρατίας.

Παροχή πληροφοριών στην Αρχή.

(3) Για το σκοπό εφαρμογής της παρούσας Απόφασης, η Αρχή δύναται να απαιτεί από τους παροχείς ηλεκτρονικών επικοινωνιών:

(α) να κοινοποιούν για έλεγχο εγγράφως την πολιτική ασφάλειας πληροφοριών και τα βασικά μέτρα ασφάλειας στην Αρχή τηρουμένων των κατευθυντήριων γραμμών που εκδίδονται από την Αρχή,

(β) να παρέχουν εγγράφως τεκμηρίωση και να διαβιβάζουν πληροφορίες και έγγραφα στην Αρχή σε ηλεκτρονική μορφή για την αξιολόγηση της ασφάλειας δικτύων και των υπηρεσιών τους καθώς και σχετικά με τα μέτρα ασφάλειας που έχουν ληφθεί και τεκμηριωθεί από αυτούς σύμφωνα με το εδάφιο (α) και την πολιτική ασφάλειας πληροφοριών τους,

(γ) να εφαρμόζουν όλες τις υποχρεώσεις που αφορούν την παροχή πληροφοριών και οι οποίες αναφέρονται λεπτομερώς στα άρθρα 10 και 12 της παρούσας Απόφασης,

(δ) να παρέχουν τις απαιτούμενες πληροφορίες όσον αφορά τα μέτρα εφοδιασμού, την πολιτική ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής καθώς και τη στρατηγική πολλαπλών προμηθευτών όπως αυτές αναφέρονται λεπτομερώς στο άρθρο 13 της παρούσας Απόφασης, και

(ε) να υποβάλουν έγγραφα και πληροφορίες όσον αφορά την κοινοποίηση συμβάντων και την εκτίμηση της ασφάλειας των δικτύων και συστημάτων πληροφοριών τους, μετά από αιτιολογημένο αίτημα της Αρχής.

ΜΕΡΟΣ III

Βασικά Μέτρα Ψηφιακής Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών

Τήρηση βασικών μέτρων ψηφιακής ασφάλειας και πολιτικής ασφάλειας πληροφοριών.

5. (1) Προκειμένου να διασφαλιστεί ένα κατάλληλο επίπεδο ασφάλειας των δικτύων κινητών επικοινωνιών και για το σκοπό αποφυγής συμβάντων παραβίασης ασφάλειας, οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να σχεδιάσουν, να υιοθετήσουν και να τεκμηριώσουν βασικά μέτρα ασφαλείας και πολιτική ασφάλειας πληροφοριών. Τα βασικά μέτρα ασφαλείας και η πολιτική ασφάλειας πληροφοριών οφείλουν να συνάδουν με τα Διατάγματα και τις Αποφάσεις που εκδίδονται ή και εφαρμόζονται δυνάμει του Νόμου και να καλύπτουν τους τομείς που περιγράφονται στα άρθρα 5 έως και 22 της Απόφασης Μέτρων Ασφαλείας του 2020 και στα άρθρα 5 έως και 19 του Διατάγματος Ασφάλειας Δικτύων.

(2) Οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν, κατ' ελάχιστον:

(α) να κοινοποιούν για έλεγχο εγγράφως την πολιτική ασφάλειας πληροφοριών και τα βασικά μέτρα ασφάλειας στην Αρχή τηρουμένων των κατευθυντηρίων γραμμών που εκδίδονται από την Αρχή,

(β) να παρέχουν εγγράφως τεκμηρίωση και να διαβιβάζουν πληροφορίες και έγγραφα στην Αρχή σε ηλεκτρονική μορφή για την αξιολόγηση της ασφάλειας των δικτύων και των υπηρεσιών τους καθώς και σχετικά με τα μέτρα ασφαλείας που έχουν ληφθεί και τεκμηριωθεί από αυτούς σύμφωνα με το εδάφιο 1 και την πολιτική ασφάλειας πληροφοριών τους,

(γ) να καταγράφουν και να εξηγούν στην Αρχή τον τρόπο εφαρμογής των βασικών τεχνικών μέτρων ασφαλείας που διατηρούν για το δίκτυο τους,

(δ) να εφαρμόζουν τις ελάχιστες απαιτήσεις και υποχρεώσεις σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών, σύμφωνα με τις διατάξεις του Διατάγματος Ασφάλειας Δικτύων και της Απόφασης Μέτρων Ασφαλείας του 2020,

(ε) να διατηρούν ενημερωμένο αρχείο πληροφοριών για τη γενική πολιτική ασφάλειας, των πολιτικών διαχείρισης συμβάντων και των εφαρμοστέων διαδικασιών για βασικά συστήματα δικτύου και πληροφοριών.

ΜΕΡΟΣ IV

Ειδικά Μέτρα Ασφάλειας Δικτύων 5G

Τήρηση μέτρων ασφαλείας μέσω συμμόρφωσης με

6. (1) Προκειμένου να διασφαλιστεί επαρκές επίπεδο ασφάλειας για τα δίκτυα 5G, οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να συμμορφώνονται με τα πρότυπα που καθορίζονται στο Μέρος Α του Παραρτήματος Ι και να λαμβάνουν υπόψη τα υπόλοιπα έγγραφα που περιλαμβάνει

πρότυπα ασφάλειας. Παράρτημα Ι.

το Παράρτημα Ι, καθώς και να υποβάλλουν προς την Αρχή δήλωση συμμόρφωσης με τα πρότυπα, για πρώτη φορά και σε σχέση με την τρέχουσα κατάσταση, το αργότερο μέχρι την 30 Ιουνίου 2021 και στη συνέχεια περιοδικά σε διαστήματα που δεν υπερβαίνουν τα δύο έτη ή όπως θα καθορίζεται εκάστοτε από την Αρχή.

(2) Οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να υποβάλουν τη δήλωση συμμόρφωσης με τα πρότυπα που καθορίζονται στο Παράρτημα Ι μετά από έλεγχο που πραγματοποιούν οι ίδιοι (self-assesment) για το σχεδιασμό δικτύου και την αρχιτεκτονική που ακολουθείται για την υποδομή του 5G.

Διασφάλιση αυστηρών ελέγχων πρόσβασης στο δίκτυο 5G.

7. (1) Οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να εφαρμόζουν αυστηρά τεχνικά μέτρα ασφάλειας σχετικά με τον περιορισμό πρόσβασης στα δίκτυα 5G. Τα τεχνικά μέτρα ασφαλείας σχετικά με τον περιορισμό πρόσβασης στα δίκτυα 5G οφείλουν να διασφαλίζουν κατ' ελάχιστον τα εξής:

(α) την εφαρμογή της αρχής του ελάχιστου προνομίου, μέσω της οποίας εξασφαλίζεται ότι ελαχιστοποιούνται διάφορα δικαιώματα στο δίκτυο, περιλαμβανομένων δικαιωμάτων πρόσβασης μεταξύ των λειτουργιών δικτύου, δικαιωμάτων των διαχειριστών δικτύου και της ρύθμισης παραμέτρων εικονικοποίησης,

(β) την εφαρμογή του διαχωρισμού των καθηκόντων,

(γ) την εφαρμογή διαδικασιών οι οποίες διασφαλίζουν ότι τα εν λόγω μέτρα ελέγχου πρόσβασης εφαρμόζονται συνεχώς και εξελίσσονται παράλληλα με την ανάπτυξη του δικτύου 5G, και

(δ) τον έλεγχο προσβάσεων και προνομίων για όλους τους χρήστες και ρόλους σε όλες τις εφαρμογές και τόπους του εσωτερικού δικτύου των παροχέων ανά τακτά χρονικά διαστήματα τουλάχιστον μια φορά τον χρόνο προκειμένου να διασφαλιστεί η εγκεκριμένη πρόσβαση σε εφαρμογές, συστήματα και πληροφορίες.

(2) Κατά τον καθορισμό των μέτρων ελέγχου πρόσβασης, θα πρέπει να λαμβάνεται ιδιαίτερη μέριμνα από τους παροχείς ηλεκτρονικών επικοινωνιών ώστε να διασφαλίζεται ότι ελαχιστοποιείται και/ή αποφεύγεται, όποτε είναι δυνατόν, η απομακρυσμένη πρόσβαση τρίτων, περιλαμβανομένων προμηθευτών και ιδίως προμηθευτών που θεωρούνται υψηλού κινδύνου. Όταν η απομακρυσμένη πρόσβαση είναι αναγκαία, για παράδειγμα για την αντιμετώπιση διακοπών υπηρεσίας, ο παροχέας θα πρέπει να εφαρμόζει κατάλληλες διαδικασίες επαλήθευσης ταυτότητας, εξουσιοδότησης, καταγραφής και ελέγχου ώστε να έχει σαφή εικόνα όσον αφορά την πρόσβαση στα δεδομένα και τις αλλαγές της ρύθμισης παραμέτρων ή τις τροποποιήσεις του δικτύου.

(3) Η πρόσβαση στα δίκτυα 5G των παροχέων θα πρέπει να περιορίζεται σε εξειδικευμένο προσωπικό που έχει υποβληθεί σε έλεγχο ασφαλείας, σύμφωνα με τις διατάξεις της Απόφασης Μέτρων Ασφάλειας του 2020 σχετικά με την ασφάλεια ανθρώπινων πόρων. Τα τεχνικά μέτρα ασφάλειας εφαρμόζονται σε όλες τις προσβάσεις, συμπεριλαμβανομένης της προνομιακής πρόσβασης και θα πρέπει να καλύπτουν όλα τα συστήματα εντός του παροχέα, συμπεριλαμβανομένων των λειτουργιών δικτύου και ρύθμιση παραμέτρων εικονικοποίησης (virtualisation configuration).

Διασφάλιση της ασφάλειας διαχείρισης λειτουργίας και παρακολούθησης δικτύου 5G και ενίσχυση της ακεραιότητας.

8. (1) Οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να συμμορφώνονται τουλάχιστον με τις ακόλουθες επιπρόσθετες απαιτήσεις:

(α) λειτουργία του Κέντρου Λειτουργίας Δικτύου (NOC) και του Κέντρου Επιχειρήσεων Ασφαλείας (SOC) στις εγκαταστάσεις του παροχέα ή συνδεδεμένης εταιρίας, υπό τον έλεγχο του παροχέα ή συγκροτήματος εταιριών στην οποία εντάσσεται ο παροχέας, και εντός της Δημοκρατίας ή της Ευρωπαϊκής Ένωσης,

(β) αποτελεσματική παρακολούθηση όλων των κρίσιμων στοιχείων του δικτύου και ευαίσθητων τμημάτων των δικτύων 5G από την NOC / SOC για τον εντοπισμό ανωμαλιών και τον εντοπισμό και την πρόληψη απειλών,

(γ) πραγματοποίηση δοκιμών και ελέγχων ασφαλείας στα κέντρα επιχειρήσεων ασφαλείας προκειμένου να διασφαλίζουν την απαραίτητη κάλυψη παρακολούθησης των πόρων αλλά και την καταγραφή της εκάστοτε δυνατότητας στον εντοπισμό απειλών,

(δ) προστασία της διαχείρισης δικτύων ή υπηρεσιών επικοινωνιών με σκοπό την αποτροπή μη εξουσιοδοτημένων αλλαγών σε στοιχεία δικτύου ή υπηρεσιών,

(ε) φυσική προστασία των κρίσιμων στοιχείων του δικτύου και ευαίσθητων τμημάτων των δικτύων 5G με προσέγγιση βασιζόμενη στον κίνδυνο για σταθμούς βάσης και άλλα σημεία πρόσβασης στο δίκτυο, περιλαμβανομένων σημείων πολλαπλής προσπέλασης (multi-access edge computing),

(στ) χρήση κατάλληλων εργαλείων και διαδικασιών για διασφάλιση ακεραιότητας ενημερώσεων λογισμικού και αξιόπιστη αναγνώριση, ιχνηλασιμότητα και διαχείριση αλλαγών (change management) και κατάστασης ενημέρωσης κώδικα και εφαρμογή επιδιορθώσεων ασφαλείας,

Παράρτημα Ι.

(ζ) εφαρμογή βέλτιστων πρακτικών ασφάλειας για την εικονικοποίηση δικτυακών λειτουργιών σύμφωνα με πρότυπα όπως αυτά που αναφέρονται στο Παράρτημα Ι (Δ και ΣΤ),

(η) εφαρμογή μέτρων και πρακτικών ασφάλειας που περιλαμβάνονται στις ισχύουσες νομοθεσίες, σχετικά με τους τομείς που αναφέρονται στο άρθρο 5, σε δίκτυα νεφοϋπολογιστικής και συστήματα/δίκτυα εικονικοποίησης, και

(θ) ελέγχους και αναθεωρήσεις σχετικά με τις ρυθμίσεις παραμέτρων (configuration reviews) των συστημάτων και υποδομών νεφοϋπολογιστικής (cloud systems & infrastructure) ανά τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το τρίμηνο) όπως επίσης μετά από κάθε σημαντική αλλαγή που ενδέχεται να επηρεάσει την αρχιτεκτονική συστημάτων, δικτύων ή δεδομένων.

(2) Τηρουμένων των διατάξεων του εδαφίου (3) του άρθρου 15 και του άρθρου 18 του Νόμου και του πλαισίου γενικής πολιτικής σε σχέση με την ψηφιακή ασφάλεια που εκδίδεται από τον Υφυπουργό δυνάμει του άρθρου 16 του Νόμου η Αρχή έχει το δικαίωμα με αιτιολογημένη απόφαση της να επιβάλλει περιορισμούς, συμπεριλαμβανομένων πιθανών αποκλεισμών ή ενισχυμένες διατάξεις ασφαλείας καθώς και να διεξάγει ελέγχους και διαβουλεύσεις με παροχείς ηλεκτρονικών επικοινωνιών όσον αφορά στην υιοθέτηση και εφαρμογή των μέτρων ασφαλείας που αναφέρονται στο παρόν Μέρος.

(3) Σε περίπτωση που υιοθετείται λειτουργία του 5G σε μη αυτόνομη διάταξη (non-standalone), όπως αναφέρεται στο άρθρο 11(3)(γ), θα πρέπει να υλοποιείται κάθε δυνατό μέτρο, τουλάχιστον όπως αναφέρεται στα Μέρη ΙΙΙ και IV της παρούσας Απόφασης για τη διασφάλιση επαρκούς επιπέδου ασφάλειας για το δίκτυο 5G.

Πρότυπα.

9. Οποιαδήποτε αναφορά σε πρότυπα στην παρούσα Απόφαση και στα Παραρτήματά της, περιλαμβάνει κάθε πρότυπο που εκάστοτε τα τροποποιεί ή τα αντικαθιστά.

Νοείται ότι στις περιπτώσεις που αναφέρονται στο παρόν άρθρο, η δήλωση συμμόρφωσης που αναφέρεται στο άρθρο 6 (1) θα γίνεται στην εκάστοτε επόμενη περιοδική δήλωση που θα υποβάλλεται στην Αρχή.

ΜΕΡΟΣ V

Επιχειρησιακή Συνέχεια και Αντιμετώπιση Έκτακτων Συνθηκών

Μέτρα εξασφάλισης λειτουργίας του δικτύου και πολιτική επιχειρησιακής συνέχειας και εκτάκτων συνθηκών.

10. (1) Προκειμένου να διασφαλιστεί ένα κατάλληλο επίπεδο ασφάλειας και για το σκοπό εξασφάλισης της ακεραιότητας και επιχειρησιακής συνέχειας, οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να σχεδιάσουν, υιοθετήσουν και τεκμηριώσουν βασικά μέτρα εξασφάλισης λειτουργίας του δικτύου και μία πολιτική επιχειρησιακής συνέχειας και εκτάκτων συνθηκών. Τα βασικά μέτρα διασφάλισης της ασφαλούς λειτουργίας του δικτύου και η πολιτική επιχειρησιακής συνέχειας και έκτακτων συνθηκών θα πρέπει να συντάσσονται, να εγκρίνονται και να εφαρμόζονται από τον παροχέα σύμφωνα με τις διατάξεις του Νόμου, των Διαταγμάτων και των Αποφάσεων που εκδίδονται ή και εφαρμόζονται δυνάμει του Νόμου και να καλύπτουν τουλάχιστον τους τομείς που περιγράφονται στα άρθρα 5 έως και 22 της Απόφασης Μέτρων Ασφαλείας του 2020 και στα άρθρα 5 έως και 19 του Διατάγματος Ασφάλειας Δικτύων.

(2) Οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν κατ΄ελάχιστον:

(α) να κοινοποιούν για έλεγχο στην Αρχή τα βασικά μέτρα εξασφάλισης λειτουργίας του δικτύου και την πολιτική επιχειρησιακής συνέχειας και εκτάκτων συνθηκών λαμβάνοντας υπόψη τις κατευθυντήριες γραμμές που είναι δυνατό να εκδίδονται από την Αρχή,

(β) να παρέχουν εγγράφως τεκμηρίωση και να διαβιβάζουν πληροφορίες και έγγραφα στην Αρχή σε ηλεκτρονική μορφή σχετικά με τα μέτρα ασφαλείας που έχουν ληφθεί και τεκμηριωθεί από αυτούς σύμφωνα με το εδάφιο (1) και την πολιτική επιχειρησιακής συνέχειας και εκτάκτων συνθηκών,

(γ) να τηρούν αρχείο επικοινωνιών με την Αρχή το οποίο να είναι διαθέσιμο για επιθεώρηση και λήψη αντιγράφων από την Αρχή,

(δ) να τηρούν τις υποχρεώσεις κοινοποίησης και τις άλλες υποχρεώσεις που προνοούνται στο Νόμο και το περί της Κοινοποίησης των Παραβιάσεων Ασφαλείας ή Απώλειας Ακεραιότητας Δικτύων ή και Υπηρεσιών Διάταγμα του 2013 περιλαμβανομένου κάθε Απόφασης που το τροποποιεί ή το αντικαθιστά, και

(ε) να ελέγχουν και να αναθεωρούν το πεδίο ορισμού των πλάνων επιχειρησιακή συνέχειας προκειμένου να διασφαλίσουν ότι όλοι οι απαραίτητοι πόροι και ειδικότερα όσοι πόροι σχετίζονται με τα δίκτυα 5G περιλαμβάνονται όπως επίσης και τα ανάλογα μέτρα για καθένα από τους πόρους.

(3) Τηρουμένων των διατάξεων του εδαφίου (3) του άρθρου 15 και του άρθρου 18 του Νόμου και του πλαισίου γενικής πολιτικής σε σχέση με την ψηφιακή ασφάλεια που εκδίδεται από τον Υφυπουργό δυνάμει του άρθρου 16 του Νόμου, η Αρχή έχει το δικαίωμα να επιβάλλει με αιτιολογημένη απόφασή της, περιορισμούς, συμπεριλαμβανομένων πιθανών αποκλεισμών ή ενισχυμένες διατάξεις ασφαλείας καθώς και να διεξάγει ελέγχους και διαβουλεύσεις με παροχείς ηλεκτρονικών επικοινωνιών όσον αφορά την υιοθέτηση και εφαρμογή των μέτρων ασφαλείας που αναφέρονται στο παρόν Μέρος.

ΜΕΡΟΣ VI

Διαχείριση Προμηθευτών

Βασικά μέτρα ασφάλειας εφοδιασμού και πολιτική προμήθειας εξοπλισμού και συμμετοχής προμηθευτών.

11. (1) Προκειμένου να διασφαλιστεί ένα κατάλληλο επίπεδο ασφάλειας εφοδιασμού, οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν:

(α) να σχεδιάσουν, να υιοθετήσουν και να τεκμηριώσουν βασικά και ειδικά μέτρα ασφάλειας εφοδιασμού και πολιτική προμήθειας εξοπλισμού και συμμετοχής προμηθευτών. Τα βασικά και ειδικά μέτρα ασφάλειας εφοδιασμού και η πολιτική προμήθειας εξοπλισμού και συμμετοχής προμηθευτών οφείλουν να συνάδουν με το Νόμο, τα Διατάγματα, τις Αποφάσεις και την παρούσα Απόφαση,

(β) να σχεδιάσουν και να υιοθετήσουν μία πολιτική ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής (third line support), με την οποία να καθορίζονται όρια όσον αφορά τα είδη δραστηριότητας και προϋποθέσεις βάσει των οποίων οι παροχείς ηλεκτρονικών επικοινωνιών μπορούν να αναθέτουν εξωτερικά συγκεκριμένες λειτουργίες σε παροχείς διαχειριζόμενων υπηρεσιών, τόσο για τη φυσική όσο και για την εικονική υποδομή των δικτύων κινητών επικοινωνιών, και

(γ) να σχεδιάσουν, να υιοθετήσουν και να τεκμηριώσουν στρατηγική πολλαπλών προμηθευτών για την αποφυγή ή τον περιορισμό οποιασδήποτε σημαντικής εξάρτησης από έναν μοναδικό προμηθευτή (ή από προμηθευτές με υψηλό προφίλ κινδύνου). Η στρατηγική πολλαπλών προμηθευτών θα λαμβάνει υπόψη τους τεχνικούς περιορισμούς και τις απαιτήσεις διαλειτουργικότητας μεταξύ των διαφόρων τμημάτων ενός δικτύου 5G.

(2) Για το σχεδιασμό, την υιοθέτηση και τεκμηρίωση των μέτρων ασφάλειας εφοδιασμού, της πολιτικής ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής (third line support) και της στρατηγικής πολλαπλών προμηθευτών, τα οποία αναφέρονται στο εδάφιο (1) του παρόντος άρθρου, οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν να λαμβάνουν υπόψη τα αποτελέσματα της αξιολόγησης κινδύνου σύμφωνα με τις διατάξεις του άρθρου 12 και να τεκμηριώνουν τις αποφάσεις τους σύμφωνα με τις διατάξεις του άρθρου 13, λαμβάνοντας υπόψη τυχόν περιορισμούς που επιβάλλονται από την Αρχή σχετικά με ευαίσθητα στοιχεία της υποδομής ή και γεωγραφικούς περιορισμούς σε σημεία με αυξημένη σημασία ασφάλειας όπως καθορίζεται στο άρθρο 14 και στο Παράρτημα ΙΙΙ.

Παράρτημα ΙΙΙ.

(3) Η στρατηγική πολλαπλών προμηθευτών που αναφέρεται στα άρθρα 11(1)(γ) και 13(1)(γ), πρέπει να υποβάλλεται από τους παροχείς στην Αρχή εντός τεσσάρων (4) μηνών από την ημερομηνία αδειοδότησής τους για χρήση ραδιοφάσματος 5G. Κατ' εξαίρεση, σε ειδικές περιπτώσεις, μετά από αιτιολογημένο αίτημα του παροχέα η Αρχή δύναται να αποδεχτεί παράταση των τεσσάρων (4) μηνών.

Η στρατηγική πολλαπλών προμηθευτών θα έχει ισχύ πέντε (5) έτη από την ημερομηνία υποβολής της στην Αρχή. Κατ' εξαίρεση σε ειδικές περιπτώσεις και για λόγους οι οποίοι δεν μπορούσαν να προβλεφθούν εκ των προτέρων, μετά από αιτιολογημένο αίτημα του παροχέα, η Αρχή δύναται να αποδεχτεί διάρκεια ισχύος της στρατηγικής πέραν των πέντε (5) ετών.

Η στρατηγική πολλαπλών προμηθευτών πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα:

(α) περιγραφή της συνολικής στρατηγικής, του αναμενόμενου οφέλους υλοποίησης της, τα ρίσκα που έχουν εντοπιστεί καθώς και τα μέτρα και τις ενέργειες μετριασμού τους,

(β) περιγραφή της προσέγγισης του παροχέα σχετικά με την ανάπτυξη του ραδιοδικτύου πρόσβασης 5G (RAN),

(γ) περιγραφή της προσέγγισης του παροχέα σχετικά με τη λειτουργία του 5G σε μη αυτόνομη διάταξη (non-standalone), δηλαδή με ραδιοδίκτυο πρόσβασης 5G και δίκτυο πυρήνα που δεν είναι 5G, και πως θα λειτουργεί με τον υπάρχοντα πυρήνα,

(δ) περιγραφή της προσέγγισης του παροχέα σχετικά με τη μετάβαση σ' ένα πυρήνα 5G (πλήρες δίκτυο 5G σε αυτόνομη διάταξη – standalone),

(ε) λεπτομερής περιγραφή των επιλογών του παροχέα και πως θα εφαρμοστούν στην πράξη, σχετικά με τη χρήση εξοπλισμού και λογισμικών από συνδυασμό προμηθευτών στα επιμέρους στοιχεία της υποδομής, όπως αναφέρονται στο Παράρτημα ΙΙΙ,

Παράρτημα ΙΙΙ.

(στ) περιγραφή των απαραίτητων αλλαγών ή αντικαταστάσεων που θα πρέπει να πραγματοποιηθούν σε υφιστάμενο εξοπλισμό και στοιχεία δικτύου για να συμμορφωθούν με τους σχετικούς περιορισμούς που είναι δυνατόν να επιβληθούν σχετικά με προμηθευτές υψηλού κινδύνου, δυνάμει του άρθρου 15(3).

Αξιολόγηση κινδύνου προμηθευτών. Παράρτημα ΙΙ.

12. (1) Οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν:

(α) να διεξάγουν, στη βάση αυστηρών κριτηρίων που καθορίζονται με κατευθυντήριες γραμμές που εκδίδει η Αρχή, οι οποίες περιγράφονται στο Παράρτημα ΙΙ και με εργαλεία (ερωτηματολόγια) που θα παρέχονται από την Αρχή, αξιολογήσεις κινδύνου σχετικά με τους προμηθευτές με τους οποίους προτίθενται να συνεργαστούν και να κοινοποιούν στην Αρχή τα αποτελέσματα της αξιολόγησης του προφίλ κινδύνου των προμηθευτών, πριν τη σύναψη νέων ή τροποποιητικών συμβάσεων με προμηθευτές, προκειμένου η Αρχή σύμφωνα με τις διατάξεις του άρθρου 15, να εξετάσει τα αποτελέσματα και, λαμβάνοντας υπόψιν πληροφορίες από αρμόδιους κρατικούς φορείς, να εντοπίσει υψηλού κινδύνου προμηθευτές,

(β) να διατηρούν και να παρέχουν στην Αρχή κατάλογο με τους προμηθευτές που παρέχουν τον εξοπλισμό των δικτύων 5G και/ή που παρέχουν υπηρεσίες σχετικά με τα δίκτυα 5G,

(γ) να εφαρμόζουν επαρκείς ελέγχους και διαδικασίες και να κοινοποιούν στην Αρχή μέτρα ασφάλειας για τη διαχείριση πιθανών εναπομενόντων κινδύνων (residual risks), όπως τακτικούς ελέγχους της αλυσίδας εφοδιασμού και εκτιμήσεις επικινδυνότητας, ισχυρή διαχείριση κινδύνων και ειδικές απαιτήσεις για τους προμηθευτές με βάση το προφίλ κινδύνου τους.

Τεκμηρίωση ενεργειών παροχέα ηλεκτρονικών επικοινωνιών. Μέτρα ασφάλειας εφοδιασμού.

13. (1) Προκειμένου να τεκμηριώσουν τις ενέργειες και αποφάσεις που λαμβάνουν σύμφωνα με τις διατάξεις του άρθρου 11, οι παροχείς οφείλουν:

(α) όσον αφορά τα μέτρα ασφάλειας εφοδιασμού:

(i) να κοινοποιούν για έλεγχο στην Αρχή τα βασικά μέτρα ασφάλειας εφοδιασμού και την πολιτική προμήθειας εξοπλισμού και συμμετοχής προμηθευτών τηρουμένων των κατευθυντηρίων γραμμών,

(ii) να κοινοποιούν για έλεγχο στην Αρχή τις συμβάσεις προμήθειας εξοπλισμού και συμμετοχής προμηθευτών , τις οποίες συμφωνούν οι παροχείς με τους προμηθευτές τους, ώστε η Αρχή να έχει πρόσβαση μόνο στα μέρη των συμβάσεων που τεκμηριώνουν τα μέτρα, τους όρους και τις υποχρεώσεις ασφάλειας, που αναφέρονται στο άρθρο 13(1)(α)(i),

(iii) να κοινοποιούν για έλεγχο στην Αρχή και ως πρόσθετη τεκμηρίωση της στρατηγικής πολλαπλών προμηθευτών που αναφέρεται στο άρθρο 13(1)(γ), λεπτομερείς και ενημερωμένες πληροφορίες σχετικά με τα σχέδιά τους για προμήθεια εξοπλισμού δικτύου 5G και για τη συμμετοχή προμηθευτών, και

(iv) να παρέχουν εγγράφως τεκμηρίωση και να διαβιβάζουν πληροφορίες και έγγραφα στην Αρχή σε ηλεκτρονική μορφή για την αξιολόγηση της ασφάλειας εφοδιασμού καθώς και σχετικά με τα μέτρα ασφαλείας που έχουν ληφθεί και τεκμηριωθεί από αυτούς σύμφωνα με το παρόν άρθρο,

Ανάθεση και χρήση παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής.

(β) όσον αφορά την πολιτική ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής :

(i) να κοινοποιούν για έλεγχο στην Αρχή την πολιτική ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής τηρουμένων των κατευθυντηρίων γραμμών που είναι δυνατό να εκδίδονται από την Αρχή,

(ii) να κοινοποιούν για έλεγχο στην Αρχή τις συμβάσεις ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής τηρουμένων των κατευθυντήριων γραμμών που είναι δυνατόν να εκδίδονται από την Αρχή,

(iii) να παρέχουν εγγράφως τεκμηρίωση και να διαβιβάζουν πληροφορίες και έγγραφα στην Αρχή σε ηλεκτρονική μορφή σχετικά με τα μέτρα εφαρμογής της πολιτικής ανάθεσης και χρήσης παροχέων διαχειριζόμενων υπηρεσιών και υποστήριξης τρίτης γραμμής που έχουν ληφθεί και τεκμηριωθεί από αυτούς σύμφωνα με το παρόν άρθρο,

(iv) να διεξάγουν, στη βάση αυστηρών κριτηρίων, αξιολογήσεις κινδύνου σχετικά με τους παροχείς διαχειριζόμενων υπηρεσιών με τους οποίους προτίθενται να συνεργαστούν, να εντοπίζουν υψηλού κινδύνου παροχείς διαχειριζόμενων υπηρεσιών και να κοινοποιούν στην Αρχή τα αποτελέσματα της αξιολόγησης του προφίλ κινδύνου των παροχέων διαχειριζόμενων υπηρεσιών, τηρουμένων των κατευθυντήριων γραμμών που είναι δυνατόν να εκδίδονται από την Αρχή, και

(v) να υιοθετούν και επιβάλλουν ενισχυμένες διατάξεις ασφάλειας όσον αφορά την πρόσβαση που παρέχεται στους παροχείς διαχειριζόμενων υπηρεσιών για την εκτέλεση λειτουργιών,

Στρατηγική πολλαπλών προμηθευτών και ενίσχυση της ανθεκτικότητας.

(γ) Όσον αφορά τη στρατηγική πολλαπλών προμηθευτών:

(i) να κοινοποιούν για έλεγχο και έγκριση από την Αρχή τη στρατηγική πολλαπλών προμηθευτών, τηρουμένων των κατευθυντηρίων γραμμών, όπως ορίζεται στο Άρθρο 11(3),

(ii) να παρέχουν εγγράφως τεκμηρίωση και να διαβιβάζουν πληροφορίες και έγγραφα στην Αρχή σε ηλεκτρονική μορφή για την αξιολόγηση της στρατηγικής πολλαπλών προμηθευτών,

(iii) να διασφαλίζουν κατάλληλη ισορροπία προμηθευτών ή και κατάλληλο πλαίσιο ασφάλειας ώστε να εξασφαλίζεται η ανθεκτικότητα σε περίπτωση που προκύψει περιστατικό με έναν προμηθευτή, λαμβανομένων υπόψη των διαφοροποιήσεων όσον αφορά τα γεωγραφικά χαρακτηριστικά και τον πληθυσμό της Δημοκρατίας, και

(iv) να διαβουλεύονται επί του περιεχομένου της στρατηγικής με την Αρχή για τη λήψη των κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε η στρατηγική να είναι αποδεκτή από την Αρχή, και προκειμένου η Αρχή να είναι σε θέση να αξιολογήσει την κατάσταση σε εθνικό επίπεδο.

14. (1) Για την αιτιολόγηση της επάρκειας τους σε θέματα ασφάλειας, όπως καθορίζονται στη παρούσα Απόφαση, οι παροχείς ηλεκτρονικών επικοινωνιών οφείλουν:

(α) να λαμβάνουν υπόψη τυχόν περιορισμούς που καθορίζονται από την Αρχή σε σχέση με τη χρήση εξοπλισμού από προμηθευτές υψηλού κινδύνου,

(β) να μην εγκαθιστούν και να λειτουργούν εξοπλισμό που προμηθεύονται από προμηθευτή υψηλού κινδύνου, όπως ορίζεται από την αξιολόγηση που αναφέρεται στο άρθρο 15(1):

Ευαίσθητα στοιχεία υποδομής και

(i) σε ευαίσθητα σημεία της υποδομής όπως αυτά καθορίζονται στο Παράρτημα ΙΙΙ, και

(ii) σε γεωγραφικά σημεία που ορίζονται από την Αρχή, πλησίον συγκεκριμένων κρίσιμων

γεωγραφικοί περιορισμοί . Παράρτημα III.

υποδομών πληροφοριών και εγκαταστάσεων με αυξημένη σημασία ασφάλειας για τη Δημοκρατία, εκτός εάν, κατόπιν αξιολόγησης από την Αρχή, οι παροχείς ηλεκτρονικών επικοινωνιών μπορούν να τεκμηριώσουν, επαρκή μέτρα ψηφιακής ασφάλειας για την αντιμετώπιση των κινδύνων που εντοπίζονται στην αξιολόγηση προμηθευτών.

Νοείται ότι τηρουμένων των διατάξεων των άρθρων 2(2) και 2(3) του Νόμου η λειτουργία του εξοπλισμού από προμηθευτή υψηλού κινδύνου δεν θίγει τα μέτρα που είναι δυνατόν να λαμβάνει η Δημοκρατία για την εθνική ασφάλεια της Δημοκρατίας και τη διατήρηση του νόμου και της τάξης στη Δημοκρατία.

Νοείται περαιτέρω, ότι η Αρχή, ανεξάρτητα από τις ενέργειές της βάση του παρόντος άρθρου, οφείλει να συμμορφώνεται και να εφαρμόζει τις διατάξεις των άρθρων 15 (3) και 16 του Νόμου.

Παράρτημα III.

(γ) να παρέχουν για έλεγχο στην Αρχή κατάλογο λειτουργιών και κατασκευαστών στοιχείων δικτύου που σχετίζονται με την ασφάλεια που χρησιμοποιούνται για τη λειτουργία του δικτύου 5G, όπως καθορίζεται στο Παράρτημα ΙΙΙ, και, κατά περίπτωση, άλλων εξαρτημάτων που χρησιμοποιούνται από αυτά, κάθε έξι μήνες, αρχής γενομένης από την 30η Ιουνίου 2021 και οποτεδήποτε απαιτηθεί κατόπιν αιτιολογημένου αιτήματος από την Αρχή.

Αρμοδιότητες Αρχής.

15. (1) Τηρουμένων των διατάξεων του εδαφίου (3) του άρθρου 15 και του άρθρου 18 του Νόμου και του πλαισίου γενικής πολιτικής σε σχέση με την ψηφιακή ασφάλεια που εκδίδεται από τον Υφυπουργό δυνάμει του άρθρου 16 του Νόμου, η Αρχή διεξάγει αξιολόγηση κινδύνου προμηθευτών και καθορίζει τους προμηθευτές υψηλού κινδύνου. Η Αρχή οφείλει να ολοκληρώσει την αξιολόγηση κινδύνου προμηθευτών εντός δύο μηνών από τη λήψη όλων των σχετικών πληροφοριών από τους παροχείς και τις Αρμόδιες Αρχές της Δημοκρατίας, λαμβάνοντας υπόψη και τις αντίστοιχες αξιολογήσεις των παροχέων που διεξάγονται σύμφωνα με τις διατάξεις του άρθρου 12, τις αξιολογήσεις των Αρμοδίων Αρχών της Δημοκρατίας και τυχόν κατευθυντήριες γραμμές που εκδίδονται από αρμόδια όργανα της Ευρωπαϊκής Ένωσης.

(2) Τηρουμένων των διατάξεων του εδαφίου (3) του άρθρου 15 και του άρθρου 18 του Νόμου και του πλαισίου γενικής πολιτικής σε σχέση με την ψηφιακή ασφάλεια που εκδίδεται από τον Υφυπουργό δυνάμει του άρθρου 16 του Νόμου, η Αρχή οφείλει να αξιολογεί, να ελέγχει και να εγκρίνει τα έγγραφα που υποβάλλονται από τους παροχείς σύμφωνα με τις διατάξεις του Μέρους VI της παρούσας Απόφασης.

(3) Τηρουμένων των προνοιών του Μέρους VI της παρούσας Απόφασης, η στρατηγική πολλαπλών προμηθευτών που υποβάλλεται από τους παροχείς σύμφωνα με το άρθρο 13(1)(γ) αξιολογείται από την Αρχή εντός δύο μηνών από την υποβολή πλήρους συμπληρωμένης στρατηγικής και μπορεί να γίνει αποδεκτή από την Αρχή στη βάση επαρκούς αιτιολόγησης και κατάλληλου πλαισίου ασφάλειας για την αντιμετώπιση των κινδύνων που προκύπτουν από την αξιολόγηση που αναφέρεται στο άρθρο 12.

Περιορισμοί σε υψηλού κινδύνου προμηθευτές για βασικά πάγια στοιχεία δικτύου 5G, στην αποφυγή σημαντικής εξάρτησης από μοναδικό προμηθευτή και στην ανάθεση δραστηριοτήτων.

(4) Τηρουμένων των διατάξεων του εδαφίου (3) του άρθρου 15 και του άρθρου 18 του Νόμου, του πλαισίου γενικής πολιτικής σε σχέση με την ψηφιακή ασφάλεια που εκδίδεται από τον Υφυπουργό δυνάμει του άρθρου 16 του Νόμου και λαμβάνοντας υπόψη τα έγγραφα που υποβάλλονται από τους παροχείς σύμφωνα με τα άρθρα 12 και 13, τους περιορισμούς που καθορίζονται από την Αρχή σύμφωνα με το άρθρο 14 και την αξιολόγηση προφίλ κινδύνου των προμηθευτών που αναφέρεται στο εδάφιο ένα (1) του παρόντος άρθρου η Αρχή δύναται να εγκρίνει, τροποποιήσει ή απορρίψει τις εισηγήσεις των παροχέων ή και να επιβάλει με αιτιολογημένη απόφασή της σε οποιοδήποτε χρονικό σημείο επιπρόσθετους περιορισμούς, συμπεριλαμβανομένων των αποκλεισμών, ή ενισχυμένες διατάξεις ασφαλείας ώστε να μετριάζεται η ύπαρξη κινδύνου:

(α) στην προμήθεια εξοπλισμού και συμμετοχή προμηθευτών υψηλού κινδύνου σε βασικά πάγια στοιχεία δικτύου 5G,

(β) στην ανάθεση συγκεκριμένων λειτουργιών σε ευαίσθητα τμήματα των δικτύων 5G σε παροχείς διαχειριζόμενων υπηρεσιών, και

(γ) για την αποφυγή ή τον περιορισμό οποιασδήποτε σημαντικής εξάρτησης από έναν μοναδικό προμηθευτή.

(5) Η Αρχή κατά τη λήψη των αποφάσεων της σύμφωνα με τις διατάξεις του Μέρους VI της παρούσας Απόφασης, λαμβάνει υπόψη πληροφόρηση από αρμόδιες Αρχές της Δημοκρατίας σχετικά με:

(α) κρατικές ενισχύσεις, επιχορηγήσεις ή άλλα κίνητρα προς παροχείς και προμηθευτές,

173(I) του 2011 73(I) του 2016.

(β) διαδικασίες σύναψης δημοσίων συμβάσεων .

(γ) την προστασία του ανταγωνισμού,

(δ) τα συμφέροντα των καταναλωτών και ενδεχόμενες επιπτώσεις στις τιμές αγοράς ή πώλησης ή άλλων όρων συναλλαγής των παρεχόμενων υπηρεσιών ηλεκτρονικών επικοινωνιών.

ΜΕΡΟΣ VII

Κοινοποίηση Συμβάντων, Εξασφάλιση Πληροφοριών και Έλεγχοι

Διαδικασία και περιεχόμενο κοινοποίησης συμβάντων.

16. Τηρουμένων των διατάξεων των άρθρων 35, 37 και 40 του Νόμου, οι διατάξεις της Απόφασης του 2019 εφαρμόζονται για τη διαδικασία και το περιεχόμενο κοινοποίησης που οφείλουν να υποβάλλουν οι παροχείς ηλεκτρονικών επικοινωνιών για κάθε συμβάν το οποίο έχει σοβαρό αντίκτυπο στις υπηρεσίες που παρέχουν.

Διενέργεια ελέγχων και έρευνας από την Αρχή σε παροχείς ηλεκτρονικών επικοινωνιών.

17. (1) Τηρουμένων των διατάξεων του Νόμου, η Αρχή δύναται:

(α) με αιτιολογημένο αίτημα να απαιτεί από τους παροχείς ηλεκτρονικών επικοινωνιών την υποβολή εγγράφων και πληροφοριών όσον αφορά την κοινοποίηση συμβάντων και την εκτίμηση της ασφάλειας των δικτύων και συστημάτων πληροφοριών τους,

(β) να ελέγχει και ερευνά αυτεπάγγελτα τις δραστηριότητες, λειτουργίες και την ορθή εκτέλεση των υποχρεώσεων των παροχέων που απορρέουν από την παρούσα Απόφαση και τα σχετικά παραρτήματα.

(2) Για την άσκηση των εξουσιών, ελέγχων και ερευνών που προβλέπονται στο εδάφιο (1) ανωτέρω, η Αρχή ασκεί τις εξουσίες που της χορηγούνται και τηρεί τις διαδικασίες που προβλέπονται στα άρθρα 15, 16, 17, 18, 19, 20, 23, 36, 38 και 40 του Νόμου.

(3) Σε περίπτωση κατά την οποία ο προβλεπόμενος στο εδάφιο (1) έλεγχος ή έρευνα από την Αρχή απαιτεί σύμβαση παροχής υπηρεσιών από τεχνικούς συμβούλους ή άλλα πρόσωπα, η Αρχή λαμβάνει εύλογα μέτρα για την εξασφάλιση της ανεξαρτησίας τους καθώς και για την τήρηση εκ μέρους τους εμπιστευτικότητας και αμεροληψίας.

ΜΕΡΟΣ VIII

Συμμόρφωση – κυρώσεις

Διοικητικό πρόστιμο.

18. Τηρουμένων των άρθρου 43 και 54 του Νόμου και χωρίς περιορισμό των άλλων κυρώσεων που προβλέπει αυτός, η Αρχή δύναται να επιβάλει διοικητικό πρόστιμο που δεν υπερβαίνει τις διακόσιες χιλιάδες ευρώ (€ 200.000) σε περίπτωση που διαπιστώσει ότι παροχέας ή άλλο πρόσωπο διενεργεί πράξη ή τελεί σε παράλειψη κατά παράβαση των διατάξεων της παρούσας Απόφασης.

Ποινικά αδικήματα.

19. Τα άρθρα 22, 44 και 54 του Νόμου εφαρμόζονται για τις κυρώσεις και την ευθύνη νομικού προσώπου σε περίπτωση διάπραξης ποινικού αδικήματος για παράβαση των διατάξεων της παρούσας Απόφασης.

ΜΕΡΟΣ IX

Τελικές Διατάξεις

Έναρξη ισχύος.

20. Η παρούσα απόφαση τίθεται σε ισχύ από την ημερομηνία δημοσίευσής της στην Επίσημη Εφημερίδα της Δημοκρατίας.

Τροποποιήσεις.

21. Τηρουμένων των διατάξεων του Νόμου, η Αρχή δύναται με απόφασή της να τροποποιεί, αντικαθιστά ή καταργεί την παρούσα απόφαση ή τα Παραρτήματά της.

ΠΑΡΑΡΤΗΜΑ Ι
ΠΡΟΤΥΠΑ ΚΑΙ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΟΔΗΓΙΕΣ

A. 3GPP standards:

• 3GPP TS 33.116 V15.0.0 (2018-06), Security Assurance Specification (SCAS) for the MME network product class

• 3GPP TS 33.117 V16.3.0 (2019-12), Catalogue of general security assurance requirements

• 3GPP TS 33.216 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class

• 3GPP TS 33.250 V15.1.0 (2019-09), Security assurance specification for the PGW network product class

• 3GPP TS 33.401 V16.1.0 (2019-12), 3GPP System Architecture Evolution (SAE); Security architecture

• 3GPP TS 33.402 V15.1.0 (2018-06), 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses

• 3GPP TS 33.501 V16.1.0 (2019-12), Security architecture and procedures for 5G System

• 3GPP TS 33.511 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

• 3GPP TS 33.512 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); Access and Mobility Management Function (AMF)

• 3GPP TS 33.513 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); User Plane Function (UPF)

• 3GPP TS 33.514 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class

• 3GPP TS 33.515 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class

• 3GPP TS 33.516 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class

• 3GPP TS 33.517 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

• 3GPP TS 33.518 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class

• 3GPP TS 33.519 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

B. ETSI standards:

• ETSI GS NFV-SEC001 V1.1.1 (2014-10), Network Functions Virtualisation (NFV); NFV Security; Problem Statement

• ETSI GS NFV-SEC 002 V1.1.1 (2015-08), Network Functions Virtualisation (NFV); NFV Security; Cataloguing security features in management software

• ETSI GS NFV-SEC 003 V1.1.1 (2014-12), Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance

• ETSI GS NFV-SEC 004 V1.1.1 (2015-09), Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications

• ETSI GS NFV-SEC 006 V1.1.1 (2016-04), Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns

• ETSI GS NFV-SEC009 V1.1.1 (2015-12), Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration

• ETSI GS NFV-SEC 010 V1.1.1 (2016-04), Network Functions Virtualisation (NFV); NFV Security; Report on Retained Data problem statement and requirements

• ETSI GS NFV-SEC 012 V3.1.1 (2017-01), Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components

• ETSI GS NFV-SEC 013 V3.1.1 (2017-02), Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification

• ETSI GS NFV-SEC 014 V3.1.1 (2018-04), Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points

• ETSI GS NFV-SEC 021 V2.6.1 (2019-06), Network Functions Virtualisation (NFV) Release 2; Security; VNF Package Security Specification

• ETSI GS NFV-SEC 022 V2.7.1 (2020-01), Network Functions Virtualisation (NFV) Release 2; Security; Access Token Specification for API Access

• ETSI TS 103 487 Baseline security requirements regarding sensitive functions for NFV and related platforms

• ETSI TR 103 308 Security baseline regarding LI and RD for NFV and related platforms

• ETSI TS 103 307 Security Aspects for LI and RD Interfaces

Γ. GSMA documents:

• GSMA FF.02 Fraud Management Systems - Guidelines for Mobile Operators
• GSMA FF.15 Advice on Internal Fraud Risks
• GSMA FF.19 NRTRDE Commercial Implementation Handbook
• GSMA FF.21 Fraud Manual
• GSMA FS.01 Use of SIM Boxes to bypass interconnect communications
• GSMA FS.07 SS7 and SIGTRAN Network Security
• GSMA FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines
• GSMA FS.13-16 NESAS
• GSMA FS.19 Diameter Interconnect Security
• GSMA FS.20 GTP Security
• GSMA FS.21 Interconnect Signalling Security Recommendations
• GSMA FS.22 VoLTE Security Analysis and Recommendations
• GSMA FS.24 CAMEL Roaming Fraud Management Handbook
• GSMA FS.26 Guidelines for Independent Remote Interconnect Security Testing
• GSMA FS.30 Security Manual
• GSMA FS.31 Baseline Security Controls
• GSMA FS.33 NFV Threats Analysis
• GSMA FS.34 Key Management for 4G and 5G inter-PLMN security
• GSMA FS.35 Security Algorithm Implementation Roadmap
• GSMA FS.36 5G Interconnect Security
• GSMA FS.37 GTP-U Security
• GSMA FS.38 SIP Network Security
• GSMA FS.40 5G Security
• GSMA IR.77 InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers
• GSMA IR.88 LTE and EPC roaming guidelines (5G NSA uses LTE roaming)
• GSMA SGP.21 - RSP Architecture
• GSMA SGP.22 - Technical Specification
• GSMA TS.26 - NFC Handset Requirements
• GMSA TS.27 - NFC Handset Test Book
• GSMA SGP.25 - Embedded UICC for Consumer Devices Protection Profile
• GSMA SGP.05 - Embedded UICC Protection Profile (for m2m-devices)
• BSI-CC-PP-0104-2019 - CC-PP Cryptographic Service Provider
• GSMA FS.27 Security Guidelines for UICC profiles
• GSMA FS.28 Security Guidelines for UICC credential protection

Δ. ENISA documents:

• ENISA Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services, Version 1.0, December 2016.
• Technical Guideline on Security Measures in article 13a, Version 2.0 October 2014.
• ENISA Security aspects of virtualization, February 2017

E. Certification Schemes

• ISO/IEC 27001
• ISO/IEC 22301
• NESAS (Network Equipment Security Assurance Scheme) under governance by EU-COM (CSA)
• SOGIS Common Criteria

ΣΤ: NIST Guidelines

• SP 800-125 - Guide to Security for Full Virtualization Technologies
• SP 800-125A Rev. 1 - Security Recommendations for Server-based Hypervisor Platforms
• SP 800-125B - Secure Virtual Network Configuration for Virtual Machine (VM) Protection

ΠΑΡΑΡΤΗΜΑ ΙΙ
ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΚΙΝΔΥΝΟΥ ΠΡΟΜΗΘΕΥΤΩΝ

Κριτήρια Αξιολόγησης Κινδύνων Προμηθευτών

Οι παροχείς ηλεκτρονικών επικοινωνιών διενεργούν εκτίμηση επικινδυνότητας για τους προμηθευτές, επιπλέον της ενσωμάτωσης των απαιτήσεων ασφαλείας στη διαδικασία σύναψης συμβάσεων που σχετίζονται με τα κατασκευαστικά στοιχεία του δικτύου 5G. Οι ακόλουθες κατευθυντήριες γραμμές παρέχουν μια επισκόπηση των τομέων ασφαλείας που πρέπει να λαμβάνονται υπόψη κατά την εκτίμηση επικινδυνότητας. Περαιτέρω εργαλεία στη μορφή ερωτηματολογίων θα παρέχονται από την ΑΨΑ προκειμένου να διευκολυνθεί η διενέργεια της αξιολόγησης. Το υλικό θα παρέχεται στην Αγγλική γλώσσα λόγω των τεχνικών όρων.

Η διαδικασία σύναψης συμβάσεων εξαρτημάτων ή υπηρεσιών που σχετίζονται με το δίκτυο 5G πρέπει να συμμορφώνεται με τις συστάσεις που ορίζονται στο έγγραφο ENISA «Indispensable baseline security requirements for the procurement of secure ICT products and services» το οποίο είναι σύμφωνο με την απαίτηση της ΕΕ για συμμόρφωση με τα ειδικά πρότυπα ασφαλείας στη διαδικασία σύναψης συμβάσεων για συνιστώσες και υπηρεσίες ΤΠΕ.

Α. Κύκλος ζωής ανάπτυξης προϊόντων

Κατά την εκτίμηση της επικινδυνότητας λαμβάνεται υπόψη ο κύκλος ζωής των εξαρτημάτων/υπηρεσιών που παρέχει ο προμηθευτής στην ανάπτυξη του προϊόντος. Λεπτομερειακά, αξιολογούνται τα ακόλουθα:

- Η ποιότητα και η διαφάνεια των τεχνικών πρακτικών του προμηθευτή και των ελέγχων ασφάλειας στον κυβερνοχώρο
- Γίνεται ποιοτικός έλεγχος για την εύρεση τυχαίας ή εσκεμμένης ευπάθειας ασφάλειας στα εξαρτήματα που παρέχει ο προμηθευτής αλλά και στο λογισμικό. Αυτό περιλαμβάνει τουλάχιστον:
  - Πύλες ασφάλειας/ποιότητας τόσο για την ανάπτυξη λογισμικού και υλικού
  - Μοντελοποίηση απειλών ενσωματωμένη στη φάση σχεδιασμού
  - Ασφαλής Ανάπτυξη Λογισμικού Εκπαίδευση Κύκλου Ζωής για όλους τους εργαζόμενους που εμπλέκονται
  - Στατική & Δυναμική Ανάλυση Ασφαλείας Κώδικα κατά τη διάρκεια της ανάπτυξης
  - Αυτοματοποιημένες δοκιμές για τον κωδικό παραγωγής κατά την ανάπτυξη
  - Δοκιμές ασφαλείας, συμπεριλαμβανομένων των δοκιμών διείσδυσης για προϊόντα/λογισμικό πριν από την ανάπτυξη
- Μέτρα που λήφθηκαν για να εξασφαλιστεί η ασφάλεια με σχεδιασμό και προεπιλογή με σαφείς απαιτήσεις ασφαλείας.
- Διαχείριση της εξάρτησης για την εξασφάλιση της διαλειτουργικότητας, όπου περιλαμβάνονται βιβλιοθήκες ή κατασκευαστικά στοιχεία τρίτων.
- Διατήρηση ενός λογαριασμού υλικών για βιβλιοθήκες τρίτων και συμπεριλάβετε τα εν λόγω περιουσιακά στοιχεία στο πρόγραμμα διαχείρισης ευπάθειας του προμηθευτή.

Β. Διακυβέρνηση/Διοίκηση Κινδύνου

Οι προμηθευτές πρέπει να είναι σε θέση να αποδεικνύουν την ευθυγράμμιση των πρακτικών ασφαλείας τους με τους στόχους ασφαλείας του παροχέα. Κατά συνέπεια, η εκτίμηση κινδύνου πρέπει να λαμβάνει υπόψη:

- Συμμόρφωση με τα διεθνή πρότυπα & Κανονισμούς όπως οι ISO27001, ISO22301, ISO9001, PCI-DSS & GPDR κατά περίπτωση.
- Πρόγραμμα ασφάλειας πληροφοριών του προμηθευτή, συμπεριλαμβανομένης της διαχείρισης κινδύνων σε ισχύ.
- Ο προμηθευτής θα πρέπει να διαθέτει πολιτική ασφάλειας των πληροφοριών που να εξασφαλίζει την ασφάλεια και την ανθεκτικότητα των προϊόντων και των υπηρεσιών του και να ευθυγραμμίζεται με τους υψηλού επιπέδου στόχους ασφαλείας του παροχέα.
- Ο προμηθευτής θα πρέπει να είναι σε θέση να συμμορφώνεται με τις νομικές απαιτήσεις του παροχέα που επιβάλλονται από το Νόμο.
- Ο προμηθευτής θα πρέπει να είναι σε θέση να συμμορφώνεται με Νόμο καθώς και με της δυνάμει αυτού εκδιδόμενες Αποφάσεις και Κανονισμούς.

Γ. Επιχειρηματική Συνέχεια & Αντοχή

Ο προμηθευτής διαθέτει BCP/DRP για να εξασφαλίσει τη συνέχεια των υπηρεσιών τους εκτός από τους KPIs για την παρακολούθηση των επιδόσεων. Η εκτίμηση επικινδυνότητας θα πρέπει να περιλαμβάνει τουλάχιστον:

- Δυνατότητα παροχής ανταλλακτικών μερών για το δίκτυο και διατήρηση SLAs.
- Σχέδια επιχειρησιακής συνέχειας που εξασφαλίζουν συνεχή λειτουργία και παροχή υπηρεσιών/υποστήριξης.
- Η ανθεκτικότητα του προμηθευτή τόσο από τεχνική άποψη όσο και ως προς τη συνέχεια της προσφοράς υπηρεσιών στους παροχείς ηλεκτρονικών επικοινωνιών της Κύπρου.

Δ. Διαλειτουργικότητα

Η διασφάλιση της ανθεκτικότητας των δικτύων 5G αποτελεί μείζονα προτεραιότητα για την Κύπρο. Ως εκ τούτου, το προφίλ κινδύνου του προμηθευτή εξαρτάται επίσης από τους ακόλουθους παράγοντες διαλειτουργικότητας:

- Τα προϊόντα ή οι υπηρεσίες που αποκτώνται από τον προμηθευτή πρέπει να ακολουθούν σημαντικά πρότυπα όπως το 3GPP .
- Τα προϊόντα ή οι υπηρεσίες που αποκτώνται από τον προμηθευτή πρέπει να πληρούν τις απαιτήσεις διαλειτουργικότητας του εκάστοτε παροχέα ηλεκτρονικών επικοινωνιών, επιτρέποντας την εφαρμογή στρατηγικής πολλών προμηθευτών.
- Τα προϊόντα ή οι υπηρεσίες που αποκτώνται από τον προμηθευτή εξασφαλίζουν τη συνέχιση των εργασιών σε περιβάλλοντα πολλαπλών προμηθευτών σε περιπτώσεις όπου τα ευάλωτα/προβληματικά συστατικά στοιχεία πρέπει να αφαιρεθούν/αντικατασταθούν από το δίκτυο 5G.

Ε. Ασφάλεια δεδομένων/ιδιωτικό απόρρητο

Ο προμηθευτής θα πρέπει να συμμορφώνεται με τυχόν νομικές ή κανονιστικές απαιτήσεις που αφορούν νόμους περί απορρήτου δεδομένων, όπως ο GDPR, κατά περίπτωση. Ως εκ τούτου, η εκτίμηση επικινδυνότητας πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα:

- Θέση δεδομένων και κατά πόσον αποθηκεύονται δεδομένα εκτός της ΕΕ.
- Ο προμηθευτής έχει επαρκή πολιτική απορρήτου δεδομένων.
- Κατά πόσο ο προμηθευτής θα έχει πρόσβαση σε εμπιστευτικά ή ιδιωτικά δεδομένα που σχετίζονται με δεδομένα τελικού χρήστη εντός του δικτύου κινητής τηλεφωνίας, ή εταιρικά δεδομένα, όπως διαμορφώσεις δικτύου και προνομιούχα διαπιστευτήρια πρόσβασης.
- Κατά πόσο ο προμηθευτής θα έχει πρόσβαση σε μεγάλο όγκο εγγραφών.
- Πολιτική ταξινόμησης δεδομένων σε συνδυασμό με το χειρισμό και την επισήμανση όλων των μέσων.

ΣΤ. Ασφάλεια Ανθρώπινου Δυναμικού

Στο πλαίσιο της διαδικασίας σύναψης συμβάσεων, οι παροχείς ηλεκτρονικών επικοινωνιών αξιολογούν τις διαδικασίες ασφάλειας των πληροφοριών που εφαρμόζονται όσον αφορά το ανθρώπινο δυναμικό των προμηθευτών. Θα πρέπει να διασφαλίζονται τουλάχιστον τα ακόλουθα:

- Ο προμηθευτής διενεργεί έλεγχο σε όλους τους εργαζόμενους πριν από την απασχόληση, εκτός από τις περιοδικές οθόνες για να εντοπίσει οποιονδήποτε θα μπορούσε να παραποιήσει τον εξοπλισμό (ως μέρος του χακτιβισμού, του οργανωμένου εγκλήματος, της κυβερνητικής πίεσης ή κατασκοπείας).
- Ο προμηθευτής διεξάγει επαρκή εκπαίδευση στους εργαζομένους για την ασφάλεια στον κυβερνοχώρο.
- Ο προμηθευτής οφείλει να ενσωματώνει σχετική ρήτρα μη γνωστοποίησης δεδομένων και πληροφοριών σε όλες τις συμβάσεις των εργαζομένων.
- Ο προμηθευτής περιλαμβάνει μια διεξοδική διαδικασία εξόδου για τον τερματισμό της απασχόλησης των εργαζομένων.

Ζ. Έλεγχοι Εσωτερικής Ασφάλειας

Οι προμηθευτές είναι υποχρεωμένοι να εφαρμόζουν εσωτερικές διαδικασίες ασφάλειας για να εξασφαλίζουν την ασφάλεια των προϊόντων, των υπηρεσιών και των δεδομένων των πελατών τους. Κατά συνέπεια, στην εκτίμηση επικινδυνότητας περιλαμβάνονται οι ακόλουθοι έλεγχοι:

- Ο προμηθευτής εφαρμόζει πρόγραμμα διαχείρισης ευπαθειών, το οποίο περιλαμβάνει:
  - Διαχείριση patching για όλα τα εσωτερικά συστήματα και κατασκευαστικά στοιχεία.
  - Εκτιμήσεις ευπάθειας σε όλα τα συστήματα.
- Ο προμηθευτής διαθέτει μηχανισμούς παρακολούθησης και ανίχνευσης που εξασφαλίζουν τον εντοπισμό απειλών ή συμβάντων κατά την ασφάλεια.
- Ο προμηθευτής έχει πολιτική διαχείρισης συμβάντων, με τις σχετικές διαδικασίες που πρέπει να ακολουθούνται αλλά και εγχειριδίων, η οποία επιτρέπει την άμεση αντιμετώπιση σε περιστατικά ασφαλείας.
- Ο προμηθευτής εκτελεί διαχωρισμό/διαμέριση δικτύου.
- Οι προμηθευτές εφαρμόζουν μηχανισμούς και διαδικασίες ελέγχου πρόσβασης, συμπεριλαμβανομένης της διαχείρισης πρόσβασης σε διαχειριστές συστημάτων για να εξασφαλίσουν ότι τηρείται η αρχή ελαχίστων προνομίων και η αρχή ανάγκης γνώσης.
- Ο προμηθευτής διαθέτει φυσικά μέτρα ασφαλείας και πληροφοριών που προστατεύουν την μη εξουσιοδοτημένη πρόσβαση στην πνευματική ιδιοκτησία και τις διαδικασίες του.
- Ο προμηθευτής διαθέτει εφεδρικές πολιτικές και τα δεδομένα αποκαθιστούν διαδικασίες που καθορίζονται τεκμηριωμένες και συνδέονται σαφώς με ρόλους και ευθύνες. Τα αντίγραφα ασφαλείας κρυπτογραφούνται και αποθηκεύονται με ασφάλεια.
- Ο προμηθευτής διενεργεί τακτικές δοκιμές ασφαλείας, συμπεριλαμβανομένων δοκιμών διείσδυσης στην υποδομή του δικτύου του και εφαρμογές για υφιστάμενα και νέα συστήματα.

Η. Στρατηγικοί Παράγοντες

- Η πιθανότητα του προμηθευτή να έχει πρόσβαση σε εμπιστευτικά ή ιδιωτικά δεδομένα. Ποσοστό και είδη υπηρεσιών που ανατίθενται/παρέχονται στους προμηθευτές από τρίτους.
- Κατά πόσο οι προμηθευτές ακολουθούν τις βέλτιστες πρακτικές ασφαλείας στη διαχείριση τρίτων (δικών τους προμηθευτών). Διασφάλιση ότι οι υπηρεσίες που παρέχονται στους προμηθευτές δεν περιλαμβάνουν τρίτους που έχουν πρόσβαση σε δεδομένα ή τμήματα του δικτύου/υποδομής των παροχέων.
- Οι προμηθευτές εκτελούν δοκιμές/επαλήθευση/έλεγχο σε κώδικα που αναπτύχθηκε από τρίτους.
- Η κρισιμότητα του στοιχείου στο δίκτυο 5G που πρέπει να παρέχει ο προμηθευτής.

ΠΑΡΑΡΤΗΜΑ ΙΙΙ
ΚΑΤΑΛΟΓΟΣ ΒΑΣΙΚΩΝ ΠΑΓΙΩΝ ΣΤΟΙΧΕΙΩΝ ΔΙΚΤΥΟΥ 5G

• Access and Mobility management Function (AMF)
• Authentication Server Function (AUSF)
• Network Exposure Function (NEF)
• Network Repository Function (NRF)
• Network Slice Selection Function (NSSF)
• Policy Control Function (PCF)
• Security Edge Protection Proxy (SEPP)
• Session Management Function (SMF)
• Unified Data Management (UDM)
• User Plane Function (UPF)
• New Radio Base Station (gNodeB) [Σε ευαίσθητα σημεία όπως στους σταθμούς βάσης που λειτουργούν με multi - access edge computing ή και σε γεωγραφικά ευαίσθητες περιοχές όπως ορίζονται σύμφωνα με το άρθρο 14 (1) (β) (ii)].