ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2017/2288 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 11ης Δεκεμβρίου 2017

για την ταυτοποίηση των τεχνικών προδιαγραφών ΤΠΕ που θα χρησιμοποιούνται ως προδιαγραφές αναφοράς στις δημόσιες συμβάσεις

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2012, σχετικά με την ευρωπαϊκή τυποποίηση, την τροποποίηση των οδηγιών 89/686/ΕΟΚ και 93/15/ΕΟΚ του Συμβουλίου και των οδηγιών 94/9/ΕΚ, 94/25/ΕΚ, 95/16/ΕΚ, 97/23/ΕΚ, 98/34/ΕΚ, 2004/22/ΕΚ, 2007/23/ΕΚ, 2009/23/ΕΚ και 2009/105/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της απόφασης 87/95/ΕΟΚ του Συμβουλίου και της απόφασης αριθ. 1673/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([1]) και ιδίως το άρθρο 13 παράγραφος 1,

Έπειτα από διαβούλευση με την ευρωπαϊκή πολυμερή πλατφόρμα φορέων για την τυποποίηση των ΤΠΕ και με τους εμπειρογνώμονες του κλάδου,

Εκτιμώντας τα ακόλουθα:

(1) Η τυποποίηση διαδραματίζει σημαντικό ρόλο στην υποστήριξη της στρατηγικής «Ευρώπη 2020» ([2]). Πολλές εμβληματικές πρωτοβουλίες της στρατηγικής «Ευρώπη 2020» υπογραμμίζουν τη σημασία της εθελοντικής τυποποίησης σε αγορές προϊόντων ή υπηρεσιών, ώστε να εξασφαλίζεται η συμβατότητα και η διαλειτουργικότητα μεταξύ προϊόντων και υπηρεσιών, να προωθείται η τεχνολογική ανάπτυξη και να υποστηρίζεται η καινοτομία.

(2) Τα πρότυπα είναι σημαντικά για την ευρωπαϊκή ανταγωνιστικότητα και καθοριστικά για την καινοτομία και την πρόοδο. Οι ανακοινώσεις της Επιτροπής σχετικά με την ενιαία αγορά ([3]) και την ψηφιακή ενιαία αγορά ([4]) επιβεβαιώνουν τη σημασία των κοινών προτύπων για τη διασφάλιση της απαραίτητης διαλειτουργικότητας των δικτύων και των συστημάτων στην ευρωπαϊκή ψηφιακή οικονομία. Αυτό ενισχύεται με την έκδοση της ανακοίνωσης για τις προτεραιότητες τυποποίησης στον τομέα των ΤΠΕ ([5]), στην οποία η Επιτροπή προσδιορίζει τις τεχνολογίες ΤΠΕ προτεραιότητας για τις οποίες η τυποποίηση θεωρείται κομβικής σημασίας για την ολοκλήρωση της ψηφιακής ενιαίας αγοράς.

(3) Η ανακοίνωση της Επιτροπής με τίτλο «Ένα στρατηγικό όραμα για τα ευρωπαϊκά πρότυπα: προχωρώντας προς τα εμπρός για την ενίσχυση και την επιτάχυνση της βιώσιμης ανάπτυξης της ευρωπαϊκής οικονομίας έως το 2020» ([6]) αναγνώρισε την ιδιαιτερότητα της τυποποίησης στον τομέα των τεχνολογιών των πληροφοριών και των επικοινωνιών (ΤΠΕ), στο πλαίσιο της οποίας συχνά αναπτύσσονται λύσεις, εφαρμογές και υπηρεσίες από παγκόσμια φόρουμ και κοινοπραξίες για τις ΤΠΕ που σήμερα αποτελούν ηγετικούς οργανισμούς ανάπτυξης προτύπων ΤΠΕ.

(4) Ο κανονισμός (ΕΕ) αριθ. 1025/2012 σχετικά με την ευρωπαϊκή τυποποίηση θέσπισε ένα σύστημα βάσει του οποίου η Επιτροπή μπορεί να αποφασίσει να αναγνωρίσει τις σχετικότερες και ευρύτερα αποδεκτές τεχνικές προδιαγραφές των ΤΠΕ που έχουν εκδοθεί από οργανισμούς που δεν είναι ευρωπαϊκοί, διεθνείς ή εθνικοί οργανισμοί τυποποίησης, οι οποίες μπορούν στη συνέχεια να χρησιμοποιηθούν ως προδιαγραφές αναφοράς κυρίως για να εξασφαλιστεί διαλειτουργικότητα στις δημόσιες συμβάσεις. Η δυνατότητα χρήσης του πλήρους φάσματος των τεχνικών προδιαγραφών των ΤΠΕ κατά την προμήθεια υλισμικού, λογισμικού και υπηρεσιών τεχνολογίας των πληροφοριών θα καταστήσει δυνατή τη διαλειτουργικότητα μεταξύ συσκευών, υπηρεσιών και εφαρμογών, θα βοηθήσει τις δημόσιες διοικήσεις να αποφεύγουν εγκλωβισμούς που προκύπτουν όταν ο αγοραστής - δημόσιος φορέας δεν μπορεί να αλλάξει τον πάροχο υπηρεσιών μετά τη λήξη της σύμβασης λόγω της χρήσης ιδιοταγών λύσεων ΤΠΕ και θα ενθαρρύνει τον ανταγωνισμό στον τομέα της προμήθειας διαλειτουργικών λύσεων ΤΠΕ.

(5) Για να είναι οι τεχνικές προδιαγραφές των ΤΠΕ επιλέξιμες για αναφορά στις δημόσιες συμβάσεις, πρέπει να συμμορφώνονται με τις απαιτήσεις που ορίζονται στο παράρτημα ΙΙ του κανονισμού (ΕΕ) αριθ. 1025/2012. Η συμμόρφωση με τις απαιτήσεις αυτές εξασφαλίζει για τις δημόσιες αρχές ότι οι τεχνικές προδιαγραφές των ΤΠΕ καθορίζονται σύμφωνα με τις αρχές των ανοιχτών διαδικασιών, της διαφάνειας, της αμεροληψίας και της συναίνεσης που αναγνωρίζονται από τον Παγκόσμιο Οργανισμό Εμπορίου (ΠΟΕ) στον τομέα της τυποποίησης.

([1]) ΕΕ L 316 της 14.11.2012, σ. 12.
([2]) Ανακοίνωση της Επιτροπής με τίτλο «Ευρώπη 2020 — Στρατηγική για έξυπνη, διατηρήσιμη και χωρίς αποκλεισμούς ανάπτυξη», COM(2010) 2020 τελικό, της 3ης Μαρτίου 2010.
([3]) Ανακοίνωση της Επιτροπής με τίτλο «Αναβάθμιση της ενιαίας αγοράς: περισσότερες ευκαιρίες για τους πολίτες και τις επιχειρήσεις», COM(2015) 550 final, της 28ης Οκτωβρίου 2015.
([4]) Ανακοίνωση με τίτλο «Στρατηγική για την ψηφιακή ενιαία αγορά της Ευρώπης», COM(2015) 192 final, της 6ης Μαΐου 2015.
([5]) COM(2016) 176 final, της 19ης Απριλίου 2016.
([6]) COM(2011) 311 τελικό, της 1ης Ιουνίου 2011.

(6) Η απόφαση για την ταυτοποίηση των προδιαγραφών των ΤΠΕ πρόκειται να εκδοθεί ύστερα από διαβούλευση με την ευρωπαϊκή πολυμερή πλατφόρμα φορέων για την τυποποίηση των ΤΠΕ η οποία συγκροτήθηκε με την απόφαση 2011/C 349/04 της Επιτροπής ([1]), όπως συμπληρώνεται από άλλες μορφές διαβούλευσης με εμπειρογνώμονες του κλάδου.

(7) Η ευρωπαϊκή πολυμερής πλατφόρμα φορέων για την τυποποίηση των ΤΠΕ αξιολόγησε τις ακόλουθες τεχνικές προδιαγραφές και εξέδωσε θετική γνώμη σχετικά με την ταυτοποίησή τους ως προδιαγραφών αναφοράς για τις δημόσιες συμβάσεις: «SPF-Sender Policy Framework for Authorizing Use of Domains in Email» («SPF»), «STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security (»STARTTLS-SMTP«)» και «DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (»DANE- SMTP«)», που ανέπτυξε η Ομάδα Μελέτης του Διαδικτύου (IETF)· «Structured Threat Information Expression (»STIX 1.2«)» και «Trusted Automated Exchange of Indicator Information (»TAXII 1.1«)», τις οποίες ανέπτυξε ο Οργανισμός για την Προώθηση των Δομημένων Συστημάτων Πληροφοριών («OASIS»). Η αξιολόγηση και η γνώμη της πλατφόρμας φορέων υποβλήθηκε στη συνέχεια σε διαβούλευση με τομεακούς εμπειρογνώμονες, οι οποίοι επιβεβαίωσαν τη θετική γνώμη σχετικά με την ταυτοποίηση των προαναφερόμενων προδιαγραφών.

(8) Η τεχνική προδιαγραφή «SPF» που ανέπτυξε η IETF είναι ένα ανοικτό πρότυπο που καθορίζει μια τεχνική μέθοδο για να ανιχνεύεται η παραποίηση της διεύθυνσης του αποστολέα. Η SPF προσφέρει την επιλογή ελέγχου ενός ηλεκτρονικού μηνύματος ώστε να εξακριβώνεται αν έχει αποσταλεί από εξυπηρετητή που έχει το δικαίωμα αποστολής του. Συνίσταται σε ένα απλό σύστημα επικύρωσης ηλεκτρονικών μηνυμάτων που έχει σχεδιαστεί έτσι ώστε να ανιχνεύει την παραποίηση δεδομένων χάρη σε έναν μηχανισμό που επιτρέπει στα συστήματα ανταλλαγής εισερχόμενων μηνυμάτων να ελέγχουν ότι τα εν λόγω μηνύματα από έναν τομέα προέρχονται όντως από έναν κεντρικό υπολογιστή ο οποίος έχει λάβει τη σχετική έγκριση από τους διαχειριστές του εν λόγω τομέα. Σκοπός της SPF είναι η πρόληψη των ανεπιθύμητων ηλεκτρονικών μηνυμάτων από πλαστές διευθύνσεις παραλήπτη σε έναν συγκεκριμένο τομέα. Οι παραλήπτες μπορούν να καταφύγουν σε ένα αρχείο SPF για να κρίνουν αν ένα μήνυμα που υποτίθεται ότι έρχεται από τον εν λόγω τομέα προέρχεται όντως από έναν εγκεκριμένο εξυπηρετητή ηλεκτρονικού ταχυδρομείου.

(9) Η «STARTTLS-SMTP», την οποία ανέπτυξε η IETF, είναι ένας τρόπος ώστε μια υπάρχουσα μη ασφαλής σύνδεση να αναβαθμιστεί σε ασφαλή. Η STARTTLS αποτελεί επέκταση της υπηρεσίας πρωτοκόλλου μεταφοράς απλού ταχυδρομείου («SMTP») που επιτρέπει σε έναν εξυπηρετητή και πελάτη SMTP να χρησιμοποιεί το πρωτόκολλο ασφάλειας επιπέδου μεταφοράς («TLS») για να εξασφαλίζει ιδιωτική επικοινωνία με επαλήθευση ταυτότητας στο διαδίκτυο. Η μη ασφαλής επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου αποτελεί, ιδιαίτερα, ένα μέσο σοβαρών επιθέσεων με σκοπό την παραβίαση των κρατικών δικτύων. Εάν ένας χρήστης στείλει ένα ηλεκτρονικό μήνυμα, ο εξυπηρετητής μηνυμάτων του παρόχου μηνυμάτων του χρήστη θα στείλει το μήνυμα αυτό στον εξυπηρετητή ηλεκτρονικού ταχυδρομείου του παραλήπτη. Η σύνδεση μεταξύ αυτών των εξυπηρετητών ταχυδρομείου μπορεί να προστατευτεί εκ των προτέρων με το πρωτόκολλο TLS. Η STARTTLS δίνει τη δυνατότητα να αναβαθμιστεί μια μη κρυπτογραφημένη (απλού κειμένου) σύνδεση σε κρυπτογραφημένη σύνδεση TLS.

(10) Η «DANE-SMTP», την οποία ανέπτυξε η IETF, αποτελεί μια σειρά πρωτοκόλλων για τη βελτίωση της ασφάλειας στο διαδίκτυο, καθώς επιτρέπει την εγκατάσταση κλειδιών στο σύστημα ονομάτων τομέα («DNS») τα οποία προστατεύονται με τη DNSSEC («DNS Security»). Κατά τη δημιουργία ασφαλούς σύνδεσης με ένα άγνωστο μέρος είναι επιθυμητό να γίνεται ένας ηλεκτρονικός έλεγχος της γνησιότητας του μέρους αποστολής και του προορισμού. Αυτό μπορεί να γίνει με πιστοποιητικά που εκδίδονται από τις αρχές έκδοσης («CAs») εντός του συστήματος PKI ή με αυθυπόγραφα πιστοποιητικά. Η DANE επιτρέπει στον κάτοχο ενός τομέα («καταχωρών») να παράσχει πρόσθετες πληροφορίες πέραν από τα ηλεκτρονικά πιστοποιητικά μέσω του αρχείου DNS που προστατεύεται μέσω DNSSEC. Η DANE είναι, κατά συνέπεια, ιδιαίτερα σημαντική για την καταπολέμηση επαναλαμβανόμενων επιθέσεων.

(11) Η «STIX 1.2», την οποία ανέπτυξε η OASIS, είναι μια γλώσσα για την περιγραφή των πληροφοριών για κυβερνοαπειλές με τυποποιημένο και διαρθρωμένο τρόπο. Καλύπτει σημαντικά θέματα όσον αφορά τα δεδομένα για τις κυβερνοαπειλές, διευκολύνοντας την ανάλυση και την ανταλλαγή πληροφοριών σχετικά με τις επιθέσεις. Χαρακτηρίζει μια εκτεταμένη δέσμη πληροφοριών για τις κυβερνοαπειλές, συμπεριλαμβανομένων των δεικτών αντίπαλης δραστηριότητας, όπως είναι οι διευθύνσεις IP και οι κατακερματισμοί αρχείων, καθώς και οι πληροφορίες με βάση το περιεχόμενο όσον αφορά τις απειλές, όπως είναι οι αντίπαλες τακτικές, τεχνικές και διαδικασίες («TTPs»)· οι στόχοι εκμετάλλευσης· οι εκστρατείες και τα προγράμματα δράσης («COA»). Στο σύνολό τους όλες αυτές οι πληροφορίες περιγράφουν με ολοκληρωμένο τρόπο τα κίνητρα, τις ικανότητες και τις δραστηριότητες των κυβερνοαντιπάλων και με τον τρόπο αυτό συμβάλλουν στην άμυνα κατά των επιθέσεων.

(12) Η τεχνική προδιαγραφή «TAXII v1.1», την οποία επίσης ανέπτυξε η OASIS, τυποποιεί την έμπιστη, αυτοματοποιημένη ανταλλαγή πληροφοριών για τις κυβερνοαπειλές. Η TAXII ορίζει τις υπηρεσίες και τις ανταλλαγές μηνυμάτων με σκοπό την κατανομή των πληροφοριών για τις κυβερνοαπειλές που επιτρέπουν την ανάληψη δράσης πέρα από τα όρια οργανισμών, προϊόντων ή υπηρεσιών με σκοπό την ανίχνευση, την πρόληψη και την αντιμετώπιση των κυβερνοαπειλών. Η TAXII δίνει σε οργανισμούς τη δυνατότητα να αυξήσουν τις γνώσεις τους για την κατάσταση των αναδυόμενων απειλών και να μοιράζονται εύκολα τις πληροφορίες με τους εταίρους τους διατηρώντας παράλληλα τον έλεγχο των υφιστάμενων σχέσεων και συστημάτων,

([1]) Απόφαση 2011/C 349/04 της Επιτροπής, της 28ης Νοεμβρίου 2011, σχετικά με τη σύσταση της ευρωπαϊκής πολυμερούς πλατφόρμας φορέων για την τυποποίηση των ΤΠΕ (ΕΕ C 349 της 30.11.2011, σ. 4).

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Οι τεχνικές προδιαγραφές που αναφέρονται στο παράρτημα είναι επιλέξιμες για χρήση ως προδιαγραφές αναφοράς στην ανάθεση δημόσιων συμβάσεων.

Άρθρο 2

Η παρούσα απόφαση αρχίζει να ισχύει την εικοστή ημέρα από τη δημοσίευσή της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Βρυξέλλες, 11 Δεκεμβρίου 2017.

Για την Επιτροπή
Ο Πρόεδρος
Jean-Claude JUNCKER

ΠΑΡΑΡΤΗΜΑ

Ομάδα Μελέτης του Διαδικτύου (Internet Engineering Task Force — IETF)

Αριθ.	Τίτλος της τεχνικής προδιαγραφής ΤΠΕ
1	SPF-Sender Policy Framework
2	STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security
3	DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (TLS)

Οργανισμός για την Προώθηση των Δομημένων Συστημάτων Πληροφοριών (OASIS)

Αριθ.	Τίτλος της τεχνικής προδιαγραφής ΤΠΕ
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information