Ε.Ε. Παρ. III(I) **Κ.Δ.Π. 41/2022**
Αρ. 5659, 28.1.2022

Αριθμός 41

Ο ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΝΟΜΟΣ ΤΟΥ 2020

Απόφαση
δυνάμει των άρθρων 17(ιη), 17(ιθ), 17(λα), 20(1)(α), 20(1)(β), 20(1)(γ), 20(1)(ε), 40, 43 και 46

Προοίμιο. Η Αρχή Ψηφιακής Ασφάλειας (στο εξής "η Αρχή"), ασκώντας τις εξουσίες που της παρέχονται από

89(I) του 2020. τα άρθρα 17(ιη), 17(ιθ), 17(λα), 20(1)(α), 20(1)(β), 20(1)(γ), 20(1)(ε), 40, 43 και 46 του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020, εκδίδει την παρούσα Απόφαση με την οποία καθορίζονται οι ελάχιστες επιπρόσθετες υποχρεώσεις σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών τις οποίες πρέπει να τηρούν οι παροχείς οι οποίοι λειτουργούν δίκτυα ή/και υπηρεσίες ηλεκτρονικών επικοινωνιών.

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 τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών,

Επίσημη Εφημερίδα. Παράρτημα Πρώτο (I): 12.08.2020. (γ) τις πρόνοιες του περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020 (Ν.89(I)/2020),

Επίσημη Εφημερίδα, Παράρτημα Τρίτο (I): 21.08.2020. (δ) την περί Ασφάλειας Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφαση του 2020 (Κ.Δ.Π. 389/2020),

(ε) την Εθνική Στρατηγική για την ασφάλεια δικτύων και συστημάτων πληροφοριών και την Κυβερνοασφάλεια,

(στ) τις πρόνοιες των κατευθυντήριων γραμμών του ENISA του 2021, για τα μέτρα ασφάλειας σχετικά με τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών.

ΜΕΡΟΣ Ι
Εισαγωγικές Διατάξεις

Συνοπτικός τίτλος. 1. Η παρούσα Απόφαση θα αναφέρεται ως η περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών) Απόφαση του 2022.

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

"Ακεραιότητα δικτύου" σημαίνει την ικανότητα που παρέχεται σ' ένα δίκτυο ηλεκτρονικών επικοινωνιών, στη βάση του σχεδιασμού του, να διατηρεί τη λειτουργικότητα για την οποία έχει σχεδιαστεί και να παρέχει και διατηρεί υψηλό επίπεδο υπηρεσίας κατόπιν βλαβών και αλλαγών στα κανονικά επίπεδα λειτουργίας·

Κ.Δ.Π.389/2020. "Απόφαση των Μέτρων Ασφάλειας 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·

«Διασυνδεόμενα δίκτυα» σημαίνει τα δίκτυα τα οποία παρέχουν πρόσβαση το ένα στο άλλο για την ανταλλαγή κίνησης μέσω, ενδεικτικά, διασύνδεσης, μισθωμένων γραμμών, αδεσμοποίητης πρόσβασης στον τοπικό βρόχο και υπηρεσιών χονδρικής ευρυζωνικής πρόσβασης·

Κ.Δ.Π.63/2018. «Διάταγμα Αριθμοδότησης του 2018» σημαίνει το περί Αριθμοδότησης (Ηλεκτρονικών Επικοινωνιών) Διάταγμα του 2018 και περιλαμβάνει κάθε Διάταγμα που το τροποποιεί ή το αντικαθιστά·

«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·

Ν. 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 ηλεκτρονικών επικοινωνιών" ή “παροχείς” σημαίνει τους παροχείς δικτύων ηλεκτρονικών επικοινωνιών ή/και τους παροχείς υπηρεσιών ηλεκτρονικών επικοινωνιών·

"περιστατικό" σημαίνει το συμβάν με βάση τον περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμο·

"σχέδιο έκτακτης ανάγκης" σημαίνει το οποιοδήποτε σχέδιο για την αντιμετώπιση έκτακτων συνθηκών συμπεριλαμβανομένου του σχεδίου επιχειρησιακής συνέχειας και του σχεδίου αποκατάστασης από καταστροφή·

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

Πεδίο Εφαρμογής. Κ.Δ.Π.389/2020. 3. (1) Η παρούσα Απόφαση καθορίζει ελάχιστες επιπρόσθετες υποχρεώσεις, πέραν από τις υποχρεώσεις που καθορίζονται στην Απόφαση των Μέτρων Ασφάλειας του 2020 σχετικά με την ασφάλεια δικτύων και πληροφοριών, τις οποίες πρέπει να τηρούν οι παροχείς ηλεκτρονικών επικοινωνιών.

(2) Η Αρχή έχει τη δυνατότητα έκδοσης κατευθυντήριων γραμμών για τον καθορισμό του επιπέδου υλοποίησης των μέτρων ασφάλειας από τους παροχείς ηλεκτρονικών επικοινωνιών:

Νοείται ότι, η Αρχή δύναται να διαβουλεύεται με τους παροχείς ηλεκτρονικών επικοινωνιών, που δεν έχουν οριστεί ως φορείς εκμετάλλευσης βασικών υπηρεσιών ή/και φορείς κρίσιμων υποδομών πληροφοριών, για το πλάνο εφαρμογής των μέτρων ασφάλειας που επιβάλλεται να υιοθετήσουν ως αυτό προνοείται στη Δευτερογενή Νομοθεσία της Αρχής.

Σκοπός. 4. Ο σκοπός της παρούσας Απόφασης είναι η εισαγωγή ελάχιστων υποχρεώσεων, ικανών να μετριάσουν τους κύριους κινδύνους που αφορούν την ασφάλεια των παροχέων ηλεκτρονικών επικοινωνιών, έτσι ώστε να διασφαλιστεί η ακεραιότητα και η επιχειρησιακή συνέχεια των δικτύων και των υπηρεσιών που παρέχονται προς τους καταναλωτές/συνδρομητές σε περίπτωση καταστρεπτικής βλάβης ή σε περίπτωση ανωτέρας βίας:

Νοείται ότι, είναι μέγιστης σημασίας, στην περίπτωση καταστροφικών συμβάντων, η εξασφάλιση της αδιάκοπης πρόσβασης σε υπηρεσίες έκτακτης ανάγκης, όπως είναι ενδεικτικά οι κλήσεις στον αριθμό 112 ή σε εθνικούς αριθμούς έκτακτης ανάγκης ή/και σε εναρμονισμένους αριθμούς για εναρμονισμένες υπηρεσίες κοινωνικού ενδιαφέροντος όπως είναι οι αριθμοί της σειράς 116xxx, ως αυτοί αναφέρονται στο Διάταγμα Αριθμοδότησης του 2018, ως εκάστοτε τροποποιείται ή/και αντικαθίσταται.

Κ.Δ.Π.63/2018.

ΜΕΡΟΣ ΙΙ

Επιπρόσθετες υποχρεώσεις παροχέων ηλεκτρονικών επικοινωνιών

Διακυβέρνηση. Κ.Δ.Π.389/2020. 5. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διακυβέρνηση», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να ακολουθεί τα πρότυπα ή τις προδιαγραφές που θεσπίζονται σε κοινοτικό επίπεδο, χαρακτηρίζονται ως υποχρεωτικά και έχουν δημοσιευθεί σε κατάλογο προτύπων ή και προδιαγραφών στην Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, για την παροχή

υπηρεσιών, τεχνικών διεπαφών ή και λειτουργιών δικτύων. Σε περίπτωση τεχνικών δυσκολιών συμμόρφωσης με την παραπάνω υποχρέωση, ο παροχέας, σε εύλογο χρόνο κατόπιν συμφωνίας με την Αρχή, προβαίνει στα αναγκαία μέτρα για τη συμμόρφωση με τις παραπάνω υποχρεώσεις του:

Νοείται ότι, στην απουσία τέτοιων προτύπων ή και προδιαγραφών, ο παροχέας καλείται να εφαρμόζει τις τελευταίες εκδόσεις των διεθνών προτύπων ή συστάσεων που εγκρίνονται από τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU), τον Διεθνή Οργανισμό Τυποποίησης (ISO) ή τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC).

(2) (α) Να ενημερώνει όλο το προσωπικό σχετικά με την πολιτική ασφάλειας, η οποία θα είναι εγκεκριμένη από τη διοίκηση και στην οποία θα συμπεριλαμβάνονται εφαρμοστέοι Νόμοι και Κανονισμοί στους οποίους θα έχει πρόσβαση το προσωπικό. Ο παροχέας οφείλει να ενημερώνει το προσωπικό σχετικά με τις επιπτώσεις που ενδέχεται να επιφέρει στην εργασία του, η μη τήρηση της πολιτικής ασφάλειας,

(β) Να επανεξετάζει και, εφόσον απαιτείται, να επικαιροποιεί την πολιτική ασφάλειας μετά από περιστατικά ασφάλειας.

(3) Να βεβαιώνεται ότι, το προσωπικό που κατέχει ρόλους ασφάλειας είναι προσβάσιμο σε περίπτωση περιστατικών ασφάλειας.

(4) Να ενημερώνει το προσωπικό για τα αρμόδια άτομα που κατέχουν ρόλο ασφάλειας, καθώς και σε ποιες περιπτώσεις πρέπει να επικοινωνεί το προσωπικό μαζί τους.

(5) Να θεσπίζει τις επιχειρησιακές διαδικασίες και να αναθέτει αρμοδιότητες σε προσωπικό σχετικά με τη λειτουργία κρίσιμων συστημάτων.

(6) Να εφαρμόζει πολιτική, για τη λειτουργία των συστημάτων, για να βεβαιωθεί ότι όλα τα κρίσιμα συστήματα λειτουργούν και διαχειρίζονται σύμφωνα με προκαθορισμένες διαδικασίες.

(7) Να εφαρμόζει πολιτική και διαδικασίες για την παρακολούθηση και τον έλεγχο της συμμόρφωσης με σχετικές νομικές και κανονιστικές υποχρεώσεις.

Διαχείριση κινδύνων. Κ.Δ.Π. 389/2020.

6. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διαχείριση κινδύνων», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να βεβαιώνεται ότι το βασικό προσωπικό (key personnel) είναι ενήμερο για τους κύριους κινδύνους και τα μέτρα αντιμετώπισης τους.

(2) Να επανεξετάζει και, εφόσον απαιτείται, να επικαιροποιεί την αξιολόγηση κινδύνων κατόπιν αλλαγών (change management) ή περιστατικών ασφάλειας.

Ευαισθητοποίηση και εκπαίδευση. Κ.Δ.Π. 389/2020.

7. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Ευαισθητοποίηση και εκπαίδευση», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με την ακόλουθη υποχρέωση:

(1) Να εφαρμόζει πρόγραμμα εκπαίδευσης διασφαλίζοντας ότι όλο το βασικό προσωπικό έχει επαρκείς και επικαιροποιημένες γνώσεις ασφάλειας.

Διαχείριση τρίτων μερών και προμηθευτών. Κ.Δ.Π. 389/2020.

8. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διαχείριση τρίτων μερών και προμηθευτών», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) (α) Να ορίζει πολιτική ασφάλειας συμβάσεων με τρίτα μέρη, με σκοπό να διασφαλίζει ότι τυχόν εξαρτήσεις σε αυτά δεν θα επηρεάζουν αρνητικά την ασφάλεια των δικτύων ή/και υπηρεσιών του.

Κατ' ελάχιστον, η πολιτική πρέπει να περιλαμβάνει πρόνοιες για εμπιστευτικότητα και για ασφαλή ανταλλαγή πληροφοριών,

(β) Να εξασφαλίζει ότι όλες οι προμήθειες υπηρεσιών ή προϊόντων από τρίτα μέρη ακολουθούν την πολιτική ασφάλειας συμβάσεων με τρίτα μέρη,

(γ) Να επανεξετάζει και, εφόσον απαιτείται, να επικαιροποιεί την πολιτική ασφάλειας συμβάσεων με τρίτα μέρη, μετά από περιστατικά ασφάλειας ή αλλαγές,

(δ) Να απαιτεί, κατά τη διάρκεια της προμήθειας, τη χρήση συγκεκριμένων προτύπων ασφάλειας στις διαδικασίες του προμηθευτή,

(ε) Να περιορίζει τους εναπομείναντες κινδύνους οι οποίοι δεν αντιμετωπίζονται από τα τρίτα μέρη.

Διαχείριση αλλαγών. Κ.Δ.Π. 389/2020.

9. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διαχείριση αλλαγών», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να εφαρμόζει διαδικασίες διαχείρισης αλλαγών και να καταγράφει, για την κάθε αλλαγή, τα βήματα της διαδικασίας που έχει ακολουθήσει.

(2) Οι παροχείς οφείλουν να διατηρούν, ανά πάσα στιγμή, διαθέσιμα αντίγραφα ασφαλείας της πλέον πρόσφατης διάρθρωσης (configuration) του εξοπλισμού του δικτύου τους, τα οποία είναι απαραίτητα για την αποκατάσταση του δικτύου τους και των παρεχόμενων υπηρεσιών. Τα αντίγραφα ασφαλείας θα πρέπει να φυλάσσονται σε προστατευμένο χώρο.

(3) Οι παροχείς οφείλουν να διαθέτουν διαδικασίες διαχείρισης αλλαγών τις οποίες πρέπει να εφαρμόζουν στις περιπτώσεις που επέρχονται αλλαγές (ενδεικτικά οργανωτικές αλλαγές, αλλαγές λογισμικού ή υλικού), οι οποίες θα μπορούσαν με οποιοδήποτε τρόπο να επηρεάσουν το δίκτυο ή τη διαθεσιμότητα των παρεχόμενων υπηρεσιών:

Νοείται ότι, οποιεσδήποτε αλλαγές θα πρέπει να γίνονται με τέτοιο τρόπο ώστε να προκαλούν τις ελάχιστες δυνατές επιπτώσεις στη λειτουργία του δικτύου, στις παρεχόμενες υπηρεσίες και σε άλλους συνεργαζόμενους παροχείς. Αν οι αλλαγές αυτές αναπόφευκτα επηρεάζουν τα δίκτυα ή τις υπηρεσίες άλλου παροχέα, τα εμπλεκόμενα μέρη οφείλουν να συνεργάζονται για τη διαχείριση των αλλαγών ώστε να ελαχιστοποιηθούν οποιεσδήποτε επιπτώσεις.

Διαχείριση στοιχείων ενεργητικού. Κ.Δ.Π. 389/2020.

10. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διαχείριση στοιχείων ενεργητικού», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να ακολουθεί βέλτιστες πρακτικές για τη χρήση αλγόριθμων κρυπτογράφησης και τα κλειδιά κρυπτογράφησης που θα χρησιμοποιούνται να έχουν το συνιστώμενο μέγεθος ανάλογα με τον αλγόριθμο που χρησιμοποιείται.

(2) (α) Να βεβαιώνεται ότι το κρυπτογραφικό υλικό, όπως τα κλειδιά και οι απόρρητες πληροφορίες αυθεντικοποίησης, δεν αποκαλύπτονται ή παραποιούνται,

(β) Να ελέγχει αυστηρά και να παρακολουθεί την πρόσβαση σε ιδιωτικά κλειδιά (private keys).

(3) Να εφαρμόζει πολιτική για τη διαχείριση κρυπτογραφικών κλειδιών.

(4) (α) Να εφαρμόζει πολιτική για την παρακολούθηση κρίσιμων συστημάτων και την τήρηση αρχείων καταγραφής (logs),

(β) Να χρησιμοποιεί εργαλεία για τη συλλογή και αποθήκευση των αρχείων καταγραφής σε ανεξάρτητο εξυπηρετητή.

(5) (α) Να εκτελεί εργασίες προληπτικής συντήρησης του εξοπλισμού του, καθώς και των κτιρίων στα οποία αυτός στεγάζεται, στη βάση προδιαγεγραμμένου χρονοδιαγράμματος που ορίζεται είτε από τον κατασκευαστή του εξοπλισμού, είτε από εσωτερικές διαδικασίες του παροχέα, προκειμένου να ελαχιστοποιηθεί η πιθανότητα δυσλειτουργίας του δικτύου και των παρεχόμενων υπηρεσιών:

Νοείται ότι, στο μέτρο του δυνατού οι εργασίες συντήρησης του δικτύου θα πρέπει να διεκπεραιώνονται χωρίς τη διακοπή του δικτύου ή των παρεχόμενων υπηρεσιών,

(β) Στις περιπτώσεις προγραμματισμένων εργασιών συντήρησης, ο παροχέας υποχρεούται εκ των προτέρων, εντός εύλογου χρονικού διαστήματος, να ενημερώνει γραπτώς τους συνεργάτες – παροχείς του (στην περίπτωση διασυνδεδεμένων δικτύων), καθώς επίσης και τους συνδρομητές/χρήστες των υπηρεσιών του δικτύου οι οποίοι ενδέχεται να επηρεαστούν από την προγραμματιζόμενη διακοπή. Ο παροχέας οφείλει να ενημερώνει τους συνδρομητές/χρήστες των υπηρεσιών του δικτύου οι οποίοι ενδέχεται να επηρεαστούν από την προγραμματιζόμενη διακοπή όπως ορίζεται στο άρθρο 21(1) της παρούσας Απόφασης.

Διαχείριση ταυτότητας και πρόσβασης. Κ.Δ.Π. 389/2020.

11. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διαχείριση ταυτότητας και πρόσβασης», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να ενισχύει τους ελέγχους για απομακρυσμένη πρόσβαση, σε κρίσιμα στοιχεία ενεργητικού των δικτύων και συστημάτων πληροφοριών, από τρίτους:

Νοείται ότι, η απομακρυσμένη πρόσβαση σε κρίσιμα στοιχεία ενεργητικού από τρίτους, πρέπει να παρέχεται κατόπιν εύλογης αιτίας και να υπόκειται σε αυστηρούς ελέγχους πρόσβασης, συμπεριλαμβανομένου του ελέγχου ταυτότητας και εξουσιοδότησης, ειδικά για προνομιακούς λογαριασμούς.

(2) Να εφαρμόζει πολιτική για τη διαχείριση των κωδικών πρόσβασης του χρήστη.

Ασφάλεια δικτύου. Κ.Δ.Π. 389/2020.

12. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Ασφάλεια δικτύου», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) (α) Να εξασφαλίζει την κατάλληλη εφεδρεία των κρίσιμων στοιχείων του δικτύου, έτσι ώστε πιθανή βλάβη να μην προκαλέσει σημαντική αλλοίωση της λειτουργίας του δικτύου και των παρεχομένων υπηρεσιών στους συνδρομητές του,

(β) Να σχεδιάζει λύσεις εφεδρείας στα μέρη του δικτύου του, με την εφεδρεία να αντανακλά την κρισιμότητα των μερών του δικτύου, στη βάση των αποτελεσμάτων της αξιολόγησης επικινδυνότητας του δικτύου την οποία έχει διενεργήσει προηγουμένως:

Νοείται ότι, ο σχεδιασμός του δικτύου θα πρέπει να προνοεί για την υλοποίηση λύσεων αυτόματης εφεδρείας που επιτρέπουν την αδιάλειπτη λειτουργία του δικτύου. Στις περιπτώσεις που δεν είναι τεχνικώς δυνατή η υλοποίηση σχεδιασμού αυτόματων λύσεων εφεδρείας (αυτόματη δρομολόγηση κίνησης μέσω εναλλακτικών διοδεύσεων), τότε ο παροχέας οφείλει να προβαίνει στις απαραίτητες ενέργειες για την ταχεία επιδιόρθωση της βλάβης,

(γ) Να σχεδιάζει τα δίκτυα του ώστε η εφεδρεία των κρίσιμων στοιχείων των δικτύων να επιτυγχάνεται με τρόπο που να επιτρέπει την εγκατάσταση των κρίσιμων στοιχείων σε διαφορετικά υποστατικά του παροχέα, με τρόπο ώστε να εξασφαλίζεται η εφεδρεία μέσω της γεωγραφικής διασποράς. Ο παροχέας δύναται να αφίσταται της υποχρέωσης αυτής, όταν αντικειμενικοί λόγοι επιβάλουν διαφορετική σχεδίαση του δικτύου του. Σε κάθε περίπτωση, ο παροχέας οφείλει να ενημερώνει την Αρχή για τους λόγους της αδυναμίας αυτής, ώστε να αξιολογήσει τη βασιμότητά του και να επιβάλει αναλογικές υποχρεώσεις.

Ασφάλεια συστημάτων. Κ.Δ.Π. 389/2020.

13. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Ασφάλεια συστημάτων», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με την ακόλουθη υποχρέωση:

(1) Να εφαρμόζει ενισχυμένα μέτρα σχετικά με την ακεραιότητα λογισμικού και τη διαχείριση ενημερώσεων ασφάλειας για κρίσιμα στοιχεία ενεργητικού σε εικονικοποιημένα δίκτυα (virtualised networks).

Φυσική ασφάλεια. Κ.Δ.Π. 389/2020.

14. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Φυσική ασφάλεια», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) (α) Να εφαρμόζει πολιτική για μέτρα φυσικής ασφάλειας και περιβαλλοντικούς ελέγχους, συμπεριλαμβανομένων των εγκαταστάσεων και των συστημάτων που καλύπτονται,

(β) Να εφαρμόζει ενισχυμένα μέτρα για φυσική πρόσβαση σε κρίσιμα στοιχεία ενεργητικού:

Νοείται ότι, η φυσική πρόσβαση σε κρίσιμα στοιχεία ενεργητικού θα πρέπει να είναι ελεγχόμενη και να παρέχεται μόνο σε περιορισμένο αριθμό εκπαιδευμένου και εξειδικευμένου προσωπικού. Η πρόσβαση από τρίτους επιτρέπεται, μόνο, εάν υπάρχει εύλογη αιτία και πρέπει να είναι ελεγχόμενη και να παρακολουθείται.

(2) Να διασφαλίζει την ασφάλεια των κρίσιμων προμηθειών. Μεταξύ άλλων πρέπει να διαθέτει εφεδρική τροφοδοσία ισχύος ή/και εφεδρικό καύσιμο.

(3) (α) Να εφαρμόζει πολιτική για την ασφάλεια κρίσιμων προμηθειών,

(β) Να εφαρμόζει, υψηλού επιπέδου, μέτρα ασφάλειας για την προστασία κρίσιμων προμηθειών και υποστηρικτικών εγκαταστάσεων:

Νοείται ότι, υψηλού επιπέδου μέτρα ασφάλειας είναι, μεταξύ άλλων, η αυτόματη επανεκκίνηση μετά από διακοπή ρεύματος, εφεδρικές μπαταρίες, γεννήτριες και εφεδρικά καύσιμα.

(4) Να μεριμνά για τη φυσική ασφάλεια των εγκαταστάσεων, όπου βρίσκεται εγκατεστημένος ο εξοπλισμός των δικτύων του, λαμβάνοντας μέτρα φυσικής ασφάλειας για κάθε υποστατικό ανάλογα με την κρισιμότητα του εξοπλισμού που φιλοξενεί. Σε περίπτωση συνεγκατάστασης, η

κατανομή της ευθύνης για τη φυσική ασφάλεια των εγκαταστάσεων καθώς και για τον έλεγχο της πρόσβασης γίνεται με τη σχετική συμφωνία πλαίσιο των μερών, σύμφωνα με το άρθρο 9(1)(δ) του περί Παροχής Συνεγκατάστασης και από Κοινού Χρήσης Διευκολύνσεων Διατάγματος του 2012, ως εκάστοτε τροποποιείτε ή/και αντικαθίσταται.

Κ.Δ.Π. 247/2013.

Ενδεικτικά μέτρα φυσικής ασφάλειας περιλαμβάνουν τον έλεγχο πρόσβασης σε υποστατικά, προστασία από σεισμούς, πλημμύρες, υπερθέρμανση, φωτιά, κεραυνούς και άλλες φυσικές καταστροφές.

(5) Να ακολουθεί σχεδιασμούς που εγγυώνται ότι, τα στοιχεία του δικτύου ή/και των υπηρεσιών, τα οποία έχουν αξιολογηθεί ως ζωτικής σημασίας, είναι εγκατεστημένα σε διαφορετικές εγκαταστάσεις ή σε χώρους φυσικά ανεξάρτητους. Στις περιπτώσεις όπου τα στοιχεία του δικτύου δεν μπορούν να εγκατασταθούν σε διαφορετικά υποστατικά θα πρέπει να λαμβάνεται πρόνοια ώστε ο εξοπλισμός να προστατεύεται από ανεξάρτητα μέσα φυσικής προστασίας,

(6) Σχετικά με τον έλεγχο πρόσβασης σε υποστατικά όπου βρίσκεται εγκατεστημένος εξοπλισμός του δικτύου, ο οποίος έχει προηγουμένως χαρακτηριστεί ως ζωτικής σημασίας, θα πρέπει να εγκαθίστανται ειδικά συστήματα τα οποία να αποτρέπουν τη μη εξουσιοδοτημένη πρόσβαση και να καθορίζονται διαδικασίες ασφάλειας μέσω των οποίων να ελέγχεται η πρόσβαση στους παραπάνω χώρους.

(7) Να διαθέτει μηχανισμούς και διαδικασίες για την άμεση πληροφόρηση του ως προς γεγονότα που απειλούν την φυσική ασφάλεια των στοιχείων του δικτύου και των χώρων όπου αυτά είναι εγκατεστημένα.

(8) Να συνεργάζεται με τους αρμόδιους φορείς και υπηρεσίες (κρατικές και ιδιωτικές), με στόχο την ελαχιστοποίηση της πιθανότητας ζημίας στα στοιχεία του δικτύου ή/της υπηρεσίας του, στις περιπτώσεις όπου διενεργούνται εργασίες που πιθανόν να επηρεάζουν το δίκτυο του.

(9) (α) Να εξασφαλίζει ότι η παροχή της κύριας τροφοδοσίας του εξοπλισμού γίνεται στη βάση των ενδεδειγμένων προδιαγραφών του,

(β) Να εξασφαλίζει την αδιάλειπτη παροχή τροφοδοσίας σε περίπτωση διακοπής της κύριας τροφοδοσίας σε υποστατικό όπου στεγάζονται κρίσιμα σημεία του δικτύου λόγω βλάβης,

(γ) Να μεριμνά ώστε η παροχή τροφοδοσίας στα κρίσιμα στοιχεία του δικτύου να μην διακόπτεται στην περίπτωση διακοπής της κύριας τροφοδοσίας,

(δ) Κοινές πρακτικές που εφαρμόζονται σε περιπτώσεις απώλειας της κύριας πηγής τροφοδοσίας περιλαμβάνονται στο ΠΑΡΑΡΤΗΜΑ 3 της παρούσας Απόφασης.

(10) Να λαμβάνει όλα τα απαραίτητα μέτρα για την επαρκή προστασία του εξοπλισμού που χρησιμοποιείται στα δίκτυα του:

Νοείται ότι, η προστασία του εξοπλισμού αφορά ιδίως την τήρηση μέτρων για τη φυσική προστασία του εξοπλισμού, την τήρηση των προδιαγραφών λειτουργίας του εξοπλισμού καθώς και την τήρηση των απαιτήσεων συντήρησής του:

Νοείται περαιτέρω ότι, σε περίπτωση που διαπιστωθεί ότι, εξοπλισμός ή στοιχείο δικτύου προκαλεί υποβάθμιση της λειτουργικής ικανότητας του δικτύου, οι παροχείς οφείλουν να λαμβάνουν αμέσως μέτρα αποκατάστασης της εύρυθμης λειτουργίας του δικτύου, αποκαθιστώντας το συντομότερο δυνατό την κανονική λειτουργία του εξοπλισμού ή αποσυνδέοντάς τον από το δίκτυο, ως τελευταίο μέτρο.

Διαχείριση συμβάντων και περιστατικών. Κ.Δ.Π. 389/2020.

15. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Διαχείριση συμβάντων και περιστατικών», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να βεβαιώνεται ότι, το προσωπικό του είναι διαθέσιμο και προετοιμασμένο να διαχειριστεί περιστατικά ασφάλειας.

(2) Να χρησιμοποιεί αποτελεσματικά συστήματα και διαδικασίες για τον εντοπισμό περιστατικών ασφάλειας.

Επιχειρησιακή συνέχεια και ανθεκτικότητα. Κ.Δ.Π. 389/2020.

16. Επιπρόσθετα από όσα αναφέρονται στην κατηγορία «Επιχειρησιακή συνέχεια και ανθεκτικότητα», στο ΠΑΡΑΡΤΗΜΑ ΙΙΙ της Απόφασης Μέτρων Ασφαλείας του 2020, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) (α) Να παρακολουθεί την ενεργοποίηση και εκτέλεση των σχεδίων έκτακτης ανάγκης και να καταγράφει τους επιτυχημένους και αποτυχημένους χρόνους ανάκτησης λειτουργίας του δικτύου ή/και των παρεχόμενων υπηρεσιών,

(β) Να διασφαλίζει ότι τα σχέδια έκτακτης ανάγκης περιλαμβάνουν πρόνοιες για εξαρτώμενους και αλληλοεξαρτώμενους φορείς εκμετάλλευσης βασικών υπηρεσιών ή/και φορείς κρίσιμων υποδομών πληροφοριών.

(2) Να διασφαλίζει την ύπαρξη υψηλού επιπέδου δυνατοτήτων αποκατάστασης από καταστροφές ή τη διαθεσιμότητα τους από τρίτα μέρη.

(3) (α) Να εφαρμόζει πρόγραμμα ασκήσεων για τον έλεγχο σχεδίων έκτακτης ανάγκης και την ανάκτηση εφεδρικών αντιγράφων δεδομένων, σε τακτά χρονικά διαστήματα, χρησιμοποιώντας ρεαλιστικά σενάρια, που με την πάροδο του χρόνου να καλύπτουν μια σειρά διαφορετικών σεναρίων,

(β) Να βεβαιώνει ότι, τα διδάγματα που προκύπτουν από τις ασκήσεις λαμβάνονται υπόψη από τους υπεύθυνους για την κατάλληλη ενημέρωση των διαδικασιών και συστημάτων.

(4) Να λαμβάνει τα αναγκαία μέτρα για να διασφαλίσει την αδιάκοπη πρόσβαση σε υπηρεσίες έκτακτης ανάγκης. Ενδεικτικά μέτρα είναι η εναλλακτική δρομολόγηση των κλήσεων, η αποφυγή μοναδικών σημείων αποτυχίας (single points of failure), όπως η αποφυγή εξάρτησης από μηχανήματα εγκατεστημένα σε ένα χώρο για την διαχείριση των τηλεφωνημάτων σε αριθμούς έκτακτης ανάγκης και η ύπαρξη καναλιών αφιερωμένων αποκλειστικά στους αριθμούς έκτακτης ανάγκης:

Νοείται ότι, ο παροχέας οφείλει να εξασφαλίζει την προτεραιότητα των κλήσεων σε υπηρεσίες έκτακτης ανάγκης:

Νοείται περαιτέρω ότι, είναι μέγιστης σημασίας στην περίπτωση καταστροφικών συμβάντων η εξασφάλιση της αδιάκοπης πρόσβασης σε υπηρεσίες έκτακτης ανάγκης, όπως είναι ενδεικτικά οι κλήσεις στον αριθμό 112 ή σε εθνικούς αριθμούς έκτακτης ανάγκης ή σε εναρμονισμένους αριθμούς για εναρμονισμένες υπηρεσίες κοινωνικού ενδιαφέροντος όπως είναι οι αριθμοί της σειράς 116xxx, ως αυτοί αναφέρονται στο Διάταγμα Αριθμοδότησης του 2018, ως εκάστοτε τροποποιείται ή/και αντικαθίσταται.

Κ.Δ.Π.63/2018.

Άλλα μέτρα.

17. Επιπρόσθετα από τις υποχρεώσεις που αναφέρονται στην παρούσα Απόφαση, κάθε παροχέας οφείλει να συμμορφώνεται και με τις ακόλουθες υποχρεώσεις:

(1) Να πραγματοποιεί δοκιμές πάνω στα δίκτυα και τα συστήματα πληροφοριών, πριν τα χρησιμοποιήσει ή τα συνδέσει με υφιστάμενα συστήματα.

(2) (α) Να εφαρμόζει πολιτική και διαδικασίες για τη δοκιμή δικτύων και συστημάτων πληροφοριών,

(β) Να εφαρμόζει εργαλεία για αυτοματοποιημένες δοκιμές.

(3) Να ενημερώνεται, τακτικά, για απειλές στον κυβερνοχώρο μέσω της παρακολούθησης εξωτερικών ροών πληροφοριών για απειλές (threat intelligence) και μέσω της ανταλλαγής πληροφοριών με σχετικούς Οργανισμούς.

(4) Να εφαρμόζει πρόγραμμα για τη συλλογή και το διαμοιρασμό πληροφοριών για απειλές στον κυβερνοχώρο (threat intelligence program), το οποίο να περιλαμβάνει, μεταξύ άλλων, καθορισμό των ρόλων, αρμοδιοτήτων και σχετικών διαδικασιών.

Σύστημα Διαχείρισης Δικτύου.

18. (1) Κάθε παροχέας οφείλει να παρακολουθεί συνεχώς και σε πραγματικό χρόνο την κατάσταση των στοιχείων/εξοπλισμού των δικτύων του, μέσω της λειτουργίας κατάλληλου Συστήματος Διαχείρισης Δικτύου (Network Management System), ως προς τη λειτουργική τους δυνατότητα και τις πιθανές βλάβες οι οποίες μπορούν να προκύψουν κατά τη λειτουργία του εξοπλισμού. Κάθε παροχέας οφείλει, επίσης, να εξετάζει το ενδεχόμενο δημιουργίας Κέντρου Επιχειρήσεων Ασφάλειας (Security Operations Centre), για καλύτερη παρακολούθηση των θεμάτων ασφάλειας του δικτύου και

(2) Κάθε παροχέας οφείλει να διατηρεί προσωπικό το οποίο να εργάζεται με ωράριο βάρδιας, ώστε να μπορεί να ανταποκριθεί άμεσα σε βλάβες που πιθανόν να επηρεάσουν τις παρεχόμενες υπηρεσίες προς τους συνδρομητές.

Διαχείριση αύξησης κίνησης.

19. (1) Κάθε παροχέας οφείλει να προστατεύει την ακεραιότητα του δικτύου του από συνθήκες αυξημένης κίνησης, χρησιμοποιώντας τεχνικές διαχείρισης της κίνησης με στόχο τον έγκαιρο εντοπισμό της αυξημένης κίνησης και την προστασία του δικτύου από αυτήν.

(2) Κάθε παροχέας οφείλει να διαστασιοποιεί το δίκτυο του ανάλογα με προβλέψεις τις οποίες διενεργούν για γεγονότα τα οποία ενδέχεται να προκαλέσουν σημαντική αύξηση της κίνησης στο δίκτυο του.

(3) Κάθε παροχέας οφείλει να προβαίνει σε ιεράρχηση κλήσεων φορέων εκμετάλλευσης βασικών υπηρεσιών ή/και φορέων κρίσιμων υποδομών πληροφοριών, σε περιπτώσεις εκτάκτων συνθηκών, μετά από αίτημα των φορέων αυτών.

(4) Κάθε παροχέας οφείλει να καταγράφει τις τεχνικές διαχείρισης κίνησης και τις συνθήκες υπό τις οποίες τις εφαρμόζει. Οφείλει να καταγράφει, επίσης, τα μέτρα τα οποία χρησιμοποιεί προκειμένου να εξασφαλίσει την προτεραιότητα της κίνησης προς τις υπηρεσίες έκτακτης ανάγκης, ιδιαίτερα σε καταστάσεις εκτάκτων συνθηκών.

ΜΕΡΟΣ ΙΙΙ
Ενημέρωση

Αλληλο-ενημέρωση Παροχέων.

20. (1) Κάθε παροχέας οφείλει να ενημερώνει, εγκαίρως και γραπτώς και μέσω των συμφωνημένων οδών, τους παροχείς άλλων δικτύων, τα οποία ενδέχεται να επηρεαστούν από προγραμματισμένες εργασίες στο δίκτυό του, συμπεριλαμβανομένης και της συντήρησης.

(2) Κάθε παροχέας οφείλει να ειδοποιεί εγκαίρως και με κατάλληλο τρόπο τους παροχείς άλλων διασυνδεόμενων δικτύων για αναμενόμενα γεγονότα τα οποία ενδέχεται να προκαλέσουν ιδιαίτερα αυξημένη κίνηση στο δίκτυό του και να επηρεάσουν τα δίκτυα των άλλων παροχέων.

(3) Στην περίπτωση διασυνδεόμενων δικτύων, ο παροχέας, ο οποίος αντιλαμβάνεται βλάβη, οφείλει να ειδοποιεί άμεσα άλλους παροχείς τους οποίους ενδεχομένως επηρεάζει αυτή. Ο παροχέας οφείλει να λαμβάνει άμεσα μέτρα για την αποκατάσταση της βλάβης.

(4) Παροχείς οι οποίοι διασυνδέουν τα δίκτυα τους θα πρέπει να διαθέτουν σαφείς και καταγεγραμμένες διαδικασίες επικοινωνίας του προσωπικού τους με το προσωπικό των παροχέων διασυνδεόμενων δικτύων, με σκοπό την συνεργασία και τον συντονισμό των διαδικασιών αποκατάστασης της ομαλής λειτουργίας των δικτύων:

Νοείται ότι, ο τρόπος επικοινωνίας/ανταλλαγής ενημερωτικών μηνυμάτων μεταξύ των παροχέων περιγράφεται στις εξειδικευμένες συμφωνίες μεταξύ των δύο Μερών.

Ενημέρωση καταναλωτών.

21. (1) Κάθε παροχέας, όπου είναι εφικτό και στην περίπτωση που το δίκτυο αδυνατεί να διεκπεραιώσει τηλεφωνικές κλήσεις για χρονικό διάστημα διάρκειας τουλάχιστον μίας (1) ώρας λόγω βλάβης ή προγραμματισμένων εργασιών συντήρησης και σε περιπτώσεις διακοπών που θα ξεπερνούν σε διάρκεια τουλάχιστον τη μία (1) ώρα, θα πρέπει να ενημερώνει το συνδρομητή/χρήστη με ηχογραφημένο μήνυμα για την αδυναμία παροχής της υπηρεσίας καθώς επίσης και τους συνδρομητές/χρήστες των υπηρεσιών του δικτύου οι οποίοι ενδέχεται να επηρεαστούν από την προγραμματιζόμενη διακοπή. Το ηχογραφημένο μήνυμα θα μεταδίδεται κατά την απόπειρα του συνδρομητή/χρήστη να πραγματοποιήσει τηλεφωνική κλήση. Σε κάθε περίπτωση, το προσωπικό του παροχέα οφείλει να είναι επαρκώς ενημερωμένο, ώστε να παρέχει τη σχετική πληροφόρηση κατόπιν αιτήματος του καταναλωτή:

Νοείται ότι, σε περιπτώσεις όπου το δίκτυο αδυνατεί να διεκπεραιώσει τηλεφωνικές κλήσεις λόγω βλάβης ή προγραμματισμένων εργασιών συντήρησης, η ενημέρωση των συνδρομητών/χρηστών των υπηρεσιών του δικτύου, οι οποίοι ενδέχεται να επηρεαστούν από την βλάβη ή την προγραμματιζόμενη διακοπή, πρέπει να γίνεται με παροχή ηχογραφημένου μηνύματος ή/και αποστολή γραπτού μηνύματος (sms) ή/και αποστολή γραπτού ηλεκτρονικού μηνύματος (email) προς τον επηρεαζόμενο συνδρομητή/χρήστη:

Νοείται περαιτέρω ότι, η ενημέρωση των συνδρομητών/χρηστών των υπηρεσιών του δικτύου, οι οποίοι ενδέχεται να επηρεαστούν από την προγραμματιζόμενη διακοπή, πρέπει επιπλέον να γίνεται και με ανακοίνωση στην επίσημη ιστοσελίδα του παροχέα, μέσω δημόσιας ανάρτησης στους επίσημους λογαριασμούς του παροχέα σε μέσα κοινωνικής δικτύωσης ή/και με ανακοίνωση σε μέσα μαζικής ενημέρωσης:

Νοείται έτι περαιτέρω ότι, σε περιπτώσεις όπου υπάρχει γνώση ότι δεν μπορεί να λειτουργήσει ένας τρόπος επικοινωνίας, όπως αναφέρεται ανωτέρω, τότε ο παροχέας υποχρεούται να χρησιμοποιεί το ανάλογο μέσο για να ενημερώσει τους καταναλωτές/χρήστες των υπηρεσιών του δικτύου του με τρόπο που να διασφαλίζει την ολοκλήρωση της ενημέρωσης αυτής:

Νοείται έτι, έτι περαιτέρω ότι, η ενημέρωση πρέπει να είναι άμεση σε περίπτωση που επηρεάζεται η πρόσβαση σε υπηρεσίες έκτακτης ανάγκης, όπως είναι ενδεικτικά οι κλήσεις στον αριθμό 112 ή σε εθνικούς αριθμούς έκτακτης ανάγκης ή/και σε εναρμονισμένους αριθμούς για εναρμονισμένες υπηρεσίες κοινωνικού ενδιαφέροντος όπως είναι οι αριθμοί της σειράς 116xxx, ως αυτοί αναφέρονται στο Διάταγμα Αριθμοδότησης του 2018, ως εκάστοτε τροποποιείται ή/και αντικαθίσταται.

Κ.Δ.Π.63/2018.

(2) Κάθε παροχέας οφείλει να εφαρμόζει πολιτική και διαδικασίες για την τακτική ενημέρωση των τελικών χρηστών (end-users), σχετικά με απειλές ασφάλειας στα δίκτυα ή/και τις υπηρεσίες που ενδέχεται να τους επηρεάσουν.

ΜΕΡΟΣ IV
Έλεγχος και διαβουλεύσεις

Έλεγχος και αξιολόγηση πληροφοριών. Κ.Δ.Π. 389/2020.

22. Η Αρχή δύναται κατά την κρίση της να ελέγχει την ορθή εκτέλεση των υποχρεώσεων που απορρέουν από την παρούσα Απόφαση και τα σχετικά Παραρτήματα, καθώς επίσης και την ακρίβεια των πληροφοριών που της παρέχονται σύμφωνα με την παρούσα Απόφαση, εφαρμόζοντας τα οριζόμενα στο άρθρο 16, του ΜΕΡΟΥΣ VIII της Απόφασης των Μέτρων Ασφάλειας του 2020:

Νοείται ότι, τα έγγραφα που προβλέπονται στο άρθρο 13 της Απόφασης των Μέτρων Ασφάλειας του 2020, με τα οποία υποχρεούται ο κάθε παροχέας να παρέχει τη σχετική πληροφόρηση στην Αρχή, καλύπτουν και τις επιπρόσθετες υποχρεώσεις που περιλαμβάνονται στην παρούσα Απόφαση.

Δημόσιες Διαβουλεύσεις. Κ.Δ.Π. 389/2020.

23. Τηρουμένων των διατάξεων του άρθρου 17, του ΜΕΡΟΥΣ VIII της Απόφασης των Μέτρων Ασφάλειας του 2020, η Αρχή, εάν το θεωρεί αναγκαίο, δύναται να έχει διαβουλεύσεις με τα κατά περίπτωση ενδιαφερόμενα μέρη σχετικά με θέματα ασφάλειας δικτύων και συστημάτων πληροφοριών.

ΜΕΡΟΣ V
Συμμόρφωση – κυρώσεις

Παραβίαση υποχρέωσης. Κ.Δ.Π. 389/2020.

24. Σε περίπτωση που παροχέας παραβιάζει υποχρέωση που απορρέει από την παρούσα Απόφαση ισχύουν οι διατάξεις του ΜΕΡΟΥΣ IX της Απόφασης των Μέτρων Ασφάλειας του 2020.

ΜΕΡΟΣ VI
Τελικές Διατάξεις

Συμμόρφωση με πρόγραμμα ενεργειών. Κ.Δ.Π. 389/2020.

25. Κάθε παροχέας, για την υλοποίηση των προνοιών της παρούσας Απόφασης οφείλει να συμμορφωθεί με το πρόγραμμα ενεργειών που προνοεί το άρθρο 21 (1) (β), (γ) και (δ) της Απόφασης των Μέτρων Ασφάλειας του 2020.

Σε εξαιρετικές περιπτώσεις, μετά από αιτιολογημένη αίτηση του παροχέα δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών και εφόσον αυτό δικαιολογείται αντικειμενικά, η Αρχή μπορεί να αποδεχτεί κατάλληλη προσαρμογή των προθεσμιών συμμόρφωσης για κάθε περίπτωση ξεχωριστά.

Τροποποιήσεις.

26. Η Αρχή δύναται με Απόφαση της να καταργεί/αντικαθιστά, τροποποιεί ή/και να συμπληρώνει την παρούσα Απόφαση ή/και τα Παραρτήματα της. Για την τροποποίηση ή συμπλήρωση της παρούσας Απόφασης ή/και των Παραρτημάτων της, η Αρχή δύναται να προβαίνει σε δημόσια διαβούλευση. Η εκάστοτε τροποποίηση θα δημοσιεύεται στην Επίσημη Εφημερίδα της Δημοκρατίας και θα αναρτάται στην ιστοσελίδα της Αρχής.

Κατάργηση. Κ.Δ.Π. 253/2011.

27. Τρεις (3) μήνες από την ημερομηνία δημοσίευσης στην Επίσημη Εφημερίδα της Δημοκρατίας της παρούσας Απόφασης, το περί Ασφάλειας Δικτύων και Πληροφοριών Διάταγμα του 2011 καταργείται και αντικαθίσταται από την παρούσα Απόφαση.

Έναρξη ισχύος.

28. Η παρούσα Απόφαση τίθεται σε ισχύ τρεις (3) μήνες από την ημερομηνία δημοσίευσής της στην Επίσημη Εφημερίδα της Δημοκρατίας.

ΠΑΡΑΡΤΗΜΑ 1 : ΠΛΑΙΣΙΟ ΑΞΙΟΛΟΓΗΣΗΣ ΕΠΙΚΙΝΔΥΝΟΤΗΤΑΣ

Επιπρόσθετα, από όσα αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Ι της Απόφασης των Μέτρων Ασφαλείας του 2020 (Κ.Δ.Π.389/2020), στο πλαίσιο αξιολόγησης επικινδυνότητας κάθε παροχέας οφείλει να συμμορφώνεται και με τα ακόλουθα:

(1) Ως βέλτιστη πρακτική, οι παροχείς προτρέπονται όπως καθορίζουν κριτήρια/παραμέτρους βάσει των οποίων ιεραρχούνται τα στοιχεία του δικτύου τους, ως προς την κρισιμότητά/σημασία τους, αναφορικά με τη λειτουργία του δικτύου και τη διαθεσιμότητα των υπηρεσιών. Η ιεράρχηση της σημασίας των μερών του δικτύου επηρεάζει σημαντικά τη λήψη διορθωτικών μέτρων.

(2) Στο πλαίσιο της διασύνδεσης δικτύων ενός ή περισσοτέρων παροχέων, οι παροχείς θα πρέπει επίσης να καταγράφουν τη σύνδεση των κρίσιμων μερών του δικτύου τους με άλλα δίκτυα.

ΠΑΡΑΡΤΗΜΑ 2: ΣΧΕΔΙΟ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

Το σχέδιο επιχειρησιακής συνέχειας κάθε παροχέα ηλεκτρονικών επικοινωνιών θα πρέπει, εκτός από όσα αναφέρονται στο ΠΑΡΑΡΤΗΜΑ ΙΙ της Απόφασης των Μέτρων Ασφαλείας του 2020 (Κ.Δ.Π.389/2020), να περιλαμβάνει και:

Τους χρόνους αποκατάστασης σε διαφορετικές συνθήκες βλάβης. Σε περιπτώσεις βλαβών που οφείλονται σε τρίτο δίκτυο (σε περίπτωση που δίκτυο ενός παροχέα φιλοξενείται στις εγκαταστάσεις άλλου δικτύου), ισχύουν οι πρόνοιες που περιλαμβάνονται στις σχετικές συμφωνίες που συνάπτονται στη βάση Υποδειγμάτων Προσφοράς Υπηρεσίας, όπως τροποποιούνται από τον Επίτροπο.

ΠΑΡΑΡΤΗΜΑ 3: ΚΟΙΝΕΣ ΠΡΑΚΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΩΛΕΙΑΣ ΤΡΟΦΟΔΟΣΙΑΣ

(1) Κοινές πρακτικές που εφαρμόζονται, από παροχείς ηλεκτρονικών επικοινωνιών, σε περιπτώσεις απώλειας της κύριας πηγής τροφοδοσίας του υποστατικού/ιστού κλπ., είναι η ύπαρξη εφεδρικών συστοιχιών (μπαταριών) που μπορούν να υποστηρίξουν τη λειτουργία του εξοπλισμού για μικρό χρονικό διάστημα, καθώς και ηλεκτρογεννητριών.

(2) Οι εφεδρικές συστοιχίες (μπαταρίες) θα πρέπει να έχουν επαρκή ικανότητα για να υποστηρίξουν τη λειτουργία των κρίσιμων στοιχείων του δικτύου, από τη στιγμή παύσης παροχής τροφοδοσίας από το δημόσιο δίκτυο τροφοδοσίας έως την έναρξη λειτουργίας των γεννητριών. Οι εφεδρικές συστοιχίες συντηρούνται, σύμφωνα με τις συνθήκες του κατασκευαστή και λαμβάνονται όλα τα μέτρα για την εξασφάλιση της εύρυθμης λειτουργίας τους.

(3) Ο χρόνος για τον οποίο εξασφαλίζεται η συνέχεια λειτουργίας των στοιχείων του δικτύου μέσω εφεδρικής τροφοδοσίας διαφέρει για κάθε στοιχείο του δικτύου και ο σχεδιασμός γίνεται πάντα στη βάση των αποτελεσμάτων της αξιολόγησης επικινδυνότητας και της αναγνώρισης των κρίσιμων στοιχείων του δικτύου του παροχέα.

(4) Περαιτέρω, κάθε παροχέας ηλεκτρονικών επικοινωνιών θα πρέπει να εξασφαλίζει ότι υπάρχει επαρκής αριθμός εφεδρικών φορητών γεννητριών για να εξυπηρετήσει το δίκτυο του και προτρέπεται όπως διαθέτει επιπρόσθετη πηγή εφεδρικής τροφοδοσίας για τα κρίσιμα στοιχεία του δικτύου του, τα οποία δεν εξυπηρετούνται από την ίδια πηγή.

(5) Κάθε παροχέας θα πρέπει να διενεργεί τακτικούς ελέγχους για την εξακρίβωση του λειτουργικού επιπέδου των συστημάτων εφεδρικής τροφοδοσίας, ανά πάσα χρονική στιγμή, συμπεριλαμβανομένων διαδικασιών για παροχή καυσίμων στις γεννήτριες.

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

Σύμφωνα με τα άρθρα 17(ιη), 17(ιθ), 17 (λα), 20(1)(α), 20(1)(β), 20(1)(γ), 20(1)(ε), 40, 43 και 46 του περί της Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμου του 2020, η Αρχή Ψηφιακής Ασφάλειας προβαίνει στην έκδοση Απόφασης για τα Μέτρα Ασφάλειας των Παροχέων Δικτύων ή/και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών.

Η Απόφαση καθορίζει τις ελάχιστες επιπρόσθετες υποχρεώσεις σχετικά με την ασφάλεια δικτύων και συστημάτων πληροφοριών, πέραν από τα οριζόμενα στην Απόφαση των Μέτρων Ασφάλειας 2020 (Κ.Δ.Π. 389/2020) ως αυτή εκάστοτε τροποποιείται ή/και αντικαθίσταται, τις οποίες πρέπει να τηρούν οι παροχείς ηλεκτρονικών επικοινωνιών οι οποίοι λειτουργούν δίκτυα ή/και υπηρεσίες ηλεκτρονικών επικοινωνιών.