ΓΝΩΜΗ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΚΕΝΤΡΙΚΗΣ ΤΡΑΠΕΖΑΣ

της 2ας Μαΐου 2019

σχετικά με την ασφάλεια συστημάτων δικτύου και πληροφοριών

(CON/2019/17)

Εισαγωγή και νομική βάση

Στις 4 Μαρτίου 2019 η Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ) έλαβε αίτημα της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ) της Κυπριακής Δημοκρατίας για την έκδοση γνώμης επί του σχεδίου ορισμένων νομοθετικών διατάξεων (εφεξής το «σχέδιο νομοθετικών διατάξεων») περιλαμβανόμενων σε σχέδιο νόμου σχετικά με τη σύσταση, τις αρμοδιότητες και τη λειτουργία της ΑΨΑ (εφεξής το «σχέδιο νόμου»), το οποίο θα αντικαταστήσει τον Νόμο 17(Ι) του 2018 περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών[1] (εφεξής ο «υφιστάμενος νόμος»).

Η γνωμοδοτική αρμοδιότητα της ΕΚΤ βασίζεται στα άρθρα 127 παράγραφος 4 και 282 παράγραφος 5 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης και στην τρίτη, πέμπτη και έκτη περίπτωση του άρθρου 2 παράγραφος 1 της απόφασης 98/415/ΕΚ του Συμβουλίου[2], καθώς το σχέδιο νομοθετικών διατάξεων αφορά την Κεντρική Τράπεζα της Κύπρου (ΚΤΚ), τα συστήματα πληρωμών και διακανονισμού, τους κανόνες που εφαρμόζονται σε χρηματοπιστωτικά ιδρύματα, στο βαθμό που επηρεάζουν σημαντικά τη σταθερότητα χρηματοπιστωτικών ιδρυμάτων και αγορών, και τα καθήκοντα που έχουν ανατεθεί στην ΕΚΤ όσον αφορά την προληπτική εποπτεία των πιστωτικών ιδρυμάτων κατά το άρθρο 127 παράγραφος 6 της Συνθήκης. Η παρούσα γνώμη εκδόθηκε από το διοικητικό συμβούλιο, σύμφωνα με το άρθρο 17.5 πρώτη πρόταση του εσωτερικού κανονισμού της Ευρωπαϊκής Κεντρικής Τράπεζας.

1. Σκοπός του σχεδίου νόμου και του σχεδίου νομοθετικών διατάξεων

1.1 Σκοπός του σχεδίου νόμου είναι η καλύτερη εναρμόνιση του κυπριακού νομικού πλαισίου με την οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[3]. Το σχέδιο νόμου θα αντικαταστήσει τον υφιστάμενο νόμο, με τον οποίο η εν λόγω οδηγία ενσωματώθηκε το 2018 στο εθνικό δίκαιο.

1.2 Το σχέδιο νόμου ιδρύει την ΑΨΑ, δημιουργεί την εθνική ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών και διασφαλίζει την ασφάλεια, ακεραιότητα και ανθεκτικότητα

1 Ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος του 2018 (Ν. 17(Ι)/2018).

2 Απόφαση 98/415/ΕΚ του Συμβουλίου, της 29ης Ιουνίου 1998, σχετικά με τη διαβούλευση της Ευρωπαϊκής Κεντρικής Τράπεζας με τις εθνικές αρχές για τα σχέδια νομοθετικών διατάξεων (ΕΕ L 189 της 3.7.1998, σ. 42).

3 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 (ΕΕ L 194 της 19.7.2016, σ. 1).

των δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών[4]. Στο πλαίσιο των αρμοδιοτήτων και των καθηκόντων της, η ΑΨΑ δύναται α) να εξασφαλίζει ότι οι φορείς εκμετάλλευσης βασικών υπηρεσιών και οι φορείς κρίσιμων υποδομών πληροφοριών λαμβάνουν κατάλληλα και αναλογικά τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των δικτύων και συστημάτων πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους, καθώς και κατάλληλα μέτρα για την αποτροπή και την ελαχιστοποίηση του αντικτύπου συμβάντων που επηρεάζουν την ασφάλεια των δικτύων και συστημάτων πληροφοριών που χρησιμοποιούνται για την παροχή αυτών των υπηρεσιών, β) να επιβάλλει διοικητικά πρόστιμα και άλλες κυρώσεις, γ) να αιτείται, στο πλαίσιο συγκεκριμένων δραστηριοτήτων της, την παροχή από τους φορείς εκμετάλλευσης βασικών υπηρεσιών και φορείς κρίσιμων υποδομών πληροφοριών κάθε σχετικών τεχνικών, οικονομικών και νομικών πληροφοριών, δ) να κλητεύει και να εξαναγκάζει την παρουσία μαρτύρων σε έρευνες, και ε) να διενεργεί επιτόπιες επιθεωρήσεις[5].

1.3 Το σχέδιο νόμου προβλέπει ότι σε περίπτωση που μια τομεακή πράξη της Ένωσης απαιτεί από τους φορείς εκμετάλλευσης βασικών υπηρεσιών ή τους παρόχους ψηφιακών υπηρεσιών είτε να εξασφαλίζουν την ασφάλεια των δικτύων και συστημάτων πληροφοριών τους είτε να κοινοποιούν συμβάντα, με την προϋπόθεση ότι οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που θεσπίζονται στο σχέδιο νόμου, θα εφαρμόζονται οι διατάξεις της εν λόγω τομεακής πράξης της Ένωσης όπως αυτή ισχύει στην εθνική έννομη τάξη, σύμφωνα με το άρθρο 1 παράγραφος 7 της οδηγίας (ΕΕ) 2016/1148.

1.4 Το σχέδιο νόμου δεν προσδιορίζει τους φορείς εκμετάλλευσης βασικών υπηρεσιών ή τους φορείς κρίσιμων υποδομών πληροφοριών, παρά εξουσιοδοτεί την ΑΨΑ να εκδώσει διάταγμα προς τούτο. Στο επεξηγηματικό σημείωμα που συνοδεύει το αίτημα για την έκδοση γνώμης επισημαίνεται ότι στο πλαίσιο καθορισμού των οικείων κρίσιμων υποδομών πληροφοριών θα αξιολογηθεί ο αναφερόμενος στην οδηγία (ΕΕ) 2016/1148[6] χρηματοπιστωτικός τομέας. Ως προς αυτό, σημειώνεται περαιτέρω ότι στις περιπτώσεις όπου δεν υπάρχει *lex specialis*, είναι πιθανό το σχέδιο νόμου να καλύπτει τομείς ευθύνης της ΚΤΚ, όπως τα συστήματα και τις υποδομές της ΚΤΚ, συστήματα τα οποία επιβλέπει αλλά δεν διαχειρίζεται η ΚΤΚ, καθώς και χρηματοπιστωτικά ιδρύματα εποπτευόμενα από την ΚΤΚ.

1.5 Το σχέδιο νομοθετικών διατάξεων ενισχύει τις βάσει του σχεδίου νόμου εξουσίες και καθήκοντα της ΑΨΑ όσον αφορά α) την παρακολούθηση της συμμόρφωσης με το σχέδιο νόμου, για τους σκοπούς της οποίας η ΑΨΑ εξουσιοδοτείται να ζητεί συνδρομή από πρόσωπα τα οποία υπόκεινται σε καθεστώς εποπτείας δυνάμει άλλης νομοθεσίας καθώς και από τις αντίστοιχες εποπτικές αρχές και από τις εθνικές αρχές που συνεισφέρουν στην εποπτεία όταν αυτή ασκείται από υπερεθνικές αρχές[7], και β) τη δυνατότητα να συνάπτει μνημόνια συνεργασίας με φορείς που διέπονται από το σχέδιο νόμου ή άλλες αρχές, οργανισμούς, εταιρίες ή εποπτικές αρχές που συνεργάζονται με την ΑΨΑ. Επίσης, στις περιπτώσεις όπου η ΚΤΚ έχει καθοριστεί φορέας κρίσιμων υποδομών ή άλλως

4 Το σχέδιο νόμου μεταφέρει επίσης στο εθνικό δίκαιο την οδηγία 2002/21/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία πλαίσιο) (ΕΕ L 108 της 24.4.2002, σ. 33).

5 Βλ. άρθρα 17, 19 και 20 του σχεδίου νόμου.

6 Βλ. άρθρο 4 σημείο 4 της οδηγίας (ΕΕ) 2016/1148.

7 Βλ. άρθρο 17(λδ) του σχεδίου νόμου.

πως, βάσει του σχεδίου νόμου, ο εν λόγω καθορισμός δύναται να διέπεται και από μνημόνιο συνεργασίας μεταξύ της ΑΨΑ και της ΚΤΚ. Τηρουμένου του δικαίου της Ένωσης, η παροχή πληροφοριών από την ΚΤΚ στην ΑΨΑ στο πλαίσιο της πιο πάνω συνεργασίας δεν συνιστά παραβίαση του καθήκοντος εχεμύθειας που υπέχει η ΚΤΚ.

2. Γενικές παρατηρήσεις

2.1 Η οδηγία (ΕΕ) 2016/1148 αποτελεί οδηγία ελάχιστης εναρμόνισης, όπως διαλαμβάνεται στο άρθρο 3 αυτής, υπό την έννοια ότι τα κράτη μέλη μπορούν να θεσπίζουν ή να διατηρούν διατάξεις με στόχο την επίτευξη υψηλότερου επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών από αυτό που η ίδια προβλέπει. Το σχέδιο νόμου βαίνει πέραν της οδηγίας (ΕΕ) 2016/1148 καλύπτοντας κρίσιμες υποδομές και προβλέποντας τον καθορισμό φορέων κρίσιμων υποδομών. Η παρούσα γνώμη δεν εξετάζει εάν το σχέδιο νόμου, εφόσον ψηφιστεί όπως έχει προταθεί, θα αποτελέσει αποτελεσματικό μέσο ενσωμάτωσης της οδηγίας (ΕΕ) 2016/1148 στο κυπριακό δίκαιο.

2.2 Όπως έχει επισημάνει στο παρελθόν[8], η ΕΚΤ υποστηρίζει τους σκοπούς της οδηγίας (ΕΕ) 2016/1148, ήτοι την εξασφάλιση ενός κοινού υψηλού επιπέδου ασφάλειας δικτύου και πληροφοριών (ΑΔΠ) σε ολόκληρη την Ένωση και την επίτευξη συνεκτικής προσέγγισης μεταξύ πλειόνων επιχειρηματικών τομέων και κρατών μελών σε αυτό το πεδίο. Είναι σημαντικό να διασφαλιστεί ότι η εσωτερική αγορά αποτελεί ασφαλές πεδίο επιχειρηματικής δραστηριότητας και ότι όλα τα κράτη μέλη διαθέτουν ένα ελάχιστο επίπεδο ετοιμότητας σε περίπτωση εκδήλωσης συμβάντος ασφάλειας στον κυβερνοχώρο. Ταυτόχρονα, θα πρέπει να διασφαλιστεί ότι οι διατάξεις της εθνικής νομοθεσίας που μεταφέρουν στο εθνικό δίκαιο την οδηγία (ΕΕ) 2016/1148 συνάδουν με τις αρμοδιότητες του Ευρωσυστήματος[9] (βλ. ενότητες 3 και 4) και σέβονται την αρχή της ανεξαρτησίας των κεντρικών τραπεζών που κατοχυρώνεται στο άρθρο 130 της Συνθήκης. Πράγματι, σύμφωνα και με την πρόταση της ΕΚΤ, η αιτιολογική σκέψη 14 της οδηγίας (ΕΕ) 2016/1148 αναφέρει ότι η οδηγία δεν θίγει την επίβλεψη των συστημάτων πληρωμών και διακανονισμού από το Ευρωσύστημα[10]. Εξάλλου, η ΑΔΠ αποκομίζει οφέλη από συνέργειες και οικονομίες κλίμακας. Ειδικότερα, εξειδικευμένες εθνικές ΑΨΑ δύνανται να συγκεντρώνουν σημαντικούς πόρους και εμπειρογνωμοσύνη, τα οποία μπορεί να χρησιμοποιήσει το Ευρωσύστημα στο τομέα της ΑΔΠ. Επιπλέον, η αναγνώριση ανεξαρτησίας υπέρ της ΕΚΤ και των οργάνων λήψεως αποφάσεων αυτής δεν έχει ως συνέπεια να αποσπάσει εξ ολοκλήρου το Ευρωσύστημα από την Ένωση και να το εξαιρέσει από κάθε κανόνα του δικαίου αυτής[11]. Η εφαρμογή των εθνικών μέτρων ενσωμάτωσης της οδηγίας (ΕΕ) 2016/1148 στο Ευρωσύστημα δεν αποκλείεται prima facie.

---

8 Βλ. παράγραφο 2.1 της γνώμης CON/2014/58, παράγραφο 2.1 της γνώμης CON/2017/10, παράγραφο 2.2 της γνώμης CON/2018/22 και παράγραφο 2.2 της γνώμης CON/2018/27. Όλες οι γνώμες της ΕΚΤ δημοσιεύονται στον δικτυακό της τόπο (www.ecb.europa.eu).

9 Βλ. επίσης παράγραφο 2.2 της γνώμης CON/2017/10, παράγραφο 3.1.1 της γνώμης CON/2018/22 και παράγραφο 2.2 της γνώμης CON/2014/58.

10 Βλ. παράγραφο 3.1 της γνώμης CON/2014/58 και παράγραφο 3.5 της γνώμης CON/2017/10.

11 Βλ. απόφαση του Δικαστηρίου της 10ης Ιουλίου 2003, Επιτροπή κατά ΕΚΤ, C-11/00, ECLI:EU:C:2003:395, σκέψεις 134 έως 136.

2.3 Υπό το φως των ανωτέρω, η ΕΚΤ χαιρετίζει τη θέσπιση ρυθμίσεων συνεργασίας μεταξύ της ΑΨΑ και της ΚΤΚ. Στο πλαίσιο της εν λόγω συνεργασίας, η ΕΚΤ προτείνει τη δημιουργία αποτελεσματικών μηχανισμών ανταλλαγής πληροφοριών προκειμένου η ΚΤΚ να είναι σε θέση να εκπληρώνει τα καθήκοντα που υπέχει βάσει της Συνθήκης και του εθνικού δικαίου. Οι εν λόγω ρυθμίσεις ανταλλαγής πληροφοριών θα διασφαλίζουν επίσης ότι η ΑΨΑ και η ΚΤΚ ανταλλάσσουν έγκαιρα και αποτελεσματικά πληροφορίες σχετικά με πραγματικά και δυνητικά συμβάντα ή απειλές στον κυβερνοχώρο που αφορούν τα συστήματα και τις υποδομές του χρηματοπιστωτικού τομέα και σχετικά με προγραμματισθέντα μέτρα και μέτρα που έχουν ληφθεί[12].

2.4 Επιπροσθέτως, η ΕΚΤ είναι έτοιμη να συνεργαστεί με την ΑΨΑ σε σχέση με τα συστήματα και τις υποδομές που επιβλέπει ή διαχειρίζεται το Ευρωσύστημα, όπως συστήματα, μέσα και μηχανισμούς πληρωμών, καθώς και με την προληπτική εποπτεία των πιστωτικών ιδρυμάτων, προκειμένου να διασφαλίζεται ότι καθιερώνονται και τηρούνται οι βέλτιστες πρακτικές όσον αφορά την ΑΔΠ[13]. Η ΕΚΤ έχει στο παρελθόν κάνει έκκληση για τη θέσπιση τέτοιου είδους αποτελεσματικής συνεργασίας και ρυθμίσεων ανταλλαγής πληροφοριών μεταξύ των εθνικών αρμόδιων αρχών, περιλαμβανομένης της ΑΨΑ, και των λοιπών εθνικών αρμόδιων αρχών, περιλαμβανομένων των εθνικών κεντρικών τραπεζών (ΕθνΚΤ), και, μέσω των ΕθνΚΤ, της ΕΚΤ[14]. Η ΕΚΤ προτείνει επίσης να διασφαλιστεί ότι η ΑΨΑ ανταλλάσσει μέσω της ΚΤΚ σχετικές πληροφορίες με την ΕΚΤ κατά τρόπο έγκαιρο και αποτελεσματικό εντός του πλαισίου των οικείων αρμοδιοτήτων[15].

3. Αντίκτυπος του σχεδίου νόμου στα συστήματα πληρωμών και διακανονισμού τίτλων

3.1 *Αντίκτυπος του σχεδίου νόμου στα συστημικώς σημαντικά συστήματα πληρωμών (ΣΣΣΠ)*

3.1.1 Στο πλαίσιο των καθηκόντων της όσον αφορά την επίβλεψη, η ΕΚΤ εξέδωσε τον κανονισμό (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28)[16] με βάση τα άρθρα 3.1, 22 και 34.1 πρώτη περίπτωση του καταστατικού του ΕΣΚΤ. Ο κανονισμός (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28) εφαρμόζει τις αρχές για τις υποδομές χρηματοπιστωτικών αγορών (αρχές ΥΧΑ) που εξέδωσαν η Επιτροπή Συστημάτων Πληρωμών και Διακανονισμού (Committee on Payment and Settlement Systems – CPSS) και ο Διεθνής Οργανισμός Επιτροπών Κινητών Αξιών (International Organization of Securities Commissions – IOSCO)[17] και οι οποίες είναι νομικά δεσμευτικές και καλύπτουν τόσο τα συστήματα πληρωμών μεγάλης αξίας όσο και τα συστήματα πληρωμών μικρής αξίας με συστημική σημασία τα οποία διαχειρίζεται είτε κεντρική τράπεζα του Ευρωσυστήματος είτε ιδιωτικός φορέας.

12 Βλ. παραγράφους 3.2.4 και 3.4.3 της γνώμης CON/2018/22 και παράγραφο 4.4 της γνώμης CON/2018/47.

13 Βλ. παράγραφο 6.3 της γνώμης CON/2018/22.

14 Βλ. παραγράφους 2.3 και 6.2 της γνώμης CON/2018/22.

15 Βλ. παράγραφο 4.3 της γνώμης CON/2018/27 και παράγραφο 6.2 της γνώμης CON/2018/47.

16 Κανονισμός (ΕΕ) αριθ. 795/2014 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 3ης Ιουλίου 2014, σχετικά με τις απαιτήσεις επίβλεψης για τα συστημικώς σημαντικά συστήματα πληρωμών (ΕΚΤ/2014/28) (ΕΕ L 217 της 23.7.2014, σ. 16).

17 Διαθέσιμες στον δικτυακό τόπο της Τράπεζας Διεθνών Διακανονισμών (www.bis.org).

3.1.2 Συνεπώς, τα ΣΣΣΠ υπόκεινται σε τακτική αξιολόγηση με βάση τις απαιτήσεις του κανονισμού (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28) σε σχέση με τον λειτουργικό κίνδυνο[18], πράγμα που επιτρέπει στην αρμόδια κεντρική τράπεζα του Ευρωσυστήματος, ως αρμόδια αρχή, να επαληθεύει τη συμμόρφωσή τους. Σε περιπτώσεις μη συμμόρφωσης, η αρμόδια κεντρική τράπεζα του Ευρωσυστήματος έχει την εξουσία επιβολής κυρώσεων ή διορθωτικών μέτρων προκειμένου να διασφαλίζεται η συμμόρφωση[19]. Ο τροποποιημένος κανονισμός (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28) εισήγαγε πρόσφατα σειρά νέων απαιτήσεων για τους διαχειριστές ΣΣΣΠ όσον αφορά την αντιμετώπιση νέων κινδύνων, περιλαμβανομένων και αυτών που αφορούν τη λειτουργία και την ασφάλεια, π.χ. ανθεκτικότητα όσον αφορά την ασφάλεια στον κυβερνοχώρο[20], λαμβάνοντας υπόψη, μεταξύ άλλων, τις οδηγίες για την ανθεκτικότητα όσον αφορά την ασφάλεια στον κυβερνοχώρο για τις υποδομές χρηματοπιστωτικών αγορών που δημοσιεύθηκαν το 2016 από την Επιτροπή Πληρωμών και Υποδομών της Αγοράς (Committee on Payments and Market Infrastructures – CPMI) και τον IOSCO[21].

3.1.3 Επιπροσθέτως, σύμφωνα και με τις απαιτήσεις της οδηγίας (ΕΕ) 2016/1148, ο κανονισμός (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28) παρέχει ήδη στις αρμόδιες κεντρικές τράπεζες του Ευρωσυστήματος την εξουσία να λαμβάνουν πληροφορίες όσον αφορά, μεταξύ άλλων, συμβάντα μικρής και μεγάλης κλίμακας, τη φύση και το είδος των συμβάντων, τη σοβαρότητα και τη διάρκειά τους[22]. Ο τροποποιημένος κανονισμός (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28) ενίσχυσε περαιτέρω την εξουσία των αρμόδιων κεντρικών τραπεζών του Ευρωσυστήματος να διενεργούν επιτόπιες επιθεωρήσεις και να απαιτούν την κατά ανεξάρτητο τρόπο επανεξέταση της λειτουργίας των συστημάτων και τη διενέργεια σχετικών ερευνών.[23]

3.1.4 Η ΕΚΤ αντιλαμβάνεται ότι η ΑΨΑ δύναται με διάταγμά της να περιλάβει στο πεδίο εφαρμογής του σχεδίου νόμου υπηρεσίες που παρέχονται μέσω συστημάτων πληροφοριών τα οποία διαχειρίζεται το Ευρωσύστημα ή συστημάτων πληροφοριών τα οποία διαχειρίζεται η ΚΤΚ και επιβλέπει το Ευρωσύστημα.

3.1.5 Μεταξύ των απαριθμούμενων ΣΣΣΠ, διακεκριμένο ρόλο διαδραματίζει το TARGET2, καθώς ανήκει στο Ευρωσύστημα και τελεί υπό τη διαχείρισή του, υπόκειται δε σε αυστηρή ρύθμιση και

---

18 Βλ. άρθρο 15 του κανονισμού (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28), το οποίο επιβάλλει στους διαχειριστές ΣΣΣΠ την υποχρέωση να λαμβάνουν μέτρα όπως: α) να θεσπίζουν ολοκληρωμένες πολιτικές φυσικής ασφάλειας και ασφάλειας πληροφοριών για τον επαρκή εντοπισμό, αξιολόγηση και διαχείριση όλων των πιθανών ευπαθειών και απειλών, β) να διασφαλίζουν ότι τα κρίσιμα συστήματα τεχνολογίας πληροφοριών δύνανται να επαναλειτουργήσουν εντός συγκεκριμένου χρονικού διαστήματος σε περίπτωση συμβάντος που δημιουργεί σημαντικό κίνδυνο διακοπής των εργασιών του ΣΣΣΠ κ.λπ.

19 Βλ. παράγραφο 3.4 της γνώμης CON/2017/10.

20 Βλ. άρθρο 15 παράγραφοι 1α και 4α, το οποίο επιβάλλει την υποχρέωση στους διαχειριστές ΣΣΣΠ να προβαίνουν στις ακόλουθες ενέργειες: i) να επανεξετάζουν, να επιθεωρούν και να διενεργούν δοκιμές σε συστήματα, πολιτικές λειτουργίας, διαδικασίες και ελέγχους σε περιοδική βάση και μετά από σημαντικές μεταβολές· ii) να θεσπίζουν αποτελεσματικό πλαίσιο ανθεκτικότητας όσον αφορά την ασφάλεια στον κυβερνοχώρο και να προβλέπουν αποτελεσματικά μέτρα διακυβέρνησης· iii) να προσδιορίζουν τις κρίσιμες εργασίες τους και τα περιουσιακά στοιχεία που τις στηρίζουν και να προβλέπουν κατάλληλα μέτρα με σκοπό την προστασία τους από επιθέσεις στον κυβερνοχώρο, τον εντοπισμό και την αντιμετώπιση τέτοιων επιθέσεων, καθώς και την ανάκαμψη από αυτές· iv) να ελέγχουν τακτικά τα μέτρα που έχουν θεσπιστεί· και v) να διαθέτουν υψηλό επίπεδο επίγνωσης της κατάστασης όσον αφορά τις απειλές στον κυβερνοχώρο, προβλέποντας προς τούτο και διαδικασία διαρκούς κατάρτισης.

21 Διαθέσιμες στον δικτυακό τόπο της Τράπεζας Διεθνών Διακανονισμών.

22 Βλ. άρθρο 21 παράγραφος 1α του κανονισμού (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28).

23 Βλ. άρθρο 21 παράγραφοι 1β και 1γ του κανονισμού (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28).

επίβλεψη.[24] Η ΕΚΤ αντιλαμβάνεται ότι η κυπριακή συνιστώσα του TARGET2, το TARGET2-CY, για το οποίο η ΚΤΚ ενεργεί ως διαχειριστής, θα μπορούσε ενδεχομένως να εμπίπτει στο πεδίο εφαρμογής του σχεδίου νόμου. Βάσει της απόφασης ΕΚΤ/2014/35 της Ευρωπαϊκής Κεντρικής Τράπεζας[25], το TARGET2 έχει χαρακτηριστεί ως ΣΣΣΠ και τελεί υπό την επίβλεψη της ΕΚΤ ως αρμόδιας αρχής κατά τον κανονισμό (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28).

3.1.6 Μολονότι τα ΣΣΣΠ ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής του σχεδίου νόμου, η ΕΚΤ αντιλαμβάνεται ότι το σχέδιο νόμου δεν θα πρέπει να θίγει την επίβλεψή τους, δεδομένου ότι αυτή ασκείται βάσει κανονισμών της ΕΚΤ. Όπως αναφέρεται στην παράγραφο 2.3, η ΕΚΤ προτείνει τη θέσπιση αποτελεσματικών ρυθμίσεων ανταλλαγής πληροφοριών και συνεργασίας προκειμένου να διασφαλίζεται ότι η ΑΨΑ ανταλλάσσει κατά τρόπο έγκαιρο και αποτελεσματικό πληροφορίες με την ΚΤΚ σχετικά με πραγματικά και δυνητικά συμβάντα στον κυβερνοχώρο και προγραμματισθέντα μέτρα ή μέτρα που έχουν ληφθεί και τα οποία ενδέχεται να επηρεάσουν τα ΣΣΣΠ και το TARGET2, ώστε η ΚΤΚ να είναι σε θέση να εκπληρώνει τα καθήκοντα που υπέχει βάσει της Συνθήκης και του εθνικού δικαίου. Η ΕΚΤ προτείνει επίσης τη θέσπιση αντίστοιχων ρυθμίσεων συνεργασίας και ανταλλαγής πληροφοριών μεταξύ της ΑΨΑ και της ΕΚΤ, μέσω της ΚΤΚ.

3.2 *Αντίκτυπος του σχεδίου νόμου στα μη ΣΣΣΠ*

3.2.1 Τα μη ΣΣΣΠ περιλαμβάνουν τα μη συστημικώς σημαντικά συστήματα πληρωμών μεγάλης αξίας (large-value payment systems – LVPS) και τα μη συστημικώς σημαντικά συστήματα πληρωμών μικρής αξίας (non-systematically important retail payment systems – non-SIRPS). Σύμφωνα με το αναθεωρημένο πλαίσιο επίβλεψης συστημάτων πληρωμών μικρής αξίας[26], τα non-SIRPS χωρίζονται σε δύο διαφορετικές κατηγορίες: στα συστήματα πληρωμών μικρής αξίας με εξέχουσα σημασία (prominently important retail payments systems – PIRPS) και στα λοιπά συστήματα πληρωμών μικρής αξίας (other retail payments systems – ORPS). Τα κυπριακά τοπικά συστήματα πληρωμών μικρής αξίας, ήτοι το JCC Payment Card System, το Κυπριακό Γραφείο Συμψηφισμού επιταγών και το JCC SDD, έχουν καταταχθεί είτε στην πρώτη είτε στη δεύτερη κατηγορία[27] και η ΕΚΤ αντιλαμβάνεται ότι οι υπηρεσίες τους θα μπορούσαν να περιληφθούν στον κατάλογο των βασικών υπηρεσιών βάσει του σχεδίου νόμου και ότι οι διαχειριστές των εν λόγω συστημάτων ή κάποια από τα συστήματα αυτά θα μπορούσαν να χαρακτηριστούν ως φορείς εκμετάλλευσης βασικών υπηρεσιών.

3.2.2 Σύμφωνα με το πλαίσιο πολιτικής επίβλεψης του Ευρωσυστήματος, τα μη συστημικώς σημαντικά LVPS και τα non-SIRPS πρέπει να τηρούν τις αρχές ΥΧΑ της CPSS και του IOSCO, τα δε non-SIRPS πρέπει επιπροσθέτως να τηρούν τις προσδοκίες επίβλεψης για ζεύξεις μεταξύ συστημάτων πληρωμών μικρής αξίας (Oversight expectations for links between retail payment systems –

---

24 Βλ. παράγραφο 3.1 της γνώμης CON/2018/47.

25 Απόφαση ΕΚΤ/2014/35 της Ευρωπαϊκής Κεντρικής Τράπεζας, της 13ης Αυγούστου 2014, σχετικά με τον χαρακτηρισμό του TARGET2 ως συστημικώς σημαντικού συστήματος πληρωμών σύμφωνα με τον κανονισμό (ΕΕ) αριθ. 795/2014 σχετικά με τις απαιτήσεις επίβλεψης για τα συστημικώς σημαντικά συστήματα πληρωμών (ΕΕ L 245 της 20.8.2014, σ. 5).

26 Βλ. έγγραφο του Ευρωσυστήματος με τίτλο «Revised oversight framework for retail payment systems» (Φεβρουάριος 2016), διαθέσιμο στον δικτυακό τόπο της ΕΚΤ.

27 Βλ. έγγραφο του Ευρωσυστήματος με τίτλο «Overview of payment systems», διαθέσιμο στον δικτυακό τόπο της ΕΚΤ.

OELRPS)[28]. Τόσο οι αρχές ΥΧΑ των CPSS και IOSCO όσο και οι OELRPS αποτελούν μη δεσμευτικές πράξεις (soft law instruments), υπό την έννοια ότι τα μη συστημικώς σημαντικά LVPS, PIRPS και ORPS υπόκεινται σε κανόνες επίβλεψης (οι οποίοι είναι ανάλογοι των κανόνων του κανονισμού (ΕΕ) αριθ. 795/2014 (ΕΚΤ/2014/28))· ωστόσο δεν υπάρχει, υπό τη στενή έννοια, νομοθεσία της Ένωσης η οποία να ρυθμίζει την επίβλεψη ή εποπτεία των εν λόγω συστημάτων[29]. Στην ΚΤΚ έχει χορηγηθεί αρμοδιότητα εποπτείας και επίβλεψης των μη ΣΣΣΠ κυρίως βάσει του άρθρου 48 του περί ΚΤΚ Νόμου[30], το οποίο από την άποψη αυτή δεν ενσωματώνει «νόμους» της Ένωσης κατά τα ανωτέρω περιγραφόμενα[31].

3.2.3 Το αναθεωρημένο πλαίσιο επίβλεψης συστημάτων πληρωμών μικρής αξίας διευκρινίζει ότι όλα τα συστήματα πληρωμών μικρής αξίας αποτελούν αναπόσπαστο μέρος του τομέα πληρωμών και διακανονισμού της ζώνης του ευρώ και εμπίπτουν επομένως στο πεδίο εφαρμογής της επίβλεψης. Ως εκ τούτου, το Ευρωσύστημα έχει συμφέρον να διασφαλίσει ότι το πλαίσιο και οι κανόνες επίβλεψης που εφαρμόζονται στα εν λόγω συστήματα δεν θίγονται από την ενσωμάτωση της οδηγίας (ΕΕ) 2016/1148 ή κατά τη θέσπιση άλλων νόμων σχετικών με την ΑΔΠ[32].

3.2.4 Εάν σκοπός είναι να περιληφθούν στο πεδίο εφαρμογής του σχεδίου νόμου τα μη ΣΣΣΠ, η ΕΚΤ προτείνει να προβλεφθούν οι ίδιες διευκρινίσεις και το ίδιο αποτελεσματικό πλαίσιο ανταλλαγής πληροφοριών και συνεργασίας κατά τα αναφερόμενα στην παράγραφο 3.1.6 σε σχέση με και μεταξύ, αφενός, της ΚΤΚ και της ΑΨΑ και, αφετέρου, εφόσον κρίνεται απαραίτητο, μεταξύ της ΑΨΑ και της ΕΚΤ, μέσω της ΚΤΚ.

3.3 *Αντίκτυπος του σχεδίου νόμου στους παρόχους κρίσιμων υπηρεσιών*

3.3.1 Το αναθεωρημένο πλαίσιο πολιτικής επίβλεψης του Ευρωσυστήματος[33] καλύπτει παρόχους κρίσιμων υπηρεσιών, όπως η Society for Worldwide Interbank Financial Telecommunication (SWIFT). Η SWIFT είναι συνεταιριστική εταιρία περιορισμένη ευθύνης εγκατεστημένη στο Βέλγιο, η οποία παρέχει ασφαλείς υπηρεσίες αποστολής μηνυμάτων σε μεγάλο αριθμό χωρών. Η Nationale Bank van België/Banque Nationale de Belgique ασκεί καθήκοντα ανώτατου οργάνου επίβλεψης της SWIFT και διενεργεί την επίβλεψη σε συνεργασία με τις λοιπές κεντρικές τράπεζες της Ομάδας των Δέκα (G10), περιλαμβανομένης της ΕΚΤ, βάσει σχετικών ρυθμίσεων από κοινού επίβλεψης. Τα όργανα επίβλεψης της Ομάδας των Δέκα αναγνωρίζουν ότι επίκεντρο της επίβλεψης αποτελεί ο λειτουργικός κίνδυνος της SWIFT, καθώς αυτός θεωρείται η βασικότερη κατηγορία κινδύνου λόγω του οποίου αυτή θα μπορούσε να προκαλέσει συστημικό κίνδυνο στο χρηματοπιστωτικό σύστημα της Ένωσης. Η ομάδα από κοινού επίβλεψης της SWIFT (SWIFT Cooperative Oversight Group) κατάρτισε συγκεκριμένη δέσμη αρχών και απαιτήσεων υψηλού επιπέδου που έχουν εφαρμογή στη SWIFT, π.χ. εντοπισμός και διαχείριση κινδύνου, ασφάλεια πληροφοριών, αξιοπιστία και ανθεκτικότητα, προγραμματισμός τεχνολογίας και επικοινωνία με τους χρήστες. Τα όργανα

28 Βλ. έγγραφο του Ευρωσυστήματος με τίτλο «Oversight expectations for links between retail payment systems», διαθέσιμο στον δικτυακό τόπο της ΕΚΤ.

29 Βλ. παράγραφο 2.4.4 της γνώμης CON/2017/31 και παράγραφο 3.2.3 της γνώμης CON/2018/22.

30 Ο περί της Κεντρικής Τράπεζας της Κύπρου Νόμος του 2002 (Ν. 138(Ι)/2002).

31 Βλ. επίσης παράγραφο 2.4.4 της γνώμης CON/2017/31 και παράγραφο 4.2 της γνώμης CON/2018/47.

32 Βλ. παράγραφο 3.4.2 της γνώμης CON/2018/22 και παράγραφο 4.3 της γνώμης CON/2018/47.

33 Βλ. έγγραφο του Ευρωσυστήματος με τίτλο «Eurosystem oversight policy framework» (αναθεωρημένη έκδοση), σ. 9, διαθέσιμο στον διαδικτυακό τόπο της ΕΚΤ.

επίβλεψης της Ομάδας των Δέκα υποβάλλουν τη SWIFT σε εντατική μορφή επίβλεψης και ζητούν από αυτή να τηρεί ιδιαιτέρως τις οδηγίες της CPMI και του IOSCO όσον αφορά την ασφάλεια στον κυβερνοχώρο και άλλα διεθνή πρότυπα ασφάλειας πληροφοριακών συστημάτων, τα οποία βαίνουν πέραν των απαιτήσεων της οδηγίας (ΕΕ) 2016/1148.

3.3.2 Όπως και στην περίπτωση των μη ΣΣΣΠ, δεν μπορεί να αποκλειστεί η πιθανότητα να καλύπτονται από το σχέδιο νόμου και τις εποπτικές εξουσίες της ΑΨΑ πάροχοι κρίσιμων υπηρεσιών στους οποίους εφαρμόζονται μέτρα επίβλεψης. Προτείνεται επομένως να λαμβάνονται υπόψη από τις κυπριακές αρχές κατά την εφαρμογή του σχεδίου νόμου οι υφιστάμενες ρυθμίσεις επίβλεψης, εάν η εφαρμογή του επηρεάζει παρόχους κρίσιμων υπηρεσιών[34]. Όσον αφορά την ειδική περίπτωση της SWIFT, προτείνεται η μη συμπερίληψή της στο πεδίο εφαρμογής του σχεδίου νόμου λαμβανομένου υπόψη, αφενός, ότι η SWIFT είναι εγκατεστημένη στο Βέλγιο και η διαχείρισή της γίνεται από το Βέλγιο με κόμβους υποδομών που δεν βρίσκονται στην επικράτεια της Κύπρου και, αφετέρου, ότι απλά παρέχει ασφαλείς υπηρεσίες αποστολής μηνυμάτων στην Κύπρο, καθώς και σε έναν τεράστιο αριθμό άλλων χωρών.

3.4 *Αντίκτυπος του σχεδίου νόμου στις υπηρεσίες πληρωμών, στα μέσα πληρωμών και στους μηχανισμούς πληρωμών*

3.4.1 Το πλαίσιο πολιτικής επίβλεψης του Ευρωσυστήματος θεωρεί τα μέσα πληρωμών, όπως τις κάρτες, τις μεταφορές πίστωσης, τις άμεσες χρεώσεις και το ηλεκτρονικό χρήμα, ως αναπόσπαστο τμήμα των συστημάτων πληρωμών και για τον λόγο αυτόν τα εντάσσει στο πεδίο επίβλεψης κεντρικών τραπεζών. Όσον αφορά τα μέσα πληρωμών, ο ρόλος του κύριου επιβλέποντα (για το Ευρωσύστημα) ανατίθεται με γνώμονα την εθνική βάση αναφοράς του μηχανισμού πληρωμών και το δίκαιο έδρας της αρχής διακυβέρνησής του. Όσον αφορά τα σχήματα μεταφοράς πιστώσεων και άμεσων χρεώσεων στο πλαίσιο του Ενιαίου Χώρου Πληρωμών σε Ευρώ, καθώς και ορισμένα από τα διεθνή συστήματα πληρωμών με κάρτα, η ΕΚΤ ασκεί τα κύρια καθήκοντα επίβλεψης. Οι πάροχοι υπηρεσιών πληρωμών (ΠΥΠ), περιλαμβανομένων των πιστωτικών ιδρυμάτων, των ιδρυμάτων πληρωμών και των ιδρυμάτων ηλεκτρονικού χρήματος, υπόκεινται στην οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[35], η οποία εφαρμόζεται από τον Ιανουάριο του 2018 όπως έχει μεταφερθεί στο εθνικό δίκαιο. Το νομικό και κανονιστικό πλαίσιο θεσπίζει υποχρεώσεις που αφορούν τους κινδύνους λειτουργίας και ασφάλειας και την αναφορά συμβάντων. Ωστόσο, τα όργανα προληπτικής εποπτείας θα πρέπει να κρίνουν με προσοχή όταν αποφασίζουν εάν θα δημοσιεύσουν πληροφορίες όσον αφορά επιμέρους συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο προκειμένου να διασφαλίζουν ότι δεν κλονίζεται η εμπιστοσύνη του κοινού στα ιδρύματα που θίγονται. Επιπλέον, η Ευρωπαϊκή Αρχή Τραπεζών (ΕΑΤ) κατάρτισε σχέδιο κατευθυντήριων γραμμών σχετικά με τη διαχείριση κινδύνου τεχνολογιών πληροφοριών και επικοινωνιών (ΤΠΕ) και ασφάλειας[36] οι οποίες σκοπούν στην εναρμόνιση των προτύπων που

34 Βλ. παράγραφο 3.3.1 της γνώμης CON/2018/22 και παράγραφο 5 της γνώμης CON/2018/47.

35 Οδηγία (ΕΕ) 2015/2366 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2015, σχετικά με υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 2002/65/ΕΚ, 2009/110/ΕΚ και 2013/36/ΕΕ και του κανονισμού (ΕΕ) αριθ. 1093/2010 και την κατάργηση της οδηγίας 2007/64/ΕΚ (ΕΕ L 337 της 23.12.2015, σ. 35).

36 Βλ. κατευθυντήριες γραμμές της ΕΑΤ, της 26ης Σεπτεμβρίου 2017, σχετικά με την εσωτερική διακυβέρνηση βάσει της οδηγίας 2013/36/ΕΕ (EBA/GL/2017/11) και σχέδιο κατευθυντήριων γραμμών της ΕΑΤ, της 13ης Δεκεμβρίου 2018, σχετικά με τη διαχείριση κινδύνου ΤΠΕ και ασφάλειας (EBA/CP/2018/15), διαθέσιμες στον δικτυακό τόπο της ΕΑΤ (www.eba.europa.eu).

απαιτείται να τηρούν οι πάροχοι υπηρεσιών πληρωμών όσον αφορά την ασφάλεια ΤΠΕ, την αναφορά συμβάντων, τη διαχείριση έργων και την αδιάλειπτη λειτουργία. Μολονότι οι ΠΥΠ υπόκεινται στη νομοθεσία της Ένωσης και στην κυπριακή νομοθεσία, καθώς και στους κανονισμούς που βασίζονται στη νομοθεσία της Ένωσης, η επίβλεψη των διεθνών και εγχώριων συστημάτων καρτών δεν υπόκειται καθαυτή στη νομοθεσία της Ένωσης[37].

3.4.2 Η ΕΚΤ αντιλαμβάνεται ότι οι διάφοροι μηχανισμοί πληρωμών, τα μέσα πληρωμών και οι ΠΥΠ ενδέχεται να εμπίπτουν στο πεδίο εφαρμογής του σχεδίου νόμου. Προτείνεται συνεπώς η πρόβλεψη των ίδιων διευκρινίσεων και του ίδιου αποτελεσματικού πλαισίου ανταλλαγής πληροφοριών και συνεργασίας κατά τα αναφερόμενα στην παράγραφο 3.1.6 σε σχέση με και μεταξύ, αφενός, των αρχών που είναι αρμόδιες για την επίβλεψη των μηχανισμών, των μέσων και των υπηρεσιών πληρωμών και για την εποπτεία των ΠΥΠ και, αφετέρου, της ΑΨΑ[38]. Θα μπορούσε επίσης να διευκρινιστεί στο σχέδιο νόμου ότι όσον αφορά την εποπτεία των ΠΥΠ, οι αρμοδιότητες της ΑΨΑ δεν θίγουν τα καθήκοντα της ΚΤΚ και εναρμονίζονται με αυτά.

3.5 *Αντίκτυπος του σχεδίου νόμου στα κεντρικά αποθετήρια τίτλων (ΚΑΤ)*

3.5.1 Τα ΚΑΤ υπόκεινται σε αυστηρή ρύθμιση και εποπτεία από διάφορες αρχές βάσει του κανονισμού (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[39], ο οποίος επιβάλλει απαιτήσεις που αφορούν τον λειτουργικό κίνδυνο. Επιπλέον, τα ΚΑΤ θα πρέπει να λαμβάνουν υπόψη τις οδηγίες της CPMI και του IOSCO όσον αφορά την ασφάλεια στον κυβερνοχώρο, οι οποίες εφαρμόζονται σε όλες τις υποδομές χρηματοπιστωτικών αγορών.

3.5.2 Πέραν των εποπτικών αρμοδιοτήτων που έχουν ανατεθεί στις εθνικές αρμόδιες αρχές (ΕΑΑ) βάσει του κανονισμού (ΕΕ) αριθ. 909/2014, θα πρέπει να σημειωθεί ότι στις εθνικές αρχές, ιδίως στα μέλη του ΕΣΚΤ, δύνανται να ανατεθούν αρμοδιότητες επίβλεψης σε σχέση με τα ΚΑΤ. Εν προκειμένω, η αιτιολογική σκέψη 8 του κανονισμού (ΕΕ) αριθ. 909/2014 ορίζει ότι οι διατάξεις του κανονισμού ισχύουν με την επιφύλαξη των αρμοδιοτήτων της ΕΚΤ και των ΕθνΚΤ για τη διασφάλιση αποτελεσματικών και υγιών συστημάτων εκκαθάρισης και πληρωμών εντός της Ένωσης και σε άλλες χώρες και ότι ο κανονισμός δεν θα πρέπει να εμποδίζει την πρόσβαση των μελών του ΕΣΚΤ σε πληροφορίες σχετικές με την άσκηση των καθηκόντων τους, συμπεριλαμβανομένης της επίβλεψης που ασκούν στα ΚΑΤ και σε άλλες υποδομές της χρηματαγοράς[40].

3.5.3 Το Κεντρικό Αποθετήριο και Κεντρικό Μητρώο Αξιών (ΚΑΚΜΑ) Κύπρου τελεί υπό τη διαχείριση του Χρηματιστηρίου Αξιών Κύπρου (ΧΑΚ)[41], εποπτεύεται από την Επιτροπή Κεφαλαιαγοράς Κύπρου (ΕΚΚ) και υπόκειται στην επίβλεψη της ΚΤΚ. Μολονότι το ΚΑΚΜΑ ενδέχεται να εμπίπτει στο πεδίο εφαρμογής του σχεδίου νόμου, η ΕΚΤ αντιλαμβάνεται ότι το σχέδιο νόμου δεν θα πρέπει να θίγει την εποπτεία και την επίβλεψη του ΚΑΚΜΑ, δεδομένου ότι αρμοδιότητες αυτές ασκούνται βάσει

37 Βλ. παράγραφο 2.4.3 της γνώμης CON/2017/31 και παράγραφο 3.4.2 της γνώμης CON/2018/22.

38 Βλ. επίσης παράγραφο 3.4.3 της γνώμης CON/2018/22 και παράγραφο 6.2 της γνώμης CON/2018/47.

39 Κανονισμός (ΕΕ) αριθ. 909/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014, σχετικά με τη βελτίωση του διακανονισμού αξιογράφων στην Ευρωπαϊκή Ένωση και τα κεντρικά αποθετήρια τίτλων και για την τροποποίηση των οδηγιών 98/26/ΕΚ και 2014/65/ΕΕ και του κανονισμού (ΕΕ) αριθ. 236/2012 (ΕΕ L 257 της 28.8.2014, σ. 1).

40 Βλ. παράγραφο 7.2 της γνώμης CON/2018/47 και παράγραφο 7.3 της γνώμης CON/2017/10.

41 Το κυπριακό ΚΑΤ συστάθηκε κατά τις διατάξεις του Νόμου 27(Ι)/1996 περί Αξιών και Χρηματιστηρίου Αξιών Κύπρου (Κεντρικό Αποθετήριο και Κεντρικό Μητρώο Αξιών).

νομοθεσίας της Ένωσης. Στο σχέδιο νόμου θα μπορούσε επίσης να διευκρινιστεί ότι οι αρμοδιότητες της ΑΨΑ δεν θίγουν τα καθήκοντα της ΚΤΚ και της ΕΚΚ και ευθυγραμμίζονται με αυτά.

3.6 *Στρατηγική ανθεκτικότητας του Ευρωσυστήματος όσον αφορά την ασφάλεια στον κυβερνοχώρο για τις υποδομές χρηματοπιστωτικών αγορών (ΥΧΑ)*

3.6.1 Οι κυπριακές αρχές θα μπορούσαν να λάβουν υπόψη τους και τη στρατηγική ανθεκτικότητας του Ευρωσυστήματος όσον αφορά την ασφάλεια στον κυβερνοχώρο για τις ΥΧΑ, η οποία σκοπεί στη στήριξη της εφαρμογής των οδηγιών της CPMI και του IOSCO από την άποψη της επίβλεψης. Στόχος της στρατηγικής είναι i) να βελτιώσει την ανθεκτικότητα του χρηματοπιστωτικού τομέα της ζώνης του ευρώ ως συνόλου όσον αφορά την ασφάλεια στον κυβερνοχώρο ενισχύοντας την «ετοιμότητα όσον αφορά την ασφάλεια στον κυβερνοχώρο» επιμέρους ΥΧΑ οι οποίες τελούν υπό την επίβλεψη κεντρικών τραπεζών του Ευρωσυστήματος· και ii) να προάγει τη συνεργασία μεταξύ ΥΧΑ, των οικείων παρόχων κρίσιμων υπηρεσιών και των οικείων αρχών. Στο πλαίσιο της εν λόγω στρατηγικής, το Ευρωσύστημα ανέπτυξε σειρά εργαλείων τα οποία μπορούν να χρησιμοποιήσουν οι ΥΧΑ για την ενίσχυση της ανθεκτικότητάς τους όσον αφορά την ασφάλεια στον κυβερνοχώρο, π.χ. το ευρωπαϊκό πλαίσιο δοκιμών από κατάλληλα εκπαιδευμένες ομάδες (red teams)[42] και άλλα εργαλεία, όπως έρευνες που αφορούν την ασφάλεια στον κυβερνοχώρο και αξιολογήσεις που εστιάζονται ειδικά στην εκτίμηση του επιπέδου ωριμότητας των συστημάτων πληρωμών του Ευρωσυστήματος όσον αφορά την ασφάλεια στον κυβερνοχώρο και την δημιουργία προσδοκιών επίβλεψης σε σχέση με την ανθεκτικότητα όσον αφορά την ασφάλεια στον κυβερνοχώρο[43] οι οποίες θα παρέχουν λεπτομερέστερες οδηγίες στους διαχειριστές συστημάτων πληρωμών.

4. Αντίκτυπος του σχεδίου νόμου στα πιστωτικά ιδρύματα

4.1 Σύμφωνα με την αιτιολογική σκέψη 13 της οδηγίας (ΕΕ) 2016/1148 οι απαιτήσεις που αφορούν τα συστήματα πληροφοριών, οι οποίες συχνά βαίνουν πέραν των απαιτήσεων που προβλέπονται στην οδηγία (ΕΕ) 2016/1148, ορίζονται σε διάφορες νομικές πράξεις της Ένωσης, όπως, μεταξύ άλλων, στους κανόνες για την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων. Τα κράτη μέλη θα πρέπει να λαμβάνουν υπόψη τους τις εν λόγω απαιτήσεις κατά την εφαρμογή των διατάξεων που μεταφέρουν στο εθνικό δίκαιο την οδηγία (ΕΕ) 2016/1148 ως *lex specialis*. Πράγματι, οι νομικές πράξεις της Ένωσης για την εναρμόνιση του τομέα της εποπτείας των πιστωτικών ιδρυμάτων περιλαμβάνουν τον κανονισμό (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[44] και την οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[45],

42 Βλ. το πλαίσιο δοκιμών του Ευρωσυστήματος «Threat Intelligence-based Ethical Red Teaming (TIBER-EU)» (Μάιος 2018), διαθέσιμο στον δικτυακό τόπο της ΕΚΤ.

43 Βλ. το έγγραφο με τίτλο «Cyber resilience oversight expectations for financial market infrastructures» (CROE) (Δεκέμβριος 2018), διαθέσιμο στον δικτυακό τόπο της ΕΚΤ.

44 Κανονισμός (ΕΕ) αριθ. 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τις απαιτήσεις προληπτικής εποπτείας για πιστωτικά ιδρύματα και επιχειρήσεις επενδύσεων και την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 176 της 27.6.2013, σ. 1).

45 Οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, για την τροποποίηση της οδηγίας 2002/87/ΕΚ και για την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

που από κοινού θεσπίζουν το πλαίσιο του κανονισμού και της οδηγίας για τις κεφαλαιακές απαιτήσεις (πλαίσιο CRR/CRDIV). Τα εγκατεστημένα στην Κύπρο πιστωτικά ιδρύματα πρέπει επίσης να τηρούν την οδηγία για τις ρυθμίσεις διακυβέρνησης και διαχείρισης[46], την οποία έχει εκδώσει η ΚΤΚ και η οποία θεσπίζει, μεταξύ άλλων, ένα πλαίσιο αρχών για την υγιή και αποτελεσματική λειτουργία των συστημάτων τεχνολογίας πληροφοριών στο πλαίσιο διαχείρισης του λειτουργικού κινδύνου.

4.2 Η ΕΚΤ και η ΚΤΚ αποτελούν τις αρμόδιες αρχές οι οποίες ασκούν ειδικές εξουσίες εποπτείας βάσει του πλαισίου CRR/CRDIV, δυνάμει του κανονισμού (ΕΕ) αριθ. 1024/2013 του Συμβουλίου[47], ο οποίος αναθέτει ειδικά καθήκοντα στην ΕΚΤ όσον αφορά την προληπτική εποπτεία πιστωτικών ιδρυμάτων εντός της ζώνης του ευρώ και καθιστά την ΕΚΤ υπεύθυνη για την αποτελεσματική και συνεπή λειτουργία του ενιαίου εποπτικού μηχανισμού (ΕΕΜ), στο πλαίσιο του οποίου ειδικές εποπτικές αρμοδιότητες κατανέμονται μεταξύ της ΕΚΤ και των συμμετεχουσών ΕΑΑ, περιλαμβανομένης της ΚΤΚ. Ειδικότερα, η ΕΚΤ εκτελεί το καθήκον χορήγησης άδειας λειτουργίας σε όλα τα πιστωτικά ιδρύματα και ανάκλησης της άδειας αυτής. Όσον αφορά τα σημαντικά πιστωτικά ιδρύματα, η ΕΚΤ έχει επίσης το καθήκον, μεταξύ άλλων, να διασφαλίζει τη συμμόρφωση με τη σχετική νομοθεσία της Ένωσης η οποία επιβάλλει στα πιστωτικά ιδρύματα απαιτήσεις προληπτικής εποπτείας, περιλαμβανομένης της υποχρέωσης να διαθέτουν άρτιες ρυθμίσεις διακυβέρνησης, όπως υγιείς διαδικασίες εκτίμησης κινδύνου και μηχανισμούς εσωτερικού ελέγχου[48]. Προς τον σκοπό αυτόν, στην ΕΚΤ έχουν χορηγηθεί όλες οι εποπτικές εξουσίες παρέμβασης στη δραστηριότητα των πιστωτικών ιδρυμάτων οι οποίες είναι αναγκαίες για την άσκηση των καθηκόντων της.

4.3 Η προληπτική εποπτεία των πιστωτικών ιδρυμάτων, όπως ασκείται από την ΕΚΤ και την ΚΤΚ στο πλαίσιο του ΕΕΜ, καλύπτει διάφορες πτυχές που αφορούν την ασφάλεια στον κυβερνοχώρο ως συστατικό της προληπτικής εποπτείας του λειτουργικού κινδύνου, ο οποίος έχει την έννοια του κινδύνου ζημιών οφειλόμενων στην ανεπάρκεια ή την αποτυχία εσωτερικών διαδικασιών, ατόμων και συστημάτων ή σε εξωτερικά γεγονότα[49]. Επιπροσθέτως, η ΕΑΤ έχει καταρτίσει κατευθυντήριες γραμμές σχετικά με την εσωτερική διακυβέρνηση οι οποίες καλύπτουν πτυχές κινδύνων πληροφοριακών συστημάτων και, όπως επισημαίνεται στην παράγραφο 3.4.1, σχέδιο κατευθυντήριων γραμμών σχετικά με τη διαχείριση κινδύνου ΤΠΕ και ασφάλειας[50] οι οποίες σκοπούν στην εναρμόνιση των απαιτήσεων που επιβάλλονται σε πιστωτικά ιδρύματα, επιχειρήσεις επενδύσεων και παρόχους υπηρεσιών πληρωμών όσον αφορά την ασφάλεια ΤΠΕ, την αναφορά συμβάντων, τη διαχείριση έργων και την αδιάλειπτη λειτουργία. Σε εξέλιξη βρίσκεται η κατάρτιση περαιτέρω κατευθυντήριων γραμμών της ΕΑΤ σχετικά με τη συμπερίληψη πτυχών κινδύνου στον κυβερνοχώρο στη διαδικασία εποπτικού ελέγχου και αξιολόγησης (Supervisory Review and

46 Η περί Ρυθμίσεων Διακυβέρνησης και Διαχείρισης Οδηγία του 2014.

47 Κανονισμός (ΕΕ) αριθ. 1024/2013 του Συμβουλίου, της 15ης Οκτωβρίου 2013, για την ανάθεση ειδικών καθηκόντων στην Ευρωπαϊκή Κεντρική Τράπεζα σχετικά με τις πολιτικές που αφορούν την προληπτική εποπτεία των πιστωτικών ιδρυμάτων (ΕΕ L 287 της 29.10.2013, σ. 63).

48 Βλ. άρθρο 4 παράγραφος 1 στοιχείο ε) και άρθρο 6 παράγραφος 4 του κανονισμού (ΕΕ) αριθ. 1024/2013.

49 Βλ. άρθρο 4 παράγραφος 1 σημείο 52 του κανονισμού (ΕΕ) αριθ. 575/2013.

50 Βλ. κατευθυντήριες γραμμές της ΕΑΤ, της 26ης Σεπτεμβρίου 2017, σχετικά με την εσωτερική διακυβέρνηση βάσει της οδηγίας 2013/36/ΕΕ (EBA/GL/2017/11) και σχέδιο κατευθυντήριων γραμμών της ΕΑΤ, της 13ης Δεκεμβρίου 2018, σχετικά με τη διαχείριση κινδύνου ΤΠΕ και ασφάλειας (EBA/CP/2018/15), διαθέσιμες στον δικτυακό τόπο της ΕΑΤ.

Evaluation Process – SREP)[51]. Η ΕΚΤ έχει καταρτίσει ολοκληρωμένα ερωτηματολόγια για τα εποπτευόμενα πιστωτικά ιδρύματα όσον αφορά τον κίνδυνο πληροφοριακών συστημάτων, τα οποία ενσωματώνονται στα οικεία αποτελέσματα της SREP και χρησιμοποιεί πληροφορίες που αφορούν ζητήματα ασφάλειας στον κυβερνοχώρο οι οποίες μπορούν να προέρχονται από θεματικούς ελέγχους, επιτόπιες επιθεωρήσεις και αναφορές συμβάντων όσον αφορά την ασφάλεια στον κυβερνοχώρο[52]. Οι εν λόγω πληροφορίες μπορούν να αποτελούν τη βάση για ad hoc συστάσεις που απευθύνονται σε συγκεκριμένο ίδρυμα, καθώς και γενικές συγκρίσεις και πολιτικές σε ολόκληρο τον τομέα. Ταυτόχρονα, τα όργανα προληπτικής εποπτείας θα πρέπει να κρίνουν με προσοχή όταν αποφασίζουν τη δημοσίευση πληροφοριών όσον αφορά επιμέρους συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο προκειμένου να μην κλονίζεται η εμπιστοσύνη του κοινού στα ιδρύματα που θίγονται.

4.4 Επιπλέον, η ΕΚΤ και οι ΕΑΑ στο πλαίσιο του ΕΕΜ είναι υπεύθυνες για την αξιολόγηση των σχεδίων ανάκαμψης και για τη λήψη μέτρων έγκαιρης παρέμβασης σύμφωνα με τις διατάξεις της οδηγίας 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[53] (όπως μεταφέρονται στο εθνικό δίκαιο). Περαιτέρω, η πρωταρχική ευθύνη για τη διαπίστωση ότι ένα σημαντικό πιστωτικό ίδρυμα τελεί υπό πτώχευση ή ενδέχεται να πτωχεύσει, ως προϋπόθεση για την εξυγίανση πιστωτικού ιδρύματος, ανήκει στην ΕΚΤ[54]. Στην περίπτωση εξυγίανσης, ένας από τους στόχους αυτής είναι η διασφάλιση της συνέχειας των κρίσιμων λειτουργιών[55], η οποία περιλαμβάνει και τη συνέχεια της λειτουργίας του συστήματος πληρωμών και κυκλοφορίας μετρητών του πιστωτικού ιδρύματος.

4.5 Οι κεντρικές τράπεζες εξαιρούνται από το πεδίο εφαρμογής της οδηγίας 2013/36/ΕΕ και συνεπώς δεν αποτελούν εποπτευόμενα ιδρύματα τα οποία εμπίπτουν στο πεδίο εφαρμογής του κανονισμού (ΕΕ) αριθ. 575/2013. Συνεπώς, ούτε η ΕΚΤ ούτε η ΚΤΚ εμπίπτουν στην έννοια του τραπεζικού τομέα για τους σκοπούς του σημείου 3 του παραρτήματος ΙΙ της οδηγίας (ΕΕ) 2016/1148[56].

4.6 Γίνεται αντιληπτό ότι, κατά την άσκηση του καθήκοντός της προς παρακολούθηση, η ΑΨΑ μπορεί να ζητεί τη συνδρομή σημαντικών και λιγότερο σημαντικών πιστωτικών ιδρυμάτων τα οποία είναι εγκατεστημένα ή λειτουργούν στην Κύπρο, καθώς και της ΚΤΚ και της ΕΚΤ ως αρμόδιων αρχών που ασκούν ειδικές εποπτικές εξουσίες σε σχέση με τα εν λόγω πιστωτικά ιδρύματα στο πλαίσιο του ΕΕΜ[57]. Γίνεται επίσης αντιληπτό ότι τα εγκατεστημένα στην Κύπρο πιστωτικά ιδρύματα μπορούν να χαρακτηριστούν φορείς εκμετάλλευσης βασικών υπηρεσιών, και επομένως θα πρέπει

---

51 Βλ. σχέδιο κατευθυντήριων γραμμών της ΕΑΤ, της 6ης Οκτωβρίου 2016, σχετικά με την αξιολόγηση κινδύνου ΤΠΕ βάσει της διαδικασίας εποπτικού ελέγχου και αξιολόγησης (SREP) (EBA/CP/2016/14), διαθέσιμο στον δικτυακό τόπο της ΕΑΤ.

52 Βλ. επίσης το άρθρο ενημερωτικού δελτίου της 13ης Φεβρουαρίου 2019 με τίτλο «IT and cyber risk - the SSM perspective», διαθέσιμο στον δικτυακό τόπο της ΕΚΤ.

53 Βλ. άρθρα 27 έως 30 της οδηγίας 2014/59/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τη θέσπιση πλαισίου για την ανάκαμψη και την εξυγίανση πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων και για την τροποποίηση της οδηγίας 82/891/ΕΟΚ του Συμβουλίου, και των οδηγιών 2001/24/ΕΚ, 2002/47/ΕΚ, 2004/25/ΕΚ, 2005/56/ΕΚ, 2007/36/ΕΚ, 2011/35/ΕΕ, 2012/30/ΕΕ και 2013/36/ΕΕ, καθώς και των κανονισμών του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ) αριθ. 1093/2010 και (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 190).

54 Βλ. άρθρο 32 παράγραφος 1 στοιχείο α) της οδηγίας 2014/59/ΕΕ.

55 Βλ. άρθρο 31 παράγραφος 2 στοιχείο α) της οδηγίας 2014/59/ΕΕ.

56 Βλ. παράγραφο 2.4 της γνώμης CON/2017/10.

57 Βλ. άρθρο 17 στοιχείο (λδ) του σχεδίου νομοθετικών διατάξεων.

να συμμορφώνονται με τις υποχρεώσεις που υπέχουν βάσει του σχεδίου νόμου. Τέλος, γίνεται αντιληπτό ότι η ενημέρωση του ευρέος κοινού σχετικά με συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο, όπως προβλέπεται στο σχέδιο νόμου[58], μπορεί να περιλαμβάνει συμβάντα προερχόμενα από πιστωτικά ιδρύματα.

4.7 Υπό το φως των ανωτέρω, η ΕΚΤ προτείνει να διευκρινιστεί ότι το πεδίο εφαρμογής του σχεδίου νόμου και οι εξουσίες που χορηγούνται στην ΑΨΑ βάσει αυτού δεν θίγουν τις αρμοδιότητες, τα καθήκοντα και τις εξουσίες που ανατίθενται στην ΕΚΤ και στην ΚΤΚ βάσει του κανονισμού (ΕΕ) αριθ. 1024/2013 και της σχετικής εθνικής νομοθεσίας[59]. Επιπροσθέτως, προκειμένου η ΕΚΤ και η ΚΤΚ να είναι σε θέση να εκπληρώνουν τα καθήκοντά τους στο πλαίσιο του ΕΕΜ, η ΕΚΤ προτείνει, για τους σκοπούς του σχεδίου νόμου, τη θέσπιση ρυθμίσεων συνεργασίας και ανταλλαγής πληροφοριών όχι μόνο μεταξύ της ΑΨΑ και της ΚΤΚ, αλλά και μεταξύ της ΑΨΑ και της ΕΚΤ, μέσω της ΚΤΚ, κατά τα αναφερόμενα στην παράγραφο 2.3[60]. Παραδείγματα τομέων στους οποίους θα ήταν χρήσιμες οι εν λόγω ρυθμίσεις συνεργασίας και ανταλλαγής πληροφοριών αποτελούν, ενδεικτικά, οι απαιτήσεις παροχής στοιχείων που επιβάλλονται στα πιστωτικά ιδρύματα, η διαδικασία λήψης αποφάσεων σχετικά με τη δημοσίευση πληροφοριών όσον αφορά επιμέρους συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο, καθώς και η διασφάλιση της συνέχειας των κρίσιμων λειτουργιών των πιστωτικών.

Η παρούσα γνώμη θα δημοσιευθεί στον δικτυακό τόπο της ΕΚΤ.

Φρανκφούρτη, 2 Μαΐου 2019.

[υπογραφή]

Ο Πρόεδρος της ΕΚΤ

Mario DRAGHI

58 Βλ. άρθρο 35 του σχεδίου νόμου.

59 Βλ. επίσης παράγραφο 4 της γνώμης CON/2018/22, παράγραφο 3.5 της γνώμης CON/2018/39 και παράγραφο 8.7 της γνώμης CON/2018/47.

60 Βλ. επίσης παράγραφο 4.6 της γνώμης CON/2018/22 και παράγραφο 8.7 της γνώμης CON/2018/47.