ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΠΙΤΡΟΠΗΣ

ΣΤΗΝ ΕΙΔΙΚΗ ΕΚΘΕΣΗ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΕΛΕΓΚΤΙΚΟΥ ΣΥΝΕΔΡΙΟΥ

Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ: ο συνολικός βαθμός ετοιμότητας δεν είναι ανάλογος των απειλών

EL

EL

Περιεχόμενα

I. ΟΙ ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΕΝ ΣΥΝΤΟΜΙΑ 2

α) Γενική εισαγωγή 2

β) Η θέση της Επιτροπής σχετικά με τις βασικές παρατηρήσεις και συστάσεις του ΕΕΣ 3

γ) Συναφείς τελευταίες εξελίξεις και επόμενα βήματα 3

II. ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΙΣ ΚΥΡΙΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ ΤΟΥ ΕΕΣ 4

1. Επίπεδα ωριμότητας όσον αφορά την κυβερνοασφάλεια των EUIBA 4

2. Μηχανισμοί συνεργασίας των EUIBA 4

3. Ανταλλαγή πληροφοριών σχετικά με σημαντικά περιστατικά ή τρωτά σημεία 5

III. ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΑ ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΣΤΙΣ ΣΥΣΤΑΣΕΙΣ ΤΟΥ ΕΕΣ 6

Σύσταση 1 — Βελτίωση της ετοιμότητας όλων των EUIBA στον κυβερνοχώρο μέσω κοινών δεσμευτικών κανόνων και αυξημένων πόρων για τη CERT-EE 6

Σύσταση 2 — Ενεργή προαγωγή περαιτέρω συνεργειών μεταξύ των EUIBA σε επιλεγμένους τομείς 7

Σύσταση 3 — Αύξηση της εστίασης της CERT-EE και του ENISA στα λιγότερο ώριμα EUIBA 7

Το παρόν έγγραφο παρουσιάζει, σύμφωνα με το άρθρο 259 του δημοσιονομικού κανονισμού, τις απαντήσεις της Ευρωπαϊκής Επιτροπής στις παρατηρήσεις που διατυπώνονται σε ειδική έκθεση του Ευρωπαϊκού Ελεγκτικού Συνεδρίου και θα δημοσιευτεί ταυτόχρονα με την εν λόγω ειδική έκθεση.

I. ΟΙ ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΕΝ ΣΥΝΤΟΜΙΑ

α) Γενική εισαγωγή

Η κυβερνοασφάλεια έχει καταστεί κορυφαία πολιτική και επιχειρησιακή προτεραιότητα για την Ευρωπαϊκή Επιτροπή. Η κρίση της COVID-19 έχει εντείνει την εξάρτησή μας από τις ψηφιακές υπηρεσίες (υπολογιστικό νέφος, κινητές συσκευές, τεχνητή νοημοσύνη). Τα τελευταία δύο χρόνια, έχει παρατηρηθεί μαζική στροφή προς την εργασία από το σπίτι. Αυτό σημαίνει ότι το φαινόμενο τόσο της κυβερνοεγκληματικότητας όσο και της κυβερνοκατασκοπείας —οι δύο κύριες απειλές που αντιμετωπίζουν τα θεσμικά και λοιπά όργανα και οι οργανισμοί της Ευρωπαϊκής Ένωσης (στο εξής: EUIBA)— εξαπλώνονται επίσης σε μεγάλο βαθμό στο διαδίκτυο. Η Επιτροπή αναγνωρίζει την τάση αυτή και διαδραματίζει συνεπή και αποφασιστικό ηγετικό ρόλο στον τομέα της κυβερνοασφάλειας. Η πράξη για την κυβερνοασφάλεια τέθηκε σε ισχύ το 2019 και δυνάμει αυτής παρατάθηκε και απέκτησε μόνιμο χαρακτήρα η εντολή του ENISA. Με την εν λόγω πράξη καθιερώθηκε επίσης επίσημη συνεργασία μεταξύ του ENISA και της CERT-EE (της ομάδας αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ). Το 2020, η Επιτροπή πρότεινε την ενίσχυση της οδηγίας για την ασφάλεια των δικτύων και των πληροφοριών, για την οποία επίκειται συμφωνία των νομοθετών.

Η στρατηγική του 2020 για την κυβερνοασφάλεια περιλάμβανε επίσης τρεις δράσεις που αφορούσαν την κυβερνοασφάλεια των EUIBA. Η Επιτροπή ανακοίνωσε τη θέσπιση ενός κανονισμού σχετικά με την ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ και ενός κανονισμού σχετικά με τους κοινούς κανόνες κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ, καθώς και την πρόθεσή της να παράσχει νέα νομική βάση για τη CERT-EE με σκοπό την ενίσχυση της εντολής και της χρηματοδότησής της, ώστε να εξασφαλιστούν επαρκείς πόροι για την αντιμετώπιση των αυξανόμενων απειλών, κινδύνων και περιστατικών.

Οι εργασίες για την κατάρτιση των εν λόγω προτάσεων έχουν προχωρήσει. Μολονότι δεν έχουν εγκριθεί ακόμη από το Σώμα των επιτρόπων, αναμένεται ότι θα εγκριθούν κατά το πρώτο τρίμηνο του 2022. Στο προπαρασκευαστικό αυτό στάδιο, τα σημαντικά ζητήματα που συζητήθηκαν μεταξύ των θεσμικών οργάνων αφορούν τη νομική βάση της πρότασης, καθώς και τη δημοσιονομική ικανότητα όλων των EUIBA να ανταποκριθούν στις απαιτήσεις τόσο όσον αφορά τη χρηματοδότηση των αναγκών τους στον τομέα της κυβερνοασφάλειας όσο και την εξεύρεση των αναγκαίων πόρων για τη στήριξη της CERT-EE, του προϋπολογισμού και ιδίως των θέσεων εργασίας.

Τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ έχουν διαφορετικά επίπεδα ωριμότητας όσον αφορά τον βαθμό ετοιμότητας στον τομέα της κυβερνοασφάλειας. Αρκετά θεσμικά και άλλα όργανα και οργανισμοί της ΕΕ παρουσιάζουν υψηλές επιδόσεις όσον αφορά την κυβερνοετοιμότητα και θα πρέπει να συνεχίσουν να διαδραματίζουν ηγετικό ρόλο, προωθώντας την επίτευξη προόδου και περαιτέρω βελτιώσεων σε ολόκληρο το τοπίο της κυβερνοασφάλειας και αποτελώντας πηγή έμπνευσης. Για να επιτευχθεί μετρήσιμη πρόοδος, είναι σημαντικό να αναγνωριστούν τα διαφορετικά επίπεδα ωριμότητας μεταξύ των EUIBA και να καθοριστούν προτεραιότητες, ώστε οι δράσεις βελτίωσης να στοχεύουν αρχικά στα EUIBA των οποίων τα διαπιστωμένα κενά οδηγούν στην υψηλότερη έκθεση σε κίνδυνο.

β) Η θέση της Επιτροπής σχετικά με τις βασικές παρατηρήσεις και συστάσεις του ΕΕΣ

Η Επιτροπή εκφράζει την ικανοποίησή της για την έκθεση του ΕΕΣ σχετικά με την κυβερνοασφάλεια των EUIBA. Σημειώνει ότι η έκθεση υπογραμμίζει τη σημασία που έχουν τα κοινά νομικά πλαίσια όλων των EUIBA όσον αφορά την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια προκειμένου να αυξηθεί το συνολικό επίπεδο κυβερνοασφάλειας σε όλους τους τομείς. Η Επιτροπή επισημαίνει ότι οι κύριες παρατηρήσεις και συστάσεις του ΕΕΣ δεν αφορούν μόνο την επιχειρησιακή κυβερνοασφάλεια της ίδιας της Επιτροπής, αλλά τον ρόλο της πολιτικής της Επιτροπής στην υποβολή νομοθετικών προτάσεων για την αύξηση της κυβερνοωριμότητας των EUIBA.

Στους μελλοντικούς κανονισμούς σχετικά με την «ασφάλεια των πληροφοριών στα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ» και τους «κοινούς κανόνες κυβερνοασφάλειας για τα θεσμικά και λοιπά όργανα και τους οργανισμούς της ΕΕ» θα καθοριστούν οι κοινοί κανόνες για την επίτευξη υψηλών επιπέδων ασφάλειας των πληροφοριών και κυβερνοασφάλειας, αλλά η εφαρμογή τους, εντός του οργανωτικού και επιχειρησιακού πλαισίου κάθε EUIBA (ιδίως λαμβανομένου υπόψη του προφίλ τους όσον αφορά τις απειλές και τους κινδύνους), παραμένει υπό την αυτόνομη ευθύνη των EUIBA. Ο προτεινόμενος κανονισμός για την κυβερνοασφάλεια θα περιλαμβάνει κατάλληλους μηχανισμούς συμμόρφωσης ανάλογους προς τον στόχο και το πεδίο εφαρμογής των νέων κανόνων, με την επιφύλαξη της αυτονομίας των EUIBA.

Επί του παρόντος, η Επιτροπή προεδρεύει της υποομάδας κυβερνοασφάλειας της διοργανικής επιτροπής για τον ψηφιακό μετασχηματισμό (ICDT), της οποίας η προεδρία είναι εναλλασσόμενη (για περίοδο έως και 2 ετών). Σημειώνεται ότι δεν διατίθενται ειδικοί πόροι για τις εργασίες της υποομάδας: όλες οι δράσεις βασίζονται στις βέλτιστες προσπάθειες που καταβάλλουν οι συμμετέχοντες σε εθελοντική βάση.

Η Επιτροπή συμφωνεί με τη γενική ιδέα της ενίσχυσης των πόρων και της εντολής της CERT-ΕΕ.

Υπό το πνεύμα αυτό, η Επιτροπή συμφωνεί με τις βασικές παρατηρήσεις και συστάσεις της έκθεσης. Η θέση μας επεξηγείται λεπτομερώς στις πρόσθετες παρατηρήσεις στο τμήμα ΙΙΙ. Όσον αφορά τις συστάσεις, η Επιτροπή αποδέχεται τη σύσταση 1 στοιχεία α), β), γ), δ), ε), στ), ζ) και τη σύσταση 2 στοιχεία α), β), γ).

γ) Συναφείς τελευταίες εξελίξεις και επόμενα βήματα

Έχει ολοκληρωθεί επίσημη διαβούλευση σε επίπεδο γενικών διευθυντών των EUIBA σχετικά με τα ενοποιημένα σχέδια των δύο κανονισμών (ασφάλεια των πληροφοριών, κυβερνοασφάλεια) και επί του παρόντος αξιολογούνται οι παρατηρήσεις που ελήφθησαν πριν από την ολοκλήρωση της δέσμης μέτρων και την έγκριση από το Σώμα των επιτρόπων κατά το πρώτο τρίμηνο του 2022.

II. ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΙΣ ΚΥΡΙΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ ΤΟΥ ΕΕΣ

1. Επίπεδα ωριμότητας όσον αφορά την κυβερνοασφάλεια των EUIBA

Η Επιτροπή συμφωνεί ότι είναι σημαντικό να λαμβάνονται υπόψη οι απειλές και οι κίνδυνοι σε σχέση με το επίπεδο δαπανών των EUIBA για την κυβερνοασφάλεια.

Ομοίως, όσον αφορά την πτυχή των ανθρώπινων πόρων, η σταθερότητα του προσωπικού των EUIBA επηρεάζεται από διάφορους παράγοντες. Η αγορά προσλήψεων για εξειδικευμένους εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας είναι ολοένα και πιο πολύπλοκη. Σε πολλές περιπτώσεις, οι κανόνες για τους ανθρώπινους πόρους δεν είναι προσαρμοσμένοι στα εξειδικευμένα προφίλ (προσλήψεις, επαγγελματική εξέλιξη, κατάρτιση). Επιπλέον, η γενικευμένη πίεση που ασκείται στα επίπεδα προσωπικού των EUIBA από την αρμόδια για τον προϋπολογισμό αρχή σημαίνει ότι στους αναδυόμενους τομείς υψηλής προτεραιότητας, όπως η κυβερνοασφάλεια, εξακολουθεί να υπάρχει έλλειψη θέσεων εργασίας, ιδίως στις εσωτερικές επιχειρησιακές υπηρεσίες.

Όσον αφορά την πρόοδο στους τομείς της διακυβέρνησης και της διαχείρισης κινδύνων θα πρέπει να λαμβάνεται υπόψη το γεγονός ότι η παρακολούθηση της συμμόρφωσης μεταβαίνει τώρα από το πιλοτικό στάδιο στην πλήρη εφαρμογή. Ως εκ τούτου, είναι φυσιολογικό η κάλυψη μέχρι στιγμής να είναι αρκετά χαμηλή. Το εν λόγω έργο συμμόρφωσης αποτελεί το επόμενο στάδιο μιας μακροπρόθεσμης διαδικασίας βελτίωσης της κυβερνοωριμότητας, η οποία ξεκίνησε με τον καθορισμό κοινής μεθοδολογίας κινδύνου, την κατασκευή κοινών εργαλείων, την ανάπτυξη της διαχείρισης τρωτών σημείων και την παρακολούθηση, τον έλεγχο και την επικύρωση της απογραφής περιουσιακών στοιχείων. Έχει σημειωθεί πρόοδος στο μακροπρόθεσμο αυτό εγχείρημα, παρά την πολυπλοκότητα της βάσης περιουσιακών στοιχείων της Επιτροπής, η οποία αποτελείται από περισσότερα από 1 000 συστήματα πληροφοριών τα οποία διαχειρίζονται πάνω από 50 Γενικές Διευθύνσεις και εκτελεστικοί οργανισμοί.

2. Μηχανισμοί συνεργασίας των EUIBA

Η CERT-EE αποτελεί μεγάλη επιτυχία για την προώθηση της συνεργασίας όχι μόνο μεταξύ των EUIBA, αλλά και σε ευρωπαϊκό επίπεδο, μέσω της συμμετοχής της ως πλήρους μέλους του δικτύου CSIRT που συστάθηκε βάσει της οδηγίας NIS. Έτσι, η CERT-EE αποτελεί υποδειγματική περίπτωση του τρόπου με τον οποίο η συνεργασία και οι υπηρεσίες κυβερνοασφάλειας μπορούν να ενισχυθούν. Στις παρατηρήσεις του ΕΕΣ σχετικά με τη CERT-EE περιγράφεται με μεγάλη σαφήνεια το εξαιρετικό έργο που επιτελεί η CERT-EE για την αντιμετώπιση ενός τοπίου κυβερνοαπειλών που είναι ολοένα και πιο εχθρικό, καθώς και της χρόνιας έλλειψης πόρων.

Στο πλαίσιο της παρούσας διοργανικής ρύθμισης, οι αποκεντρωμένοι οργανισμοί και οι κοινές επιχειρήσεις της ΕΕ εκπροσωπούνται επίσημα από τον ENISA στο διοικητικό συμβούλιο της CERT-EE. Πέραν τούτου, οι απόψεις τους εκφράζονται στις συνεδριάσεις του διοικητικού συμβουλίου από εκπρόσωπο της συμβουλευτικής επιτροπής ΤΠΕ, ο οποίος επιτρέπεται να παρίσταται για να επικουρεί τον ENISA στον ρόλο του ως εκπροσώπου των οργανισμών, αλλά δεν έχει επίσημη θέση ή δικαίωμα ψήφου. Στον προτεινόμενο κανονισμό θα εξεταστεί το ζήτημα της επαρκούς εκπροσώπησης των οργανισμών στο διοικητικό συμβούλιο της CERT-EE. Με βάση τον εν λόγω κανονισμό, η σύνθεση του

διοικητικού συμβουλίου θα συμπληρωθεί με έως και τρεις εκπροσώπους που ορίζονται από το δίκτυο οργανισμών της Ένωσης (EUAN), κατόπιν πρότασης της συμβουλευτικής επιτροπής ΤΠΕ.

Η συμμετοχή στην υποομάδα κυβερνοασφάλειας της ICDT πραγματοποιείται με τον καλύτερο δυνατό τρόπο, στο επίπεδο δέσμευσης που αποφασίζει κάθε EUIBA. Οι βελτιώσεις όσον αφορά την ανταλλαγή πληροφοριών σχετικά με δημόσιες συμβάσεις αποτελούν σημαντικό θέμα στο πλαίσιο της ειδικής ομάδας 2 της υποομάδας κυβερνοασφάλειας και εξετάζονται κατά την κατάρτιση της νέας σύμβασης-πλαισίου για την κυβερνοασφάλεια.

Όσον αφορά τα κοινά εργαλεία για υπηρεσίες, όπως το ηλεκτρονικό ταχυδρομείο και οι βιντεοδιασκέψεις, υπάρχει ήδη η δυνατότητα χρήσης του συστήματος SECEM-2 που εφαρμόζει η Επιτροπή για όλα τα EUIBA για την αποστολή κρυπτογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου, ανάλογα με την αποτελεσματική διαχείριση των κλειδιών και των πιστοποιητικών κρυπτογράφησης. Επιπλέον, βρίσκεται υπό ανάπτυξη το εργαλείο SECABC για τη διευκόλυνση της αποστολής κρυπτογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου μεταξύ των θεσμικών οργάνων, στο οποίο αναμένεται να έχουν πρόσβαση όλα τα ενδιαφερόμενα EUIBA από το 2022. Υπάρχει ήδη η δυνατότητα πραγματοποίησης ασφαλών βιντεοδιασκέψεων για υπηρεσίες ανταλλαγής ευαίσθητων μη διαβαθμισμένων (SNC) πληροφοριών και μπορεί να επεκταθεί σε άλλα EUIBA σε ad hoc βάση μέσω της διαχείρισης της ταυτότητας των συμμετεχόντων στη συνεδρίαση. Η ανταλλαγή ευαίσθητων πληροφοριών θα εξεταστεί επίσης στον προτεινόμενο κανονισμό για την ασφάλεια των πληροφοριών (δηλαδή μέσω κοινής επισήμανσης και σήμανσης).

3. Ανταλλαγή πληροφοριών σχετικά με σημαντικά περιστατικά ή τρωτά σημεία

Το γεγονός ότι δεν κοινοποιούν στη CERT-EE σημαντικά περιστατικά ή τρωτά σημεία όλα τα EUIBA εξετάζεται στο σχέδιο κανονισμού για την κυβερνοασφάλεια σύμφωνα με την πρόταση της Επιτροπής στην οδηγία NIS-2[1]. Το επίπεδο εφαρμογής θα εξαρτηθεί από πρόσθετους πόρους που θα διατεθούν για τον σκοπό αυτόν από τα αυτόνομα EUIBA. Οι δυνατότητες να καταστούν υποχρεωτικές οι εν λόγω κοινοποιήσεις παραμένουν περιορισμένες, μεταξύ άλλων και στο πλαίσιο του προτεινόμενου κανονισμού, όπως προβλέπεται επί του παρόντος, λόγω της θεσμικής αυτονομίας των EUIBA. Ο προτεινόμενος κανονισμός για την κυβερνοασφάλεια θα περιλαμβάνει κατάλληλους μηχανισμούς συμμόρφωσης ανάλογους προς τον στόχο και το πεδίο εφαρμογής των νέων κανόνων, με την επιφύλαξη της αυτονομίας των EUIBA.

[1] Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση και για την κατάργηση της οδηγίας (ΕΕ) 2016/1148, COM/2020/823 final.

III. ΑΠΑΝΤΗΣΕΙΣ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΑ ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΣΤΙΣ ΣΥΣΤΑΣΕΙΣ ΤΟΥ ΕΕΣ

Σύσταση 1 — Βελτίωση της ετοιμότητας όλων των EUIBA στον κυβερνοχώρο μέσω κοινών δεσμευτικών κανόνων και αυξημένων πόρων για τη CERT-EE

Το προτεινόμενο κείμενο του κανονισμού θα περιλαμβάνει ειδικά μέτρα για την περαιτέρω αύξηση του κοινού επιπέδου κυβερνοασφάλειας. Τα εν λόγω μέτρα θα μετουσιωθούν σε σχέδια για την κυβερνοασφάλεια, τα οποία θα καθοριστούν και θα εφαρμοστούν σε επίπεδο EUIBA εντός του οικείου πλαισίου διακυβέρνησης στον τομέα της κυβερνοασφάλειας.

Η Επιτροπή αποδέχεται τη συγκεκριμένη σύσταση. Όσον αφορά τις ειδικές επιμέρους συστάσεις, η Επιτροπή επισημαίνει τα εξής:

α) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο α). Το σχέδιο κανονισμού θα περιλαμβάνει διατάξεις σχετικά με τα πλαίσια διακυβέρνησης και ελέγχου, τα οποία θα θεσπιστούν στο ανώτατο επίπεδο εκτελεστικής διοίκησης κάθε EUIBA, προκειμένου να διασφαλιστεί η αποτελεσματική και συνετή διαχείριση όλων των κινδύνων κυβερνοασφάλειας.

β) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο β). Το σχέδιο κανονισμού θα ενισχύσει την προσέγγιση βάσει κινδύνου για τη διαχείριση της κυβερνοασφάλειας και θα καταστήσει σαφές ότι οι δράσεις, τα σχέδια ασφάλειας ΤΠ και η πραγματική εφαρμογή των απαραίτητων ελέγχων θα πρέπει να ακολουθούν τις αξιολογήσεις.

γ) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο γ). Τα προγράμματα εκπαίδευσης, ευαισθητοποίησης και κατάρτισης στον τομέα της κυβερνοασφάλειας θα αναφέρονται στο σχέδιο κανονισμού ως μέρος της βάσης αναφοράς για την κυβερνοασφάλεια.

δ) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο δ). Με βάση την εμπειρία μας, μολονότι οι τακτικοί έλεγχοι και οι δοκιμές είναι καίριας σημασίας, δεν επαρκούν για να εξασφαλιστεί η επίτευξη προόδου. Ως εκ τούτου, η τακτική υποβολή εκθέσεων και η διαφάνεια είναι απαραίτητα στοιχεία για τη διακυβέρνηση στον τομέα της κυβερνοασφάλειας βάσει του στοιχείου α).

ε) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο ε). Το σχέδιο κανονισμού θα περιλαμβάνει διατάξεις σχετικά με την κοινοποίηση στη CERT-EE σημαντικών κυβερνοαπειλών, τρωτών σημείων και περιστατικών από τα EUIBA.

στ) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο στ). Η Επιτροπή συμφωνεί με την ανάγκη ενίσχυσης των πόρων της CERT-EE. Στο κείμενο του σχεδίου κανονισμού θα περιληφθούν διατάξεις σχετικά με το προσωπικό και τις χρηματοδοτικές συνεισφορές από τα EUIBA.

ζ) Η Επιτροπή αποδέχεται τη σύσταση 1 στοιχείο ζ). Ο προτεινόμενος κανονισμός θα περιλαμβάνει σχετικούς μηχανισμούς συμμόρφωσης ανάλογους προς τον στόχο και το πεδίο εφαρμογής των διατάξεων, με σεβασμό στη θεσμική αυτονομία των EUIBA. Το περιεχόμενο του μελλοντικού κανονισμού εξαρτάται από την έκβαση της νομοθετικής διαδικασίας και είναι το αποτέλεσμα της απόφασης που θα λάβει ο νομοθέτης της ΕΕ σχετικά με την πρόταση της Επιτροπής.

Σύσταση 2 — Ενεργή προαγωγή περαιτέρω συνεργειών μεταξύ των EUIBA σε επιλεγμένους τομείς

Η Επιτροπή, η οποία επί του παρόντος προεδρεύει της υποομάδας κυβερνοασφάλειας της διοργανικής επιτροπής για τον ψηφιακό μετασχηματισμό (ICDT), συμφωνεί με τις συστάσεις για την προώθηση λύσεων για τη συνεπή και ασφαλή ανταλλαγή ευαίσθητων πληροφοριών και τη συστηματική ανταλλαγή πληροφοριών σχετικά με έργα κυβερνοασφάλειας, συμβάσεις για υπηρεσίες κυβερνοασφάλειας και κοινά πλαίσια για δημόσιες συμβάσεις.

Η Επιτροπή αποδέχεται τη συγκεκριμένη σύσταση. Όσον αφορά τις ειδικές επιμέρους συστάσεις, η Επιτροπή επισημαίνει τα εξής:

α) Η Επιτροπή αποδέχεται τη σύσταση 2 στοιχείο α). Η Επιτροπή προτείνει τεχνικές πρωτοβουλίες και υπηρεσίες στην υποομάδα κυβερνοασφάλειας της ICDT με σκοπό την προώθηση και τη στήριξη κοινών εργαλείων για την ανταλλαγή ευαίσθητων πληροφοριών, ιδίως όσον αφορά υπηρεσίες, όπως το ηλεκτρονικό ταχυδρομείο και οι βιντεοδιασκέψεις. Σημειώνουμε επίσης ότι οι κοινές σημάνσεις και οι κοινοί κανόνες για τον χειρισμό ευαίσθητων μη διαβαθμισμένων πληροφοριών θα εξεταστούν στον προτεινόμενο κανονισμό για την ασφάλεια των πληροφοριών.

β) Η Επιτροπή αποδέχεται τη σύσταση 2 στοιχείο β). Οι υφιστάμενες ειδικές ομάδες στο πλαίσιο της υποομάδας κυβερνοασφάλειας της ICDT εξετάζουν το ζήτημα, το οποίο θα αναπτυχθεί περαιτέρω. Κατά την κατάρτιση της νέας σύμβασης-πλαισίου για την κυβερνοασφάλεια εξετάζονται οι βελτιώσεις όσον αφορά την ανταλλαγή πληροφοριών σχετικά με τη σύναψη δημόσιων συμβάσεων.

γ) Η Επιτροπή αποδέχεται τη σύσταση 2 στοιχείο γ). Τα EUIBA έχουν ήδη πρόσβαση σε διοργανικές συμβάσεις-πλαίσια στον τομέα των ΤΠΕ που διαχειρίζεται η Επιτροπή. Η κατάρτιση της νέας σύμβασης-πλαισίου για την κυβερνοασφάλεια θα συντονιστεί με την υποομάδα κυβερνοασφάλειας της ICDT.

Σύσταση 3 — Αύξηση της εστίασης της CERT-EE και του ENISA στα λιγότερο ώριμα EUIBA

Η παρούσα σύσταση απευθύνεται στη CERT-EE και στον ENISA.