DIGITALEUROPE

Ενσωμάτωση της οδηγίας για την ασφάλεια των δικτύων και των πληροφοριών (ΑΔΠ) στις εθνικές νομοθεσίες

Βρυξέλλες, 5 Ιούλιος 2016

ΕΚΤΕΝΗΣ ΠΕΡΙΛΗΨΗ

Το Συμβούλιο της Ευρωπαϊκής Ένωσης δημοσίευσε στις 21 Απριλίου 2016 την τελική έκδοση της οδηγίας για την ασφάλεια των δικτύων και των πληροφοριών (ΑΔΠ). Παρόλο που αυτή χρειάζεται να επικυρωθεί επισήμως από το Ευρωπαϊκό Κοινοβούλιο εντός του καλοκαιριού, το ίδιο το κείμενο αποτελεί αποτέλεσμα συμφωνίας ανάμεσα στα τρία θεσμικά όργανα της ΕΕ και δεν αναμένεται να τροποποιηθεί. Τα κράτη μέλη αναμένεται να το ενσωματώσουν στις εθνικές τους νομοθεσίες εντός 21 μηνών από την ψήφισή της. Προκειμένου να συνδράμουμε σε αυτή τη διαδικασία, επισυνάπτουμε υπό μορφή παραρτήματος τον οδηγό βέλτιστων πρακτικών για την εφαρμογή των παραμέτρων που σχετίζονται με τη βιομηχανία της τεχνολογίας και την αποτελεσματική υλοποίηση των προθέσεων των συντακτών.

Η οδηγία ΑΔΠ της ΕΕ αποτελεί το πρώτο πανευρωπαϊκό νομοθέτημα για την ασφάλεια του κυβερνοχώρου και εστιάζει στην ενδυνάμωση των αρχών καταπολέμησης του ηλεκτρονικού εγκλήματος σε εθνικό επίπεδο, ενίσχυση της μεταξύ τους συνεργασίας και καθιέρωση απαιτήσεων ασφαλείας για σημαντικούς τομείς της βιομηχανίας.

Τα εθνικά νομοθετήματα με τα οποία θα ενσωματωθεί η οδηγία θα πρέπει να λαμβάνουν υπόψη τους δύο βασικούς στόχους της οδηγίας: (1) τη διασφάλιση ασφάλειας υψηλού επιπέδου στον κυβερνοχώρο για τις σημαντικότερες υποδομές της χώρας, και (2) τη δημιουργία ενός αποτελεσματικού μηχανισμού συνεργασίας ανάμεσα στα κράτη μέλη για την προαγωγή του πρώτου στόχου. Οι διάφοροι πόροι θα πρέπει να κατανεμηθούν με κύριο γνώμονα την επίτευξη των δύο αυτών σημαντικών στόχων.

Για τη βιομηχανία της τεχνολογίας, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι διατάξεις περί των λεγόμενων παρόχων ψηφιακών υπηρεσιών (DSP). Στην οδηγία αναφέρεται ρητά ότι υπάρχουν θεμελιώδεις διαφορές ανάμεσα στους παρόχους βασικών υπηρεσιών (OES) και τους DSP. Για την ακρίβεια, οι τελευταίοι δεν θα πρέπει να θεωρείται ότι συγκαταλέγονται στις υποδομές ζωτικής σημασίας. Όπως αναγνωρίζεται στο νομοθέτημα, ένα περιστατικό το οποίο θα επηρέαζε αυτές τις ψηφιακές υπηρεσίες θα έθετε σε σημαντικά μικρότερο κίνδυνο την οικονομική και τη δημόσια ασφάλεια μιας χώρας. Η διατήρηση αυτής της διαφοράς είναι ουσιώδης για την αποτελεσματική και αποδοτική αξιοποίηση των περιορισμένων πόρων που θα έχουν στη διάθεσή τους οι αρχές για να εφαρμόσουν τους κανόνες και να επιβλέψουν την εφαρμογή τους.

Κατά συνέπεια, συνιστούμε να δώσετε μεγάλη προσοχή στο επιδιωκόμενο αντικείμενο των εν λόγω υπηρεσιών και να απευθύνετε έκκληση στους αρμόδιους για τη χάραξη πολιτικής να μην επιβάλουν απαιτήσεις ασφαλείας σε τομείς εκτός των DSP και των OES στα εθνικά τους νομοθετήματα.

Όσον αφορά τη δικαιοδοσία, οι DSPs θα πρέπει να μπορούν να βασιστούν στην ισχύουσα νομοθεσία της χώρας κύριας εγκατάστασής τους, ακόμη και σε περιπτώσεις όπου ενδέχεται να εμπλέκονται περισσότερες από μία χώρες. Ως προς την εποπτεία, οι αρμόδιες αρχές θα πρέπει να εφαρμόσουν μια προσέγγιση εποπτείας εκ των υστέρων αντί της επιβολής μιας γενικής υποχρέωσης εποπτείας των DSP. Επιπλέον, θα πρέπει να εστιάσουν στα

DIGITALEUROPE
Rue de la Science, 14 - 1040 Βρυξέλλες [Βέλγιο]
Τηλ. +32 (0) 2 609 53 10 Φαξ +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Μέλος μητρώου διαφάνειας για την Επιτροπή: 64270747023-20

αποτελέσματα και να διατηρήσουν τη διάκριση ανάμεσα στους OES και τους DSP, μέσω της μη επιβολής απαιτήσεων στους τελευταίους, οι οποίες δεν προβλέπονται από την οδηγία, π.χ. ελεγκτικές και δεσμευτικές οδηγίες.

Τα μέτρα ασφαλείας για τους DSP θα πρέπει να είναι διαφορετικά από εκείνα για τους OES, δεδομένου ότι στην οδηγία δηλώνεται πως αποτελούν σημαντικά χαμηλότερο κίνδυνο για την ασφάλεια. Οι ιθύνοντες θα πρέπει να υλοποιήσουν τον στόχο της εναρμόνισης για αυτές τις υπηρεσίες, να αναγνωρίσουν τα υπάρχοντα διεθνή πρότυπα που έχουν αναπτυχθεί από την ίδια τη βιομηχανία, να αποφύγουν τεχνολογικές απαιτήσεις και να σεβαστούν το δικαίωμα των DSP το οποίο περιλαμβάνεται στην οδηγία να ορίζουν μόνοι τους τα πιο κατάλληλα μέτρα ασφαλείας για τα συστήματά τους. Η αναφορά περιστατικών θα πρέπει, επίσης, να εναρμονιστεί σε Ευρωπαϊκό επίπεδο όσο το δυνατόν περισσότερο, να εστιάσει σε περιστατικά που επηρεάζουν τη συνέχεια παροχής της υπηρεσίας, να σέβεται την ευελιξία στους χρόνους αναφοράς και να δημιουργεί ένα περιβάλλον εμπιστοσύνης, το οποίο ενθαρρύνει την κοινή χρήση πληροφοριών χωρίς να αποδίδει εκείνον που παρέχει την αναφορά εκτεθειμένο σε αυξημένη ευθύνη

Τα μέτρα που επιβάλλονται στους OES θα έχουν, επίσης, αντίκτυπο σε άλλες βιομηχανίες, καθώς η υποχρέωση για μέτρα ασφαλείας και αναφορές περιστατικών θα αναπαράγεται σε διατάξεις συμβάσεων. Αυτό ισχύει ιδιαίτερα για υπηρεσίες υπολογιστικού νέφους (cloud). Κατά συνέπεια, οι DSP ενδέχεται να υπόκεινται έμμεσα στην εθνική νομοθεσία των πελατών τους και, επομένως, μας συμφέρει εξαιρετικά να φροντίσουμε να εφαρμοστούν διεθνώς αναγνωρισμένα μέτρα ασφαλείας σε αυτές τις υπηρεσίες. Επιπλέον, προτείνουμε όσο το δυνατόν καλύτερο συντονισμό και όσο το δυνατόν περισσότερες συνεργίες ανάμεσα στις απαιτήσεις αναφοράς τόσο για τους OES όσο και για τους DSP, δεδομένου ότι είναι πιθανό οι δεύτεροι να υπόκεινται σε διπλή υποχρέωση αναφοράς.

Στην οδηγία ορίζεται η φιλοδοξία επίτευξης ενός υψηλού κοινού επιπέδου ασφαλείας για δίκτυα και πληροφοριακά συστήματα με σκοπό τη βελτίωση της λειτουργίας της εσωτερικής αγοράς. Για να επιτευχθεί αυτός ο μεγαλόπνοος στόχος, **τα εθνικά μέτρα μεταφοράς θα πρέπει να εστιάζουν σε μια εναρμονισμένη και διεθνή προσέγγιση βάσει κινδύνου**, η οποία θα παρέχει στον ιδιωτικό τομέα την ευελιξία να προσαρμοστεί σε ένα συνεχώς μεταβαλλόμενο περιβάλλον απειλών, θα επιτρέπει στις αρχές καταπολέμησης του ηλεκτρονικού εγκλήματος να αφιερώνουν τους περιορισμένους τους πόρους στις σημαντικότερες προκλήσεις, και θα αναγνωρίζει ότι η λύση σε ένα πρόβλημα που δεν έχει σύνορα πρέπει να είναι διεθνής. Ελπίζουμε ότι αυτός ο οδηγός θα αποτελέσει χρήσιμο εργαλείο για το σκοπό αυτό και θα χαρούμε να απαντήσουμε τυχόν περαιτέρω ερωτήσεις σας.

DIGITALEUROPE
Rue de la Science, 14 - 1040 Βρυξέλλες [Βέλγιο]
Τηλ. +32 (0) 2 609 53 10 Φαξ +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Μέλος μητρώου διαφάνειας για την Επιτροπή: 64270747023-20

Παράρτημα: Οδηγός βέλτιστων πρακτικών για την εφαρμογή της οδηγίας ΑΔΠ

1. Πάροχοι ψηφιακών υπηρεσιών

a) Πεδίο εφαρμογής

- Η οδηγία ορίζει ότι οι διαδικτυακές αγορές, οι διαδικτυακές μηχανές αναζήτησης και οι υπηρεσίες υπολογιστικού νέφους θα θεωρούνται πάροχοι ψηφιακών υπηρεσιών και, συνεπώς θα ανήκουν στο πεδίο εφαρμογής της οδηγίας. Ενώ αυτή είναι μια οδηγία ελάχιστης εναρμόνισης (άρθρο 2), είναι σημαντικό να διατηρηθεί μια συνέπεια σε ολόκληρη την ΕΕ και, συνεπώς, τα κράτη μέλη δε θα πρέπει να επιβάλουν σε τομείς πέραν εκείνων που ορίζονται ως DPS ή πάροχοι βασικών υπηρεσιών (OES) -όπως ορίζονται στο άρθρο 3- απαιτήσεις ασφαλείας μέσω της εθνικής νομοθεσίας.

- Η οδηγία αναφέρει ρητώς ότι οι εταιρείες κατασκευής υλικού και ανάπτυξης λογισμικού δεν είναι OES ή DPS και επομένως δεν θα πρέπει να επηρεάζονται από τους εθνικούς νόμους με τους οποίους θα γίνεται η εφαρμογή της οδηγίας (αιτιολογική σκέψη 50).

- Η οδηγία εξαιρεί ρητώς από το πεδίο εφαρμογής των διαδικτυακών αγορών διαδικτυακές υπηρεσίες οι οποίες λειτουργούν ως μεσάζοντες για υπηρεσίες τρίτων, μεταξύ των οποίων συνάπτεται τελικά η σύμβαση παροχής υπηρεσιών (π.χ. Ιστότοπους σύγκρισης) (αιτιολογική σκέψη 15).

- Οι λειτουργίες αναζήτησης που περιορίζονται στο περιεχόμενο ενός συγκεκριμένου ιστοτόπου δεν λογίζονται ως διαδικτυακές μηχανές αναζήτησης, ακόμη κι αν χρησιμοποιούν τις υπηρεσίες εξωτερικού παρόχου (αιτιολογική σκέψη 16).

- Ο ορισμός μιας υπηρεσίας υπολογιστικού νέφους βάσει της οδηγίας εξαρτάται από το εάν γίνεται κοινή χρήση των υπολογιστικών πόρων από πολλαπλούς χρήστες (άρθρο 4(19) και αιτιολογική σκέψη 17). Δεδομένου ότι τα ιδιωτικά νέφη (σε αντίθεση με τα δημόσια νέφη) αφορούν έναν μόνο οργανισμό, δεν θα πρέπει να επηρεάζονται.

- Η οδηγία υπογραμμίζει ότι υπάρχουν θεμελιώδεις διαφορές ανάμεσα στους OES και τους DSP, για αυτόν το λόγο οι DSP υπόκεινται σε διαφορετικούς κανόνες (αιτιολογική σκέψη 57). Τέτοιες διακρίσεις θα πρέπει να διατηρούνται κατά την εφαρμογή της οδηγίας.

b) Δικαιοδοσία και Επίβλεψη

- Η δικαιοδοσία για τους DSP θα πρέπει να ανατίθεται μόνο σε ένα κράτος μέλος, συγκεκριμένα στη χώρα κύριας εγκατάστασης του παρόχου στην ΕΕ, που κατ' αρχήν αντιστοιχεί στη χώρα στην οποία έχει τα κεντρικά της γραφεία στην ΕΕ (άρθρο 18.1 και αιτιολογική σκέψη 64). Υποστηρίζουμε ότι οι DSP θα πρέπει να πάρουν οι ίδιοι αυτή την απόφαση και ότι η απόφαση θα πρέπει να υπόκειται σε επανεξέταση μόνο εάν οι αρμόδιες αρχές την αμφισβητούν στο πλαίσιο δραστηριοτήτων εποπτείας εκ των υστέρων.

- Εάν οι DSP διαθέτουν δίκτυα και πληροφοριακά συστήματα σε χώρες πέραν της χώρας κύριας εγκατάστασής τους, το άρθρο 17.3 προβλέπει τη συνεργασία των αρμόδιων αρχών. Από την οπτική γωνία των DSP, ωστόσο, είναι σημαντικό η ισχύουσα νομοθεσία να παραμείνει εκείνη της χώρας κύριας

εγκατάστασής τους και να παραμείνουν υπόλογοι μόνο στην αρμόδια αρχή αυτής της δικαιοδοσίας, η οποία θα ενεργεί ως ο συνομιλητής τους.

- Η οδηγία υπογραμμίζει ότι οι DSP υπόκεινται σε αναδρομική εποπτεία και επομένως οι αρμόδιες αρχές δεν έχουν καμία γενική υποχρέωση εποπτείας των DSP και θα πρέπει να αναλαμβάνουν δράση μόνο όταν τους παρέχονται αποδεικτικά στοιχεία. (Αριθμός 17.1 και αιτιολογική σκέψη 60). Αυτές οι διατάξεις θα πρέπει να τηρούνται κατά την εφαρμογή της οδηγίας.

- Αντίθετα με τους OES, στην περίπτωση των DSP οι αρχές μπορούν μόνο να ζητήσουν πληροφορίες και να απαιτήσουν οι DSP να επανορθώσουν για οποιαδήποτε μη συμμόρφωση. Η οδηγία καθιστά σαφές ότι οι αρχές δεν διαθέτουν ελεγκτικές εξουσίες και δεν μπορούν να εκδίδουν δεσμευτικές οδηγίες. Οι διατάξεις αυτές θα πρέπει, επίσης, να τηρούνται σε εθνικό επίπεδο.

c) Πρόσθετες απαιτήσεις

- Οι απαιτήσεις ασφάλειας και αναφοράς των DSP υπόκειται σε μέγιστη εναρμόνιση (άρθρο 16.10). Αυτό το άρθρο θα πρέπει να θεωρείται ότι ισχύει για τα προϊόντα, τις υπηρεσίες και τις λύσεις που συγκροτούν τα δίκτυά τους και τα πληροφοριακά τους συστήματα. Κατά συνέπεια, πρόσθετες διατάξεις, όπως δοκιμές προϊόντων, δεν θα πρέπει να απαιτούνται εφόσον τα προϊόντα και οι υπηρεσίες χρησιμοποιούνται σε αυτό το πλαίσιο.

d) Μέτρα και πρότυπα ασφαλείας

- Τα μέτρα ασφαλείας για τους DSP θα πρέπει να είναι λιγότερο βαριά από εκείνα για τους OES. Οι DSP θα πρέπει να είναι ελεύθεροι να ορίζουν τι είδους ασφάλεια θέλουν να εφαρμόζουν και πώς θέλουν να διασφαλίσουν ότι η προστασία του δικτύου τους και των πληροφοριακών συστημάτων τους είναι η κατάλληλη για τους κινδύνους που παρουσιάζονται (αιτιολογική σκέψη 49).

- Τα μέτρα ασφαλείας θα πρέπει να σχετίζονται με τη διαδικασία και να εστιάζουν στη διαχείριση κινδύνου. Δεν θα πρέπει να απαιτούν το σχεδιασμό, την ανάπτυξη ή την κατασκευή προϊόντων ΤΠΕ με συγκεκριμένο τρόπο (αιτιολογική σκέψη 51).

- Η οδηγία τονίζει ότι τα κράτη μέλη δεν θα επιβάλουν περαιτέρω απαιτήσεις ασφαλείας στους DSP (άρθρο 16.10).

- Ωστόσο, περιμένουμε κατευθυντήριες γραμμές από πολλούς παράγοντες. Τα κράτη μέλη θα διασφαλίσουν ότι τα μέτρα τα οποία περιγράφονται στην οδηγία έχουν υιοθετηθεί (άρθρο 16.1), ενώ μπορούν να ενθαρρύνουν τη χρήση προτύπων για την εφαρμογή τους (άρθρο 19.1) και να συζητήσουν τα πρότυπα με τους Ευρωπαϊκούς Οργανισμούς Προτύπων στην Ομάδα Συνεργασίας (άρθρο 11.3, στοιχείο η). Η ENISA θα προτείνει τα κατάλληλα πρότυπα (άρθρο 19.2), ενώ η Ευρωπαϊκή Επιτροπή είναι επιφορτισμένη με την έκδοση εκτελεστικών πράξεων για τα μέτρα ασφαλείας (άρθρο 16.8).

- Δεδομένου αυτού του βαθμού περιπλοκότητας και δεδομένων των οφελών που προκύπτουν από την εναρμόνιση, προτείνουμε η εθνική διαδικασία να συμμορφώνεται με τις εκτελεστικές πράξεις για τη συμφωνία των κατάλληλων μέτρων, τα οποία σε κάθε περίπτωση θα πρέπει να οριστικοποιηθούν εντός

ενός έτους από την έκδοση της οδηγίας. Οι ίδιες οι εκτελεστικές πράξεις δεν θα πρέπει να θίγουν την ικανότητα του DSP να ορίζει τα μέτρα ασφαλείας τα οποία είναι πιο κατάλληλα για τα συστήματά του.

- Το άρθρο περί προτύπων επιτρέπει την αναφορά σε Ευρωπαϊκά ή διεθνώς αποδεκτά πρότυπα (άρθρο 19.1). Δεδομένου του σταδίου ανάπτυξης των διεθνών προτύπων που ισχύουν σε αυτόν τον τομέα, συστήνουμε, όπου υπάρχουν κατάλληλα πρότυπα, η πιστοποίηση με βάση κάποιο εξ αυτών (π.χ. του ISO 27001) να επαρκεί για τη συμμόρφωση με τις απαιτήσεις.

- Σε κάθε περίπτωση, η πιστοποίηση σύμφωνα με τα πρότυπα θα πρέπει να είναι προαιρετική, όχι υποχρεωτική. Το άρθρο 19 τονίζει ότι η συμμόρφωση με οποιοδήποτε πρότυπο θα πρέπει μόνο να «ενθαρρύνεται», κι αυτό «χωρίς επιβολές ή διακρίσεις υπέρ της χρήσης συγκεκριμένου τύπου τεχνολογίας».

e) Αναφορά περιστατικών ασφαλείας

- Όπως συμβαίνει και με τα μέτρα ασφαλείας, πολλοί παράγοντες διαδραματίζουν ρόλο στη διαμόρφωση της διαδικασίας αναφοράς περιστατικών σύμφωνα με την οδηγία ΑΔΠ. Τα κράτη μέλη πρέπει να διασφαλίσουν ότι οι DSP θα αναφέρουν τα εν λόγω περιστατικά ασφαλείας, τα οποία επηρεάζουν σημαντικά την παροχή της υπηρεσίας (η οποία εμπίπτει στο πεδίο εφαρμογής της οδηγίας) που παρέχουν (άρθρο 16.3), ενώ η Ομάδα Συνεργασίας είναι επιφορτισμένη με την αναζήτηση μέσων αναφοράς (άρθρο 11.3, στοιχείο μ) και η Επιτροπή με την έκδοση εκτελεστικών πράξεων (άρθρα 16.8 και 9).

- Και πάλι, η σύστασή μας είναι τα εθνικά μέτρα μεταφοράς να συμμορφώνονται με τη διαδικασία που ορίζεται από τις εκτελεστικές πράξεις, από τις οποίες η εκτελεστική πράξη για το ανώτατο όριο αναφοράς θα πρέπει να εκδοθεί εντός ενός έτους από την οριστικοποίηση της οδηγίας.

- Όσον αφορά τους τύπους περιστατικών οι οποίοι θα πρέπει να αναφέρονται, οι DSP είναι επιφορτισμένοι με το καθήκον να αναφέρουν «οποιοδήποτε περιστατικό είχε σημαντικό αντίκτυπο στην παροχή της υπηρεσίας [τους]» (άρθρο 16.3). Αναφορικά με την εφαρμογή των ισοδύναμων διατάξεων για τους παρόχους υπηρεσιών τηλεπικοινωνιών βάσει του άρθρου 13α της οδηγίας πλαίσιο, πιστεύουμε ότι θα πρέπει να ερμηνευθεί έτσι ώστε να εστιάζει στη **συνέχεια (ή διαθεσιμότητα)** των παρεχόμενων υπηρεσιών. Με άλλα λόγια, θα πρέπει να αναφέρονται βλάβες οι οποίες φθάνουν ένα συγκεκριμένο ανώτατο όριο (το οποίο θα ορίζεται από τις εκτελεστικές πράξεις) σε αντίθεση με οποιονδήποτε άλλο τύπο περιστατικού ασφαλείας. Σε αυτό υπάρχει το πλεονέκτημα ότι θα δίνεται βάση στα περιστατικά που είναι περισσότερο πιθανό να επηρεάσουν την οικονομία ή την κοινωνία, ενώ θα ελαχιστοποιείται (αν και δεν θα εξαλείφεται) η αλληλοεπικάλυψη με απαιτήσεις αναφοράς παραβίασης προσωπικών δεδομένων που προκύπτει από τον γενικό κανονισμό για την προστασία των δεδομένων.

- Επιπλέον, η υποχρέωση αναφοράς των «παρόχων βασικών υπηρεσιών» ορίζει ότι αυτοί οι πάροχοι θα αναφέρουν «περιστατικά που επηρεάζουν τη συνέχεια των βασικών υπηρεσιών που παρέχουν», κάτι το οποίο και πάλι εστιάζει σαφώς στη συνέχεια (ή τη διαθεσιμότητα) των υπηρεσιών. Οι συννομοθέτες συμφώνησαν ότι οι υποχρεώσεις των DSP δεν θα είναι τόσο αυξημένες όσο των OES (βλ. αιτιολογική σκέψη 49). Η υποχρέωση των DSP να αναφέρουν περιστατικά βάσει της ΑΔΠ, επομένως, δεν θα περιλαμβάνει περισσότερα από εκείνη των OES – αντιθέτως, θα πρέπει να είναι προσαρμοσμένη

ακόμη περισσότερο σε ανώτατα όρια. Αυτό, από την άλλη, τονίζει το γεγονός ότι η αναφορά περιστατικών για DSP θα πρέπει να περιορίζεται σε περιστατικά που φτάνουν ένα συγκεκριμένο ανώτατο όριο και **επηρεάζουν τη συνέχεια/διαθεσιμότητα της υπηρεσίας** και όχι σε περιστατικά που σχετίζονται με την ακεραιότητα ή την εμπιστευτικότητα δεδομένων, η οποία σε μεγάλο βαθμό καλύπτεται ήδη από σχετικές απαιτήσεις αναφοράς βάσει του γενικού κανονισμού για την προστασία των δεδομένων και του κανονισμού για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά.

- Σχετικά με το χρόνο της αναφοράς, εκτιμούμε την ευελιξία που δίνεται μέσω της διατύπωσης για την αναφορά «χωρίς περιττή καθυστέρηση» (άρθρο 16.3). Η εφαρμογή της οδηγίας δεν θα πρέπει να περιλαμβάνει αυστηρές προθεσμίες, καθώς τα περιστατικά διαφέρουν σημαντικά ως προς την περιπλοκότητά τους. Η αυστηρότητα στους χρόνους αναφοράς θα οδηγούσε σε ανακριβείς αναφορές, όπου ο αρχικός βαθμός της επιρροής των συστημάτων δεν είναι σαφής και θα επηρέαζε αρνητικά την ικανότητα των επαγγελματιών της αντιμετώπισης περιστατικών να θέσουν ως προτεραιότητα την αντιμετώπιση του περιστατικού έναντι της αναφοράς του.

- Όπως αναλύθηκε παραπάνω, τα περιστατικά ασφαλείας που θα πρέπει να αναφέρονται βάσει της οδηγίας μπορεί επίσης να χρειάζεται να αναφερθούν βάσει της νομοθεσίας περί προστασίας δεδομένων, ανάλογα με το αν παραβιάζονται προσωπικά δεδομένα. Αυτό σημαίνει ότι όχι μόνο το ίδιο περιστατικό θα πρέπει να αναφέρεται σε διάφορες αρχές αλλά και ότι αυτές οι αρχές ενδέχεται να βρίσκονται σε διαφορετικά κράτη μέλη, ανάλογα με τη δικαιοδοσία που ισχύει για τον DSP βάσει των δύο νομοθεσιών. Συνιστούμε στα κράτη μέλη να αναγνωρίσουν την ανάγκη και να προσπαθήσουν να εξασφαλίσουν μία μόνο αναφορά περιστατικών και να δημιουργήσουν μέσα επικοινωνίας ώστε να κοινοποιούν μεταξύ τους σχετικές πληροφορίες χωρίς να θίγεται η επιχειρηματική εμπιστευτικότητα.

- Οι αρμόδιες αρχές θα πρέπει να λάβουν υπόψη τις συνέπειες για τη φήμη και την εμπορική δραστηριότητα των DSP προτού κοινοποιήσουν δημόσια πληροφορίες σχετικά με περιστατικά. Το σημαντικότερο, όμως, είναι, ότι η κοινοποίηση του περιστατικού θα μπορούσε να πολλαπλασιάσει τον κίνδυνο ασφαλείας. Για το λόγο αυτό, είναι σημαντικός ο συντονισμός μεταξύ των παραγόντων που επηρεάζονται πριν από κάθε κοινοποίηση.

- Η οδηγία τονίζει ότι πληροφορίες οι οποίες θεωρούνται εμπιστευτικές θα πρέπει να αντιμετωπίζονται ως τέτοιες (αιτιολογικές σκέψεις 41, 59, άρθρο 1.5).

- Το άρθρο 16.3 υπογραμμίζει ότι η κοινοποίηση ενός περιστατικού ασφαλείας δεν θα έχει ως αποτέλεσμα αυξημένη ευθύνη για όποιον το αναφέρει.

2. Πάροχοι βασικών υπηρεσιών

a) Μεταφορά των μέτρων ασφαλείας

- DSP που έχουν πελάτες OES θα πρέπει να εφαρμόζουν τα ισχύοντα μέτρα ασφαλείας που μεταφέρονται σε συμβατικές διαβουλεύσεις λόγω των νομικών υποχρεώσεων των παρόχων βασικών υπηρεσιών (άρθρο 14.1). Έτσι, ενδέχεται να πρέπει εμμέσως να εφαρμόζουν την εθνική νομοθεσία των πελατών τους, ανεξάρτητα από τη νομοθεσία που ισχύει στη χώρα όπου έχουν την Ευρωπαϊκή τους έδρα.

- Κατά συνέπεια, τυχόν προσπάθειες εναρμόνισης των μέτρων ασφαλείας για τους παρόχους βασικών υπηρεσιών θα ήταν ευπρόσδεκτες. Ενώ τα κράτη μέλη έχουν το δικαίωμα να επιβάλουν πιο αυστηρές υποχρεώσεις στους παρόχους βασικών υπηρεσιών από εκείνες που προβλέπονται στην οδηγία (άρθρο 3), συνιστούμε κράτει και ενθαρρύνουμε τα κράτη μέλη να συνεργαστούν για την εφαρμογή μιας εναρμονισμένης προσέγγισης. Για να επιτευχθεί αυτό, θα μπορούσαν να αποφευχθούν πρόσθετα μέτρα στα εθνικά μέτρα μεταφοράς και να γίνει προσπάθεια προσδιορισμού των απαραίτητων μέτρων ασφαλείας στην Ομάδα Συνεργασίας αντί να δοθεί έμφαση στην εθνική διαδικασία.

- Οι απαιτήσεις ασφαλείας θα πρέπει να βασίζονται όσο το δυνατόν περισσότερο σε διεθνή πρότυπα (όπως η σειρά ISO 27x) και σε αναγνωρισμένες βέλτιστες πρακτικές όσον αφορά την ασφάλεια.

- Τα μέτρα ασφαλείας που επιβάλλονται στους OES δεν θα πρέπει σε καμία περίπτωση να απαιτούν το σχεδιασμό, την ανάπτυξη ή την κατασκευή συγκεκριμένων προϊόντων ΤΠΕ με συγκεκριμένο τρόπο (αιτιολογική σκέψη 51).

b) Μεταφορά της υποχρέωσης αναφοράς περιστατικών ασφαλείας

- Οι πάροχοι βασικών υπηρεσιών υποχρεούνται να αναφέρουν περιστατικά ασφαλείας στους συμβεβλημένους με αυτούς DSP, εφόσον αυτά επηρεάζουν τη συνέχεια παροχής των βασικών τους υπηρεσιών (άρθρο 16.5). Συνεπώς, οι DSP θα υποχρεούνται βάσει σύμβασης να αναφέρουν στον εν λόγω πάροχο βασικών υπηρεσιών περιστατικά ασφαλείας τα οποία ενδέχεται να τον επηρεάσουν.

- Εκτιμούμε την ευελιξία που δίνεται μέσω της διατύπωσης για την αναφορά «χωρίς περιττή καθυστέρηση» από τους OES (άρθρο 14.3). Τα εθνικά μέτρα μεταφοράς δεν θα πρέπει να ορίζουν συγκεκριμένους χρόνους και σε κάθε περίπτωση, αν οι OES κληθούν να δικαιολογήσουν τον χρόνο που μεσολάβησε μέχρι να αναφέρουν το περιστατικό, θα πρέπει να κριθούν για το διάστημα που μεσολάβησε από τη στιγμή που το περιστατικό γνωστοποιήθηκε στον OES κι όχι από τη στιγμή που το γνώριζε ο DSP.

- Το άρθρο 14.7 προβλέπει την κατάρτιση οδηγιών από την Ομάδα Συνεργασίας σχετικά με τις συνθήκες που θα πρέπει να συντρέχουν για την αναφορά, ενώ αντίθετα η Επιτροπή θα διαδραματίσει εναρμονιστικό ρόλο όσον αφορά τις αναφορές από τον DSP. Δεδομένης της διπλής απαίτησης αναφοράς εκ μέρους των DSP, είναι σημαντικό οι αντίστοιχες απαιτήσεις αναφοράς να μην έρχονται σε αντίθεση η μία με την άλλη αλλά, στο βαθμό του δυνατού, σε συμφωνία. Συνεπώς, αυτή η διαδικασία θα πρέπει να ελεγχθεί ώστε να συμβαίνει αυτό. Επιπλέον, οι απαιτήσεις αναφοράς για τους DSP θα πρέπει να σέβονται τις υποχρεώσεις εμπιστευτικότητας που έχουν εκείνοι απέναντι στους OES πελάτες τους και όχι να απαιτούν την κοινοποίηση εμπορικά εμπιστευτικών πληροφοριών.

Η DIGITALEUROPE

Η DIGITALEUROPE εκπροσωπεί τη βιομηχανία της τεχνολογίας στην Ευρώπη. Στα μέλη μας συγκαταλέγονται κάποιες από τις μεγαλύτερες παγκοσμίως εταιρείες πληροφορικής, τηλεπικοινωνιών και καταναλωτικών ηλεκτρονικών αγαθών, καθώς και εθνικές εμπορικές ενώσεις από κάθε μέρος της Ευρώπης. Επιθυμία της DIGITALEUROPE είναι οι Ευρωπαϊκές επιχειρήσεις και οι Ευρωπαίοι πολίτες να ωφελούνται πλήρως από τις ψηφιακές τεχνολογίες και η Ευρώπη να αποτελέσει έδαφος για την ανάπτυξη, την προσέλκυση και την διατήρηση των καλύτερων εταιρειών ψηφιακής τεχνολογίας του πλανήτη.

Η DIGITALEUROPE εξασφαλίζει τη συμμετοχή της βιομηχανίας στη χάραξη και την εφαρμογή των πολιτικών της ΕΕ. Την DIGITALEUROPE αποτελούν 62 εταιρικά μέλη και 37 εθνικές εμπορικές ενώσεις από όλη την Ευρώπη. Στον ιστότοπό μας θα βρείτε περισσότερες πληροφορίες για τα τελευταία μας νέα και τις δραστηριότητές μας: http://www.digitaleurope.org

ΜΕΛΗ ΤΗΣ DIGITALEUROPE

Εταιρικά μέλη

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Ingram Micro, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies, ZTE Corporation.

Εθνικές κλαδικές ενώσεις

Αυστρία: IOÖ
Λευκορωσία: INFOPARK
Βέλγιο: AGORIA
Βουλγαρία: BAIT
Κύπρος: CITEA
Δανία: DI Digital, IT-BRANCHEN
Εσθονία: ITL
Φινλανδία: FFTI
Γαλλία: AFNUM, Force Numérique, Tech in France
Γερμανία: BITKOM, ZVEI
Ελλάδα: ΣΕΠΕ
Ουγγαρία: IVSZ
Ιρλανδία: ICT IRELAND
Ιταλία: ANITEC
Λιθουανία: INFOBALT
Κάτω Χώρες: Nederland ICT, FIAR
Πολωνία: KIGEIT, PIIT, ZIPSEE
Πορτογαλία: AGEFE
Ρουμανία: ANIS, APDETIC
Σλοβακία: ITAS
Σλοβενία: GZS
Ισπανία: AMETIC
Σουηδία: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Ελβετία: SWICO
Τουρκία: Digital Turkey Platform, ECID
Ουκρανία: IT UKRAINE
Ηνωμένο Βασίλειο: techUK