ΠΡΟΤΑΣΗ

Σύμφωνα με το άρθρο 116 παράγραφος 6 του νόμου για τις ηλεκτρονικές επικοινωνίες (UL RS αριθ. 130/22 και 18/23 — ZDU-1O), ο Οργανισμός Επικοινωνιακών Δικτύων και Υπηρεσιών της Δημοκρατίας της Σλοβενίας, λαμβάνοντας υπόψη τη διαδικασία πληροφόρησης σύμφωνα με την οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών (ΕΕ L 241 της 17.9.2015, σ. 1), εκδίδει τα ακόλουθα:

ΓΕΝΙΚΗ ΠΡΑΞΗ
σχετικά με πρόσθετες απαιτήσεις και περιορισμούς ασφάλειας

Άρθρο 1
(Περιεχόμενο της γενικής πράξης)

Η παρούσα γενική πράξη προβλέπει τα εξής:

1. κατευθυντήριες γραμμές που πρέπει να ακολουθούνται από τους φορείς εκμετάλλευσης δικτύων κινητών επικοινωνιών (στο εξής: φορείς εκμετάλλευσης) οι οποίοι παρέχουν τα εν λόγω δίκτυα σε κρίσιμες οντότητες που είναι διαχειρίστριες κρίσιμων υποδομών σε άλλους τομείς ρύθμισης κρίσιμων υποδομών, όπως ορίζεται στη νομοθεσία που διέπει τον τομέα των κρίσιμων υποδομών (στο εξής: διαχειριστές κρίσιμων υποδομών), από τους παρόχους βασικών υπηρεσιών όπως ορίζονται στη νομοθεσία που διέπει την ασφάλεια των πληροφοριών (στο εξής: πάροχοι βασικών υπηρεσιών), από τα όργανα της κρατικής διοίκησης όπως ορίζονται στη νομοθεσία που διέπει την ασφάλεια των πληροφοριών (στο εξής: όργανα κρατικής διοίκησης) ή από τους φορείς βασικών τμημάτων του συστήματος ασφάλειας της χώρας και
2. κρίσιμα στοιχεία του δικτύου και των συναφών πληροφοριακών συστημάτων με τις λειτουργίες τους που αναφέρονται στο άρθρο 116 παράγραφος 6 του νόμου για τις ηλεκτρονικές επικοινωνίες (UL RS αριθ. 130/22 και 18/23 — ZDU-1O, στο εξής: νόμος), όπως ορίζονται στο παράρτημα, το οποίο αποτελεί αναπόσπαστο μέρος της παρούσας γενικής πράξης και καταρτίζεται σε συνεργασία με το όργανο που είναι αρμόδιο για την ασφάλεια των πληροφοριών.

Άρθρο 2
(Έννοιες όρων)

(1) Οι όροι που χρησιμοποιούνται στην παρούσα γενική πράξη έχουν τις εξής έννοιες:

1. Αλυσίδα εφοδιασμού είναι το σύνολο του συστήματος διαδικασιών, προσώπων, οργάνωσης και διανομής που συμμετέχουν στον σχεδιασμό, την παραγωγή, την αποθήκευση, τη διανομή και τον εφοδιασμό, καθώς και την εγκατάσταση και συντήρηση συστατικών στοιχείων κρίσιμων στοιχείων δικτύου που είναι εγκατεστημένα στο δίκτυο του φορέα εκμετάλλευσης ή στον πάροχο υπηρεσιών υπολογιστικού νέφους που παρέχει τις εν λόγω υπηρεσίες στον φορέα εκμετάλλευσης.

2. Κρίσιμα στοιχεία του δικτύου είναι τα στοιχεία, οι λειτουργίες, οι υπηρεσίες και τα υποστηρικτικά πληροφοριακά συστήματα του δικτύου υπό μορφή υλική, λογισμικού ή εικονικοποιημένη στον φορέα εκμετάλλευσης ή στον πάροχο υπηρεσιών υπολογιστικού νέφους, όπως απαριθμούνται στο παράρτημα της παρούσας γενικής πράξης.

3. Κρίσιμες οντότητες είναι οι διαχειριστές κρίσιμων υποδομών σε άλλους τομείς ρύθμισης των κρίσιμων υποδομών που καθορίζονται σύμφωνα με τη νομοθεσία που διέπει τον τομέα των κρίσιμων υποδομών, οι πάροχοι βασικών υπηρεσιών όπως καθορίζονται από τη νομοθεσία που διέπει την ασφάλεια των πληροφοριών, τα όργανα της κρατικής διοίκησης όπως καθορίζονται από τη νομοθεσία που διέπει την ασφάλεια των πληροφοριών και οι φορείς βασικών τμημάτων του συστήματος ασφάλειας της χώρας.

(2) Λοιποί όροι που χρησιμοποιούνται στην παρούσα γενική πράξη έχουν την ίδια έννοια με εκείνη που ορίζεται από τον νόμο και τη γενική πράξη για την ασφάλεια δικτύων, υπηρεσιών και δεδομένων.

Άρθρο 3
(Γενικές κατευθυντήριες γραμμές)

(1) Οι φορείς εκμετάλλευσης στην αλυσίδα εφοδιασμού συστατικών στοιχείων κρίσιμων στοιχείων δικτύου και υπηρεσιών υποστήριξης τρίτου επιπέδου για τα συστατικά στοιχεία αυτά λαμβάνουν υπόψη τουλάχιστον τις ακόλουθες κατευθυντήριες γραμμές καθ' όλη τη διάρκεια του κύκλου ζωής των εν λόγω συστατικών στοιχείων:

1. για μεμονωμένο κατασκευαστή ή προμηθευτή και για πάροχο υπηρεσιών υποστήριξης τρίτου επιπέδου λόγω σχέσεων και συμφωνιών με αυτούς, διενεργούν εκτίμηση κινδύνου όσον αφορά τον εφοδιασμό και τις πιθανές επιπτώσεις από τρίτα φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου (στο εξής: τρίτα μέρη), τη συμβατότητα με εξοπλισμό άλλων κατασκευαστών, την ποιότητα και την ασφάλεια των προϊόντων και τις πιθανές αρνητικές επιπτώσεις στη λειτουργία των υπηρεσιών και των κρίσιμων οντοτήτων του φορέα εκμετάλλευσης·
2. η ασφάλεια είναι ενσωματωμένη και εφαρμόζεται ήδη στον σχεδιασμό και οι συμβάσεις περιλαμβάνουν προθεσμίες για την εξάλειψη των αντιληπτών τρωτών σημείων·
3. βασικά χαρακτηριστικά ασφάλειας (διαθεσιμότητα, εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα) διασφαλίζονται καθ' όλη τη διάρκεια του κύκλου ζωής της χρήσης τους·
4. η ασφάλεια και ο αδιάλειπτος εφοδιασμός με τα στοιχεία αυτά είναι εγγυημένα και επιβεβαιώνεται ότι υποστηρίζει χαρακτηριστικά υψηλής ασφάλειας σύμφωνα με τα διεθνώς αναγνωρισμένα πρότυπα (3GPP) και τα ευρωπαϊκά τεχνικά πρότυπα (ETSI)·
5. οι κατευθυντήριες γραμμές που αναφέρονται στα σημεία 2 έως 4 της παρούσας παραγράφου είναι επαληθεύσιμες στη συμβατική τεκμηρίωση με τον κατασκευαστή ή με τον προμηθευτή·
6. για κάθε κατασκευαστή ή προμηθευτή, αξιολογούνται επίσης και λαμβάνονται υπόψη οι κίνδυνοι που συνδέονται με τα δικαιώματα χρήσης των βασικών τεχνολογιών, οι οποίες είναι αναγκαίες για την κατασκευή και τη χρήση του

εξοπλισμού, καθώς και οι κίνδυνοι που συνδέονται με την προμήθεια εξοπλισμού, ανταλλακτικών ή υπηρεσιών υποστήριξης τρίτου επιπέδου·

7. τα χρησιμοποιούμενα συστατικά στοιχεία δεν έχουν ανεπίλυτα γνωστά κρίσιμα τρωτά σημεία ή τρωτά σημεία που αποτελούν αντικείμενο ενεργής εκμετάλλευσης·
8. αποφεύγουν έναν μεμονωμένο0 κατασκευαστή ή προμηθευτή, όταν αυτό είναι τεχνικά εφικτό και οικονομικά βιώσιμο, με στόχο τη μείωση της εξάρτησης και την αύξηση της ανθεκτικότητας σε περίπτωση κρίσιμων τρωτών σημείων σε συστατικά στοιχεία, καταστροφικής βλάβης του δικτύου ή απειλής για την ασφάλεια των δικτύων και υπηρεσιών κρίσιμων οντοτήτων από τρίτα φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου.

(2) Κατά την παροχή εξοπλισμού, συστημάτων και υπηρεσιών πληροφοριών και επικοινωνιών, οι φορείς εκμετάλλευσης συμμορφώνονται πλήρως με τις κατευθυντήριες γραμμές του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (στο εξής: ο ENISA) και τους ισχύοντες κανονισμούς της Ευρωπαϊκής Ένωσης σχετικά με τις βασικές απαιτήσεις για την ασφάλεια κατά την προμήθεια ασφαλών προϊόντων και υπηρεσιών ΤΠΕ. Ο Οργανισμός δημοσιεύει στον ιστότοπό του συνδέσμους προς τα ισχύοντα έγγραφα του ENISA και τους κανονισμούς της ΕΕ στον προαναφερόμενο τομέα και τους επικαιροποιεί.

(3) Κατά τον εφοδιασμό συστατικών στοιχείων κρίσιμων στοιχείων δικτύου ή τη χρήση υπηρεσιών υπολογιστικού νέφους, δίνεται προτεραιότητα στην επιλογή συστατικών στοιχείων από κατασκευαστές ή προμηθευτές, ή υπηρεσιών από παρόχους υπηρεσιών υπολογιστικού νέφους, οι οποίοι έχουν πιστοποιηθεί από οργανισμούς αξιολόγησης της συμμόρφωσης που έχουν λάβει διαπίστευση και, εάν είναι αναγκαίο, εξουσιοδότηση βάσει του άρθρου 60 παράγραφος 3 του κανονισμού (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Απριλίου 2019, σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (στο εξής: κανονισμός) για την έκδοση ευρωπαϊκών πιστοποιητικών κυβερνοασφάλειας σε ορισμένο επίπεδο διασφάλισης, όπως ορίζεται στο άρθρο 52 του κανονισμού.

(4) Για τους σκοπούς της προηγούμενης παραγράφου, ο φορέας εκμετάλλευσης ανατρέχει σε ειδικό ιστότοπο, που έχει δημιουργηθεί από τον ENISA σύμφωνα με το άρθρο 55 του κανονισμού με σκοπό την ενημέρωση του κοινού σχετικά με τα ευρωπαϊκά σχέδια πιστοποίησης της κυβερνοασφάλειας, τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και τις δηλώσεις συμμόρφωσης ΕΕ, συμπεριλαμβανομένων των πληροφοριών όσον αφορά τα ευρωπαϊκά σχέδια πιστοποίησης της κυβερνοασφάλειας που δεν ισχύουν πλέον, τα ευρωπαϊκά πιστοποιητικά κυβερνοασφάλειας και τις δηλώσεις συμμόρφωσης ΕΕ που έχουν ανακληθεί ή λήξει, καθώς και το αποθετήριο συνδέσμων προς πληροφορίες για την κυβερνοασφάλεια.

Άρθρο 4
(Εκτίμηση κινδύνου)

(1) Κατά τον προσδιορισμό του κινδύνου του κατασκευαστή ή του προμηθευτή συστατικών στοιχείων και του παρόχου υπηρεσιών τρίτου επιπέδου για κρίσιμα στοιχεία του δικτύου, ο φορέας εκμετάλλευσης λαμβάνει υπόψη τις ακόλουθες πτυχές κινδύνου, τις οποίες αξιολογεί.

(2) Κατά την αξιολόγηση που αναφέρεται στην προηγούμενη παράγραφο, ο φορέας εκμετάλλευσης διενεργεί εκτίμηση και λαμβάνει υπόψη τουλάχιστον τα εξής:

1. συνολική ποιότητα (συμπεριλαμβανομένων των πτυχών ασφάλειας) και αξιοπιστία·
2. επίπεδο χρήσης ανοικτών προτύπων και διεπαφών που εμποδίζουν την εξάρτηση και τον εγκλωβισμό στα προϊόντα συγκεκριμένου κατασκευαστή ή προμηθευτή·
3. συμμόρφωση με αναγνωρισμένα διεθνή και ευρωπαϊκά τεχνικά πρότυπα (3GPP, ETSI) και τους κανονισμούς της Ευρωπαϊκής Ένωσης και τις προεπιλεγμένες παραμέτρους ασφάλειας σύμφωνα με επαγγελματικές συστάσεις (Ένωση GSMA)·
4. επίπεδο συμβατότητας με τον εξοπλισμό και τις λειτουργίες δικτύου τρίτων μερών·
5. ικανότητα παροχής αναβαθμίσεων και εξατομικεύσεων·
6. διαδικασία διαχείρισης τρωτών σημείων, δημοσιοποίησή τους και επικαιροποιημένη διαδικασία με ενημερώσεις και διορθώσεις·
7. διαθεσιμότητα και διαφάνεια της τεκμηρίωσης σχετικά με τα εξής:
   - τις βασικές λειτουργίες και πληροφορίες σχετικά με την ασφάλεια και άλλα χαρακτηριστικά του συστατικού στοιχείου και πιθανές ρυθμίσεις, και
   - το λογισμικό που χρησιμοποιείται, συμπεριλαμβανομένου του κώδικα ανοικτής πηγής (κατάλογος υλικών — SBOM)·
8. επίπεδο εξάρτησης από υπηρεσίες υποστήριξης τρίτου επιπέδου για τη διαχείριση και τη συντήρηση του εξοπλισμού, εάν ο φορέας εκμετάλλευσης δεν εκτελεί τις υπηρεσίες αυτές μόνο με τους υπαλλήλους του·
9. προκαταρκτική αξιολόγηση της συμμόρφωσης εξοπλισμού ή οντότητας που θα παρέχει υπηρεσία υποστήριξης τρίτου επιπέδου από φορείς διαπιστευμένους στην Ευρωπαϊκή Ένωση σύμφωνα με τα ευρωπαϊκά σχέδια πιστοποίησης της κυβερνοασφάλειας, βάσει των οποίων οι διαπιστευμένοι οργανισμοί δημοσιεύονται στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

(3) Ο φορέας εκμετάλλευσης τεκμηριώνει τους παράγοντες κινδύνου και τα αποτελέσματα της εκτίμησης κινδύνου για κάθε επιλεγμένο κατασκευαστή ή προμηθευτή ή πάροχο υπηρεσιών τρίτου επιπέδου που αναφέρεται στις παραγράφους 2 και 3 του παρόντος άρθρου και επικαιροποιεί το εν λόγω έγγραφο τεκμηρίωσης τακτικά.

Άρθρο 5
(Γενικές κατευθυντήριες γραμμές για τη λειτουργία κρίσιμων στοιχείων δικτύου)

(1) Τα συστατικά στοιχεία των κρίσιμων στοιχείων δικτύου, η λειτουργία τους και οι προεπιλεγμένες ρυθμίσεις τους δεν περιέχουν τεχνικά χαρακτηριστικά που θα μπορούσαν να επηρεάσουν αρνητικά την ασφάλεια ή τη λειτουργία κρίσιμων οντοτήτων, μεταξύ άλλων λόγω δολιοφθοράς, κατασκοπείας, κλοπής διανοητικής ιδιοκτησίας ή τρομοκρατικής ενέργειας.

(2) Τα κρίσιμα στοιχεία δικτύου βρίσκονται κατά γενικό κανόνα στη Δημοκρατία της Σλοβενίας ή, λαμβανομένων υπόψη όλων των κινδύνων για την ασφάλεια και με τη διασφάλιση μέτρων ασφάλειας υψηλού επιπέδου, και εφόσον δεν ορίζεται διαφορετικά στους εφαρμοστέους κανονισμούς, στην Ευρωπαϊκή Ένωση. Ο φορέας εκμετάλλευσης ενημερώνει τον Οργανισμό Επικοινωνιακών Δικτύων και Υπηρεσιών της Δημοκρατίας της Σλοβενίας (στο εξής: Οργανισμός) και τον φορέα που είναι αρμόδιος για την ασφάλεια των πληροφοριών σχετικά με τη σκοπούμενη μετεγκατάστασή του τουλάχιστον 30 ημέρες πριν από τη μετεγκατάσταση εκτός της Ευρωπαϊκής Ένωσης.

(3) Οι υπηρεσίες υποστήριξης τρίτου επιπέδου για κρίσιμα στοιχεία του δικτύου παρέχονται κατά γενικό κανόνα εντός της Δημοκρατίας της Σλοβενίας ή, λαμβανομένων υπόψη όλων των κινδύνων για την ασφάλεια και με τη διασφάλιση μέτρων ασφάλειας υψηλού επιπέδου, και εφόσον δεν ορίζεται διαφορετικά στους εφαρμοστέους κανονισμούς, στην Ευρωπαϊκή Ένωση. Ο φορέας εκμετάλλευσης ενημερώνει τον Οργανισμό και τον φορέα που είναι αρμόδιος για την ασφάλεια των πληροφοριών σχετικά με τη σκοπούμενη μετεγκατάσταση των υπηρεσιών υποστήριξης τρίτου επιπέδου τουλάχιστον 30 ημέρες πριν από τη μετεγκατάσταση εκτός των χωρών της Ευρωπαϊκής Ένωσης.

(4) Η υλοποίηση υπηρεσιών υποστήριξης τρίτου επιπέδου δεν θέτει σε κίνδυνο την ασφάλεια ή τη λειτουργία των υπηρεσιών κρίσιμων οντοτήτων ή την εθνική ασφάλεια.

(5) Ο φορέας εκμετάλλευσης καθιερώνει και εφαρμόζει τακτικά τη διαδικασία προσδιορισμού κρίσιμων στοιχείων δικτύου. Η διαδικασία αυτή πρέπει να πραγματοποιείται τουλάχιστον μία φορά ετησίως ή κατά την προμήθεια συστατικών στοιχείων κρίσιμων στοιχείων δικτύου.

(6) Εάν ένα μεμονωμένο συστατικό στοιχείο αποτελεί μόνο εν μέρει κρίσιμο στοιχείο δικτύου, θεωρείται ότι συνιστά μέρος κρίσιμου στοιχείου δικτύου.

(7) Ο φορέας εκμετάλλευσης τηρεί επικαιροποιημένο κατάλογο όλων των συστατικών στοιχείων των κρίσιμων στοιχείων δικτύου, των λειτουργιών, των τοποθεσιών και των διαχειριστών τους, των παρόχων υπηρεσιών υποστήριξης τρίτου επιπέδου και των κατασκευαστών ή προμηθευτών τους. Κατόπιν αιτήματος, ο κατάλογος τίθεται στη διάθεση του Οργανισμού και του φορέα που είναι αρμόδιος για την ασφάλεια των πληροφοριών.

Άρθρο 6
(Μέτρα ασφάλειας για την προμήθεια συστατικών στοιχείων κρίσιμων στοιχείων δικτύου)

(1) Ο φορέας εκμετάλλευσης γνωρίζει ολόκληρη την αλυσίδα εφοδιασμού και τους κινδύνους που συνδέονται με αυτήν, συμπεριλαμβανομένων των υπεργολάβων μεμονωμένων συστατικών στοιχείων κρίσιμων στοιχείων δικτύου, στα οποία συμπεριλαμβάνονται επίσης κλειδιά κρυπτογράφησης, UICC/eUICC και άλλα στοιχεία ασφάλειας, η παράνομη χρήση των οποίων θα μπορούσε να θέσει σε κίνδυνο την ασφάλεια κρίσιμων οντοτήτων.

(2) Ο φορέας εκμετάλλευσης διασφαλίζει ότι οι απαιτήσεις ασφάλειας μεταξύ του φορέα εκμετάλλευσης και των κατασκευαστών ή προμηθευτών συστατικών στοιχείων κρίσιμων στοιχείων δικτύου ή των παρόχων υπηρεσιών υποστήριξης τρίτου επιπέδου συμφωνούνται και τεκμηριώνονται συμβατικά και απαιτούν από τους κατασκευαστές ή τους προμηθευτές να τηρούν τα συμφωνηθέντα μέτρα ασφάλειας σε ολόκληρη την αλυσίδα εφοδιασμού.

(3) Προκειμένου να αποτραπεί εγκαίρως η εκμετάλλευση των τρωτών σημείων από κακόβουλους παράγοντες, ο φορέας εκμετάλλευσης διασφαλίζει ότι ο κατασκευαστής ή ο προμηθευτής συστατικών στοιχείων κρίσιμου στοιχείου δικτύου αναλαμβάνει συμβατικά να ενημερώνει αμέσως τον φορέα εκμετάλλευσης για τα τρωτά σημεία που εντοπίζονται και για τα μέτρα μείωσης των κινδύνων και παρέχει συμβουλές σχετικά με μέτρα προστασίας ή

αποκατάστασης, τα οποία μπορεί να λάβει ο φορέας εκμετάλλευσης για την αντιμετώπιση της απειλής.

(4) Ο φορέας εκμετάλλευσης επαληθεύει, τουλάχιστον μία φορά ετησίως, την επάρκεια των δικαιωμάτων πρόσβασης σε κρίσιμα στοιχεία δικτύου ή τα επικαιροποιεί χωρίς καθυστέρηση σύμφωνα με τις αλλαγές στην οργάνωση ή τις αλλαγές από μέρους των παρόχων υπηρεσιών υποστήριξης τρίτου επιπέδου.

(5) Ο φορέας εκμετάλλευσης αποτρέπει τη δημιουργία σχέσης εξάρτησης με μεμονωμένο προμηθευτή ή πάροχο υπηρεσιών τρίτου επιπέδου (δηλαδή «εγκλωβισμό σε συγκεκριμένο πάροχο»), όταν αυτό είναι τεχνικά εφικτό και οικονομικά βιώσιμο, με στόχο τη μείωση της εξάρτησης και την αύξηση της ανθεκτικότητας σε περίπτωση τρωτών σημείων κρίσιμων συστατικών στοιχείων, μεταξύ άλλων με την αποφυγή μακροπρόθεσμων συμβάσεων με μεμονωμένους κατασκευαστές ή προμηθευτές ή παρόχους υπηρεσιών υποστήριξης τρίτου επιπέδου, ή με τη δυνατότητα αλλαγής τους με στόχο τη μείωση των διαταραχών στην παροχή υπηρεσιών σε κρίσιμες οντότητες στο χαμηλότερο δυνατό επίπεδο.

Άρθρο 7
(Συμβατικοί όροι με κατασκευαστές, προμηθευτές ή παρόχους υπηρεσιών υποστήριξης τρίτου επιπέδου)

Προκειμένου να διασφαλιστεί υψηλό επίπεδο ασφάλειας, ο φορέας εκμετάλλευσης περιλαμβάνει τουλάχιστον τα ακόλουθα σε νέους συμβατικούς όρους με κατασκευαστές, προμηθευτές ή παρόχους υπηρεσιών υποστήριξης τρίτου επιπέδου:

1. δήλωση του κατασκευαστή ή του προμηθευτή ότι το συστατικό στοιχείο ή οι προεπιλεγμένες ρυθμίσεις του δεν έχουν μη τεκμηριωμένες κερκόπορτες ή αρνητικές επιπτώσεις στη λειτουργία των κρίσιμων οντοτήτων·
2. δέσμευση του κατασκευαστή ή του προμηθευτή ή του παρόχου υπηρεσιών τρίτου επιπέδου για την προστασία των δεδομένων των οποίων έλαβε γνώση κατά την παροχή υπηρεσιών ή την πρόσβαση σε αυτά σε σχέση με την παροχή της υπηρεσίας πρόσβασης·
3. δέσμευση του κατασκευαστή ή του προμηθευτή ή του παρόχου υπηρεσιών τρίτου επιπέδου να ενημερώσει αμέσως τον φορέα εκμετάλλευσης σε περίπτωση παραβιάσεων της προστασίας δεδομένων επικοινωνίας ή δεδομένων κίνησης που επηρεάζουν ή θα μπορούσαν να επηρεάσουν τον φορέα εκμετάλλευσης ή τις κρίσιμες οντότητες που αναφέρονται στο άρθρο 1 σημείο 1 της παρούσας γενικής πράξης·
4. δέσμευση του κατασκευαστή ή του προμηθευτή ή του παρόχου υπηρεσιών τρίτου επιπέδου να ενημερώσει αμέσως τον φορέα εκμετάλλευσης για κάθε συμβάν ασφάλειας και τρωτό σημείο που θα μπορούσε να επηρεάσει την ασφάλεια του δικτύου, των συναφών υπηρεσιών ή των δεδομένων του φορέα εκμετάλλευσης·
5. δέσμευση του κατασκευαστή ή του προμηθευτή ή του παρόχου υπηρεσιών τρίτου επιπέδου να συμμορφώνεται με τα πρότυπα και τους κανόνες ασφάλειας που καθορίζονται από τον φορέα εκμετάλλευσης και να λαμβάνει τα κατάλληλα μέτρα ασφάλειας για τη διασφάλιση της ασφάλειας των πληροφοριακών συστημάτων και δικτύων, καθώς και των δεδομένων του φορέα εκμετάλλευσης ή της κρίσιμης οντότητας·
6. ικανότητα του φορέα εκμετάλλευσης να επανεξετάζει τα περιβάλλοντα, τις διαδικασίες, τα μέτρα ασφάλειας και τα εργαλεία που χρησιμοποιεί ο πάροχος

υπηρεσιών υποστήριξης τρίτου επιπέδου κατά την πρόσβαση στο δίκτυο και στα δεδομένα του φορέα εκμετάλλευσης ανά πάσα στιγμή·

7. ευθύνη του κατασκευαστή ή του προμηθευτή ή του παρόχου υπηρεσιών υποστήριξης τρίτου επιπέδου για ζημίες που θα προέκυπταν από εντοπισθέντα τρωτά σημεία ή παράνομη χρήση συστατικών στοιχείων κρίσιμων στοιχείων του δικτύου, την προεπιλεγμένη ρύθμιση τους ή κατά την παροχή υπηρεσιών υποστήριξης τρίτου επιπέδου τις οποίες ο κατασκευαστής ή ο προμηθευτής ή ο πάροχος υπηρεσιών υποστήριξης τρίτου επιπέδου παρέλειψε ή εφάρμοσε σκόπιμα·
8. υποχρέωση τακτικής κατάρτισης του προσωπικού του κατασκευαστή ή του προμηθευτή ή του παρόχου υπηρεσιών υποστήριξης τρίτου επιπέδου στον τομέα της ασφάλειας των δεδομένων και των πληροφοριακών συστημάτων και δικτύων.

Άρθρο 8

(Κανόνες σχετικά με την πρόσβαση σε κρίσιμα στοιχεία δικτύων και τη χρήση τους)

(1) Όταν αποκτά φυσική ή λογική πρόσβαση στα συστατικά στοιχεία των κρίσιμων στοιχείων του δικτύου, στις ρυθμίσεις τους και στα δεδομένα του φορέα εκμετάλλευσης που αποθηκεύονται, υποβάλλονται σε επεξεργασία ή τροποποιούνται εντός αυτών, ο φορέας εκμετάλλευσης διασφαλίζει τα εξής:

1. ότι η πρόσβαση περιορίζεται αυστηρά σε πρόσωπα που έχουν προηγουμένως λάβει εξουσιοδότηση·
2. ότι όλες οι εργασίες σε κρίσιμα στοιχεία δικτύου που εκτελούνται επιτόπου ή μέσω απομακρυσμένης πρόσβασης ελέγχονται από τον φορέα εκμετάλλευσης·
3. ότι διενεργείται έλεγχος ταυτότητας πολλαπλών παραγόντων για χρήστες στους οποίους εκχωρούνται τα υψηλότερα προνόμια σε δικαιώματα πρόσβασης σε μεμονωμένα συστατικά στοιχεία κρίσιμων στοιχείων δικτύου, στις ρυθμίσεις τους ή στα δεδομένα που αποθηκεύονται ή υποβάλλονται σε επεξεργασία σε αυτά·
4. ότι κάθε εξουσιοδοτημένο πρόσωπο στο οποίο παρέχεται πρόσβαση διαθέτει μοναδικό λογαριασμό χρήστη και κωδικό πρόσβασης·
5. ότι χρησιμοποιούνται μόνο κωδικοί πρόσβασης που αλλάζουν τακτικά ή αμέσως σε περίπτωση εντοπισμού παράνομης χρήσης και αποτελούνται από τουλάχιστον 15 χαρακτήρες στους οποίους περιλαμβάνονται κεφαλαία και πεζά γράμματα, αριθμοί και ειδικοί χαρακτήρες, εφόσον το επιτρέπει το λογισμικό·
6. ότι η έννοια της μηδενικής ανοχής ή εμπιστοσύνης εφαρμόζεται στην πρόσβαση, όπου είναι δυνατόν·
7. ότι η ασφάλεια της σύνδεσης επικοινωνίας από τον εξουσιοδοτημένο χρήστη στα επιμέρους συστατικά στοιχεία προστατεύεται με τη χρήση κρυπτογράφησης, λαμβανομένων υπόψη των πλέον πρόσφατων τεχνολογικών εξελίξεων και των βέλτιστων βιομηχανικών ορθών πρακτικών στον τομέα της ασφάλειας των πληροφοριών, ή όπως συνιστάται από καθιερωμένα ιδρύματα στον τομέα της ασφάλειας των πληροφοριών·
8. ότι καταγράφονται σε ανεξίτηλο μέσο οι προσβάσεις και οι προσπάθειες πρόσβασης, το οποίο διατηρείται για τουλάχιστον 6 μήνες, συμπεριλαμβανομένου εφεδρικού αντιγράφου, αλλά μπορεί επίσης να διατηρηθεί για μεγαλύτερο χρονικό διάστημα, όταν η ανάλυση της διαχείρισης κινδύνου και η αξιολόγηση του αποδεκτού επιπέδου κινδύνων δείχνουν ότι οι κίνδυνοι θα πρέπει να αντιμετωπίζονται επαρκώς με την τήρηση των αρχείων καταγραφής για μεγαλύτερο χρονικό διάστημα·
9. ότι πραγματοποιείται καταγραφή και παρακολούθηση, όπου είναι δυνατόν, όλων των παρεμβάσεων λογισμικού σε συστατικά στοιχεία, συμπεριλαμβανομένων των

αλλαγών στη διαμόρφωση. Τα αρχεία, συμπεριλαμβανομένου εφεδρικού αντιγράφου των δεδομένων αυτών, φυλάσσονται για το χρονικό διάστημα που αναφέρεται στο προηγούμενο σημείο·

10. ότι η πρόσβαση σε μεμονωμένα συστατικά στοιχεία και σε δεδομένα που αποθηκεύονται ή υποβάλλονται σε επεξεργασία σε αυτά είναι χρονικά περιορισμένη και ανοικτή μόνο για τη διάρκεια των αναγκαίων εργασιών.

(2) Στην περίπτωση πρόσβασης σε μεμονωμένα συστατικά στοιχεία κρίσιμων στοιχείων δικτύου από το προσωπικό ή τους υπαλλήλους παρόχου υπηρεσιών υποστήριξης τρίτου επιπέδου, τα εν λόγω πρόσωπα:

1. χρησιμοποιούν μόνο έναν ασφαλή ενδιάμεσο ειδικό σταθμό εργασίας («jump server»), ο οποίος υπόκειται σε τακτικούς ελέγχους ασφάλειας·
2. εγκαθιστούν σε ειδικό σταθμό εργασίας μόνο τα απολύτως απαραίτητα εργαλεία, συστατικά στοιχεία και ενεργές υπηρεσίες για την πρόσβαση σε άλλους πόρους του δικτύου που είναι απολύτως απαραίτητοι και πρέπει να είναι ενημερωμένοι με τις πλέον πρόσφατες ενημερώσεις ασφάλειας·
3. χρησιμοποιούν ασφαλείς κρυπτογραφικές λειτουργίες και κλειδιά σε ειδικό σταθμό εργασίας, ο οποίος πρέπει να βρίσκεται στο δίκτυο του φορέα εκμετάλλευσης και να τελεί υπό τον αποκλειστικό του έλεγχο·
4. λαμβάνουν έγκριση για κάθε πρόσβαση από τον φορέα εκμετάλλευσης, ο οποίος την ενεργοποιεί χειροκίνητα και αποκλειστικά για τη διάρκεια της πρόσβασης·
5. όλες οι προσβάσεις και οι δραστηριότητες υποβάλλονται σε φυσικό έλεγχο και καταγράφονται από τον φορέα εκμετάλλευσης·
6. χρησιμοποιούν έλεγχο ταυτότητας δύο παραγόντων και κωδικούς πρόσβασης που έχουν μήκος τουλάχιστον 15 χαρακτήρες και περιλαμβάνουν κεφαλαία και πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες, οι οποίοι τροποποιούνται με βάση τους αξιολογούμενους κινδύνους.

(3) Προτού ο φορέας εκμετάλλευσης μεταβιβάσει την υπηρεσία διαχείρισης, συντήρησης ή ενημέρωσης κρίσιμων στοιχείων δικτύου ή των επιμέρους συστατικών τους στοιχείων σε τρίτο μέρος, επαληθεύει και διασφαλίζει ότι διαθέτει τουλάχιστον τους ίδιους ή καλύτερους μηχανισμούς ασφάλειας και διαδικασίες διαχείρισης της ασφάλειας σε σύγκριση με τους δικούς του μηχανισμούς και τις διαδικασίες. Ενημερώνει αμέσως την οικεία κρίσιμη οντότητα, τον Οργανισμό και τον φορέα που είναι αρμόδιος για την ασφάλεια των πληροφοριών σχετικά με την πρόθεση μεταβίβασης.

(4) Ο φορέας εκμετάλλευσης επαληθεύει την πραγματική κατάσταση των διαδικασιών ασφάλειας πριν από την έναρξη της παροχής υπηρεσιών και στη συνέχεια τουλάχιστον μία φορά ετησίως. Ο φορέας εκμετάλλευσης τηρεί αρχεία εσωτερικών επανεξετάσεων και ελέγχων σχετικά με την παροχή υπηρεσιών υποστήριξης από τρίτα μέρη και τα τηρεί κατά τη διάρκεια της παροχής των υπηρεσιών και για ένα έτος μετά τη λήξη τους, αλλά όχι για διάστημα μεγαλύτερο από πέντε έτη.

ΜΕΤΑΒΑΤΙΚΗ ΚΑΙ ΤΕΛΙΚΗ ΔΙΑΤΑΞΗ

Άρθρο 9
(Μεταβατικές διατάξεις)

(1) Ο φορέας εκμετάλλευσης ενημερώνει τον Οργανισμό και τον φορέα που είναι αρμόδιος για την ασφάλεια των πληροφοριών σχετικά με τις υφιστάμενες τοποθεσίες κρίσιμων στοιχείων δικτύου εντός 30 ημερών από την έναρξη ισχύος της παρούσας γενικής πράξης.

(2) Ο φορέας εκμετάλλευσης ενημερώνει τον Οργανισμό και τον φορέα που είναι αρμόδιος για την ασφάλεια των πληροφοριών σχετικά με τις υφιστάμενες τοποθεσίες υπηρεσιών υποστήριξης τρίτου επιπέδου για κρίσιμα στοιχεία δικτύου εντός 30 ημερών από την έναρξη ισχύος της παρούσας γενικής πράξης.

(3) Ο Οργανισμός δημοσιεύει για πρώτη φορά τα έγγραφα που αναφέρονται στο άρθρο 3 παράγραφος 2 της παρούσας γενικής πράξης μετά την ημερομηνία έναρξης ισχύος της.

Άρθρο 10
(Έναρξη ισχύος)

Η παρούσα γενική πράξη τίθεται σε ισχύ την τριακοστή ημέρα από τη δημοσίευσή της στην Επίσημη Εφημερίδα της Δημοκρατίας της Σλοβενίας, σύμφωνα με την οποία οι φορείς εκμετάλλευσης δύνανται να χρησιμοποιούν τον εξοπλισμό και να διατηρούν την παροχή υπηρεσιών υποστήριξης τρίτου επιπέδου μέχρι τη λήξη των προθεσμιών που ορίζονται στο άρθρο 312 παράγραφοι 2 και 3 του νόμου.

Αριθ. _____ mag. Marko Mišmaš

Λιουμπλιάνα, στις _____ διευθυντής

EVA 2023-3150-0034

ΠΡΟΤΑΣΗ

Παράρτημα

Κατάλογος κρίσιμων στοιχείων δικτύου και συναφών πληροφοριακών συστημάτων:

Κρίσιμα στοιχεία δικτύου	**Λειτουργίες του δικτύου και των πληροφοριακών συστημάτων**
Μηχανισμοί διαχείρισης συνδρομητών και κρυπτογράφησης	- Διαχείριση περιόδων λειτουργίας (φωνή και δεδομένα), - εξακρίβωση της ταυτότητας των χρηστών και του εξοπλισμού με το δίκτυο, - διαχείριση και αποθήκευση κλειδιών για την εξουσιοδότηση συνδρομητών και συστατικών στοιχείων δικτύου (UICC/eUICC, ψηφιακά πιστοποιητικά/HSM), - λειτουργίες για την ασφαλή εξακρίβωση της ταυτότητας, την προστασία της ακεραιότητας της επικοινωνίας (κρυπτογράφηση) και την αποθήκευση των κλειδιών χρήστη, των συστατικών στοιχείων δικτύου και διαχείρισης, - διαχείριση των δικαιωμάτων πρόσβασης.
Διασύνδεση	- Χαρακτηριστικά και διεπαφές φιλοξενίας σε άλλα δίκτυα και υπηρεσίες.
Διαχειριζόμενες υπηρεσίες δικτύου	- Καταχώριση και αδειοδότηση υπηρεσιών δικτύου, - αποθήκευση και επεξεργασία δεδομένων επικοινωνίας, θέσης και κίνησης, - έκθεση του δικτύου και των λειτουργιών δικτύου σε εξωτερικές εφαρμογές και υπηρεσίες.
Διαχείριση και ενορχήστρωση εικονικοποιημένων λειτουργιών δικτύου (NFV) και ενορχήστρωση δικτύου (MANO), συμπεριλαμβανομένης της υποδομής εικονικοποίησης	- Διαχειριστικές λειτουργίες ενορχήστρωσης και διαμόρφωσης της NFV ανεξάρτητα από τον τύπο υλοποίησης [VM, υποδοχέας (container), μικροϋπηρεσίες], - λειτουργίες εικονικοποίησης για την υλοποίηση και χρήση της NFV, - λειτουργία επιλογής δικτυοφέτας (NSSF).
Δίκτυο ραδιοπρόσβασης	- Σταθμοί βάσης που υποστηρίζουν τεχνολογία 5G ή υψηλότερη.
Συστήματα διαχείρισης και λοιπά συστήματα υποστήριξης	- Παρακολούθηση της λειτουργίας και της διαχείρισης του δικτύου κινητών επικοινωνιών, συμπεριλαμβανομένου του τμήματος πρόσβασης (RAN/O-RAN), - συστήματα για τον εντοπισμό συμβάντων ασφάλειας, ανωμαλιών, απειλών και για τη διαχείρισή τους (λειτουργίες ασφάλειας συμπεριλαμβανομένων των SIEM/SOAR).
Νόμιμη παρακολούθηση	- Λειτουργίες πρόσβασης στο περιεχόμενο της επικοινωνίας και στα δεδομένα σχετικά με την

	κίνηση των χρηστών από την αρμόδια αρχή.