Επίσημη Εφημερίδα
της Ευρωπαϊκής Ένωσης

EL
Σειρά C

C/2026/3795

16.7.2026

ΠΡΟΕΙΔΟΠΟΙΗΣΗ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΣΥΜΒΟΥΛΙΟΥ ΣΥΣΤΗΜΙΚΟΥ ΚΙΝΔΥΝΟΥ

της 25ης Ιουνίου 2026

σχετικά με τους συστημικούς κινδύνους στον κυβερνοχώρο που απορρέουν από μοντέλα τεχνητής νοημοσύνης αιχμής

(ΕΣΣΚ/2026/3)

(C/2026/3795)

ΤΟ ΓΕΝΙΚΟ ΣΥΜΒΟΥΛΙΟ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΣΥΜΒΟΥΛΙΟΥ ΣΥΣΤΗΜΙΚΟΥ ΚΙΝΔΥΝΟΥ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τη συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο ([1]), και ιδίως το παράρτημα IX,

Έχοντας υπόψη τον κανονισμό (ΕΕ) αριθ. 1092/2010 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Νοεμβρίου 2010, σχετικά με τη μακροπροληπτική επίβλεψη του χρηματοοικονομικού συστήματος της Ευρωπαϊκής Ένωσης και τη σύσταση Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου ([2]), και ιδίως το άρθρο 3 παράγραφος 2 στοιχείο γ), και τα άρθρα 16 και 18,

Έχοντας υπόψη την απόφαση ΕΕΣΚ/2011/1 του Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου, της 20ής Ιανουαρίου 2011, για τη θέσπιση του εσωτερικού κανονισμού του Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου ([3]), και ιδίως τα άρθρα 18 και 19,

Εκτιμώντας τα ακόλουθα:

(1) Κορυφαίοι πάροχοι τεχνητής νοημοσύνης (ΤΝ) έχουν αναπτύξει μοντέλα ΤΝ αιχμής (Frontier AI Models — FAIM) με εξαιρετικές ικανότητες στον τομέα της κυβερνοασφάλειας και με δυνατότητα διενέργειας πλήρως αυτοματοποιημένων κυβερνοεπιθέσεων κατά πολύπλοκων συστημάτων, μεταξύ άλλων μέσω του εντοπισμού ευπαθειών και της ανάπτυξης και χρήσης exploit ως όπλων, πράγμα που μεταβάλλει ριζικά το τοπίο των κυβερνοαπειλών.

(2) Τα FAIM είναι σημαντικά καλύτερα από παλαιότερα μοντέλα ΤΝ στην εξεύρεση τρόπων διενέργειας κυβερνοεπιθέσεων και υπερτερούν των παλαιότερων αυτών μοντέλων σε κόστος, ταχύτητα και ακρίβεια, ανταγωνιζόμενα πλέον κορυφαίους ανθρώπινους εμπειρογνώμονες.

(3) Τα FAIM έχουν την ικανότητα να απειλούν τα συστήματα που υποστηρίζουν τα περιβάλλοντα τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) στα οποία βασίζονται οι χρηματοοικονομικές υποδομές, αυξάνοντας την πιθανότητα και τη σοβαρότητα κυβερνοπεριστατικών με συστημικό αντίκτυπο.

(4) Τα FAIM επιδεικνύουν ήδη την ικανότητα να εντοπίζουν ευπάθειες και να σχεδιάζουν καινοτόμα exploit, εκθέτοντας στον κίνδυνο κυβερνοεπιθέσεων καίρια λειτουργικά συστήματα και λογισμικό που χρησιμοποιούνται στα περιβάλλοντα ΤΠΕ όλων σχεδόν των οργανισμών.

(5) Ιστορικά ο εντοπισμός των παραπάνω ευπαθειών είναι σπάνιος και συνήθως πραγματοποιείται από ερευνητές στον τομέα της ασφάλειας κατά τρόπο που καθιστά δυνατή τη στοχευμένη αποκατάστασή τους. Στις περιπτώσεις αυτές παρέχεται συχνά στους παρόχους λογισμικού τυποποιημένο χρονοδιάγραμμα συνήθους διάρκειας 90 ημερών για την αποκατάσταση της ευπάθειας πριν από τη δημοσιοποίησή της. Ωστόσο, πιθανολογείται ότι με τη χρήση των FAIM θα αυξηθεί ο όγκος των εντοπιζόμενων ευπαθειών.

(6) Σήμερα οι πρακτικές διόρθωσης στο χρηματοπιστωτικό σύστημα έχουν πρωτίστως κατασταλτικό χαρακτήρα, καθώς βασίζονται σε περιοδικές επικαιροποιήσεις και στην ανάληψη δράσης κατόπιν δημοσιοποίησης των ευπαθειών κατά περίπτωση. Η προσέγγιση αυτή όντως αποδίδει σε ένα περιβάλλον απειλών στο οποίο τα διαθέσιμα χρονικά περιθώρια επιτρέπουν στις εντοπιζόμενες ευπάθειες να παραμένουν διαχειρίσιμες. Ωστόσο, λόγω της αύξησης του όγκου των ευπαθειών ενδέχεται οι ισχύουσες πρακτικές να καταστούν ανεπαρκείς για τη διατήρηση της επιχειρησιακής ανθεκτικότητας.

(7) Επίσης, η αύξηση του όγκου των ευπαθειών εκθέτει τις υφιστάμενες διαδικασίες διόρθωσης στον κίνδυνο υπερβολικής επιβάρυνσης, καθώς οι διαδικασίες αυτές, αφενός, δίνουν προτεραιότητα σε μέτρα αποκατάστασης που βασίζονται στον κίνδυνο και, αφετέρου, απαιτούν τη διενέργεια δοκιμών διορθώσεων λογισμικού πριν από την εφαρμογή των μέτρων προς διασφάλιση της επιχειρησιακής σταθερότητας. Εάν εντοπιστεί εντός σύντομου χρονικού διαστήματος υπερβολικά μεγάλος αριθμός ευπαθειών με κρίσιμο αντίκτυπο, οδηγώντας σε σημαντική αύξηση του αριθμού των απαιτούμενων κρίσιμων διορθώσεων λογισμικού, τα χρηματοοικονομικά ιδρύματα ενδέχεται να αναγκαστούν να αποφανθούν αν θα προκρίνουν την έκθεσή τους σε σημαντικούς κινδύνους στον κυβερνοχώρο ή τη μείωση των απαιτήσεων διενέργειας δοκιμών διορθώσεων και, ως εκ τούτου, την έκθεσή τους στον κίνδυνο περιστατικών που επηρεάζουν τη λειτουργία τους και σε διακοπές λειτουργίας.

([1]) ΕΕ L 1 της 3.1.1994, σ. 3, ELI: http://data.europa.eu/eli/agree_internation/1994/1/oj.
([2]) ΕΕ L 331 της 15.12.2010, σ. 1, ELI: http://data.europa.eu/eli/reg/2010/1092/oj.
([3]) ΕΕ C 58 της 24.2.2011, σ. 4.

(8) Ενώ παλαιότερα η εκπόνηση και χρήση exploit ως όπλων ήταν κυρίως χειροκίνητη και οι εμπειρογνώμονες χρειάζονταν ημέρες ή εβδομάδες, τώρα μπορεί να πραγματοποιείται από FAIM εντός ολίγων λεπτών ή ωρών. Αυτό σημαίνει κατάρρευση των χρονικών περιθωρίων ασφαλείας που είναι απαραίτητα στον αμυνόμενο για τη διατήρηση της συνέχειας κρίσιμων και σημαντικών λειτουργιών όσο διαρκεί η αποκατάσταση.

(9) Με την εξάπλωση και χρήση των exploit ως όπλων που στοχεύουν στις κρίσιμες ευπάθειες τις οποίες τροφοδοτεί η ΤΝ, καθώς και με την αντίστοιχη μείωση των χρονικών περιθωρίων ασφαλείας του αμυνόμενου, αυξάνεται απότομα ο κίνδυνος για μεμονωμένες κρίσιμες ή σημαντικές λειτουργίες και ιδρύματα. Η ταυτόχρονη εκδήλωση των κινδύνων αυτών στις εν λόγω λειτουργίες και τα ιδρύματα θα μπορούσε να οδηγήσει σε μόνιμη αύξηση του συστημικού κινδύνου στον κυβερνοχώρο, για την οποία σήμερα δεν υπάρχει πλήρως αποτελεσματικό πλαίσιο μετριασμού. Λόγω της ισχυρής διασυνδεσιμότητας που υπάρχει στο εσωτερικό του ενωσιακού χρηματοοικονομικού τομέα, αλλά και μεταξύ του τομέα αυτού και άλλων τομέων και χωρών, η συγκεκριμένη κατάσταση εγείρει συστηματικό κίνδυνο και μπορεί εν δυνάμει να δημιουργήσει συστημικές αδυναμίες.

(10) Επιπλέον, τα FAIM σήμερα αναπτύσσονται από έναν μικρό μόνο αριθμό παρόχων ΤΝ, αρκετοί εκ των οποίων εκφράζουν ήδη ανησυχίες ότι τα μελλοντικά FAIM ενδέχεται να είναι υπερβολικά ισχυρά για να επιτραπεί η απεριόριστη πρόσβαση του κοινού σε αυτά.

(11) Η ΤΝ χρησιμοποιείται ήδη από κακόβουλους παράγοντες για την ενίσχυση των κυβερνοεπιθέσεων. Πιθανολογείται ότι εν τέλει οι παράγοντες αυτοί θα αποκτήσουν, μέσω διαρροών, κλοπής, ανεξάρτητης ανάπτυξης ή και ανοικτής πρόσβασης, μοντέλα ΤΝ με ικανότητες αντίστοιχες εκείνων που χρησιμοποιούνται σήμερα σε ελεγχόμενα περιβάλλοντα αμυνομένων.

(12) Ενώ τα FAIM ενδέχεται να αυξήσουν σημαντικά τις ικανότητες των επιτιθέμενων και την πιθανότητα εξελιγμένων κυβερνοεπιθέσεων, θα ενισχύσουν και τις ικανότητες των αμυνομένων, ιδίως όσον αφορά τον εντοπισμό ευπαθειών, τη συσχέτιση δεδομένων και τη λήψη διορθωτικών μέτρων από μεμονωμένα ιδρύματα. Ωστόσο, βραχυμεσοπρόθεσμα η αύξηση της ταχύτητας, της κλίμακας και του βαθμού ακρίβειας των ικανοτήτων των επιτιθέμενων είναι πιθανό να υπερκεράσει τα οφέλη.

(13) Η ραγδαία ανάπτυξη των FAIM καθιστά αναγκαία την εξέταση των εντοπιζόμενων κινδύνων για τη χρηματοπιστωτική σταθερότητα χωρίς καθυστέρηση, προκειμένου να αποτραπεί η επέλευσή τους ή τουλάχιστον να μετριαστεί ο δυνητικός αντίκτυπός τους. Για να διασφαλιστεί η χρηματοπιστωτική σταθερότητα στις χρηματοοικονομικές αγορές της Ένωσης θα πρέπει όλα τα μέλη του Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου (ΕΣΣΚ) να εξετάσουν τις επιπτώσεις των FAIM στην επιχειρησιακή ικανότητα και ανθεκτικότητα των χρηματοοικονομικών ιδρυμάτων στο πλαίσιο των δράσεων μακροπροληπτικής και μικροπροληπτικής πολιτικής τους. Αυτό ισχύει με την επιφύλαξη των εντολών νομισματικής πολιτικής των κεντρικών τραπεζών στην Ένωση. Εν είδει παραδείγματος μίας από τις τρέχουσες πρωτοβουλίες που αναλαμβάνουν διάφορες αρχές, η ΕΚΤ, ως αρχή τραπεζικής εποπτείας, ζήτησε από τα σημαντικά ιδρύματα να αξιολογήσουν χωρίς καθυστέρηση τον αντίκτυπο του εξελισσόμενου τοπίου των απειλών και να καταρτίσουν έως τις 31 Οκτωβρίου 2026 ολοκληρωμένο σχέδιο δράσης, στο οποίο θα περιγράφονται συγκεκριμένα μέτρα αντιμετώπισης των εν λόγω κινδύνων ([4]).

(14) Καθώς η τεχνολογία ΤΝ εξαπλώνεται, είναι σημαντικό να διασφαλιστεί η ετοιμότητα όλων των κρίσιμων υποδομών, και ιδίως των χρηματοοικονομικών ιδρυμάτων, να αντιμετωπίσουν κυβερνοεπιθέσεις τροφοδοτούμενες από FAIM και να προβούν σε έγκαιρες και κατάλληλες προετοιμασίες. Ωστόσο, οι εν λόγω προσπάθειες μεμονωμένων αμυνόμενων οντοτήτων ενδέχεται να αποδειχθούν ανεπαρκείς. Η αποτελεσματική ανταπόκριση και ο μετριασμός του κινδύνου απαιτούν συντονισμένη απάντηση με τη συμμετοχή όλων των επηρεαζόμενων μερών, συμπεριλαμβανομένων των παρόχων ΤΝ και λογισμικού, των επιχειρήσεων παροχής υπηρεσιών ασφαλείας, των συντηρητών ανοικτού κώδικα, των χρηματοοικονομικών ιδρυμάτων και των αρχών τόσο σε εθνικό όσο και σε ενωσιακό επίπεδο.

(15) Κατά την εξέταση των παραπάνω ζητημάτων είναι σημαντική η υπόμνηση των συναφών νομικών πλαισίων και πλαισίων πολιτικής της Ένωσης, ιδίως των κανονισμών (ΕΕ) 2022/2554 ([5]), (ΕΕ) 2024/1689 ([6]) και (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([7]), καθώς και της σύστασης του Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου (ΕΣΣΚ/2021/17) ([8]).

([4]) Η επιστολή που απευθύνεται στα σημαντικά ιδρύματα είναι διαθέσιμη στον ιστότοπο της ΕΚΤ για την τραπεζική εποπτεία (www.bankingsupervision.europa.eu).

([5]) Κανονισμός (ΕΕ) 2022/2554 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 648/2012, (ΕΕ) αριθ. 600/2014, (ΕΕ) αριθ. 909/2014 και (ΕΕ) 2016/1011 (ΕΕ L 333 της 27.12.2022, σ. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([6]) Κανονισμός (ΕΕ) 2024/1689 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Ιουνίου 2024, για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη) (ΕΕ L 2024/1689 της 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([7]) Κανονισμός (ΕΕ) 2024/2847 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2024, σχετικά με οριζόντιες απαιτήσεις κυβερνοασφάλειας για προϊόντα με ψηφιακά στοιχεία και για την τροποποίηση των κανονισμών (ΕΕ) αριθ. 168/2013 και (ΕΕ) 2019/1020 και της οδηγίας (ΕΕ) 2020/1828 (κανονισμός για την κυβερνοανθεκτικότητα) (ΕΕ L 2024/2847 της 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([8]) Σύσταση του Ευρωπαϊκού Συμβουλίου Συστημικού Κινδύνου, της 2ας Δεκεμβρίου 2021, σχετικά με ένα πανευρωπαϊκό πλαίσιο συντονισμού συστημικών κυβερνοπεριστατικών για τις σχετικές αρχές (ΕΣΣΚ/2021/17) (ΕΕ C 134 της 25.3.2022, σ. 1).

(16) Ο κανονισμός (ΕΕ) 2022/2554 παρέχει στα χρηματοοικονομικά ιδρύματα ένα ολοκληρωμένο πλαίσιο εντοπισμού, διαχείρισης, παρακολούθησης και μετριασμού των κινδύνων ΤΠΕ, μεταξύ άλλων και όσων απορρέουν από κυβερνοεπιθέσεις. Λόγω της διασυνδεσιμότητας του χρηματοοικονομικού τομέα και της εξάρτησής του από συστήματα ΤΠΕ και τρίτους παρόχους υπηρεσιών, μια επιτυχής κυβερνοεπίθεση που πλήττει ένα ή περισσότερα χρηματοοικονομικά ιδρύματα ή τους κρίσιμους παρόχους υπηρεσιών τους θα μπορούσε να έχει σημαντικές συστημικές επιπτώσεις. Οι αρχές χρηματοπιστωτικής εποπτείας θα πρέπει να δώσουν τη δέουσα προτεραιότητα στις εποπτικές δραστηριότητες αυτού του πεδίου, λαμβάνοντας υπόψη όχι μόνο τον δυνητικό αντίκτυπο των εν λόγω κυβερνοεπιθέσεων στη σταθερότητα, την ακεραιότητα και την αξιοπιστία του χρηματοπιστωτικού συστήματος, αλλά και την επιχειρησιακή και χρηματοπιστωτική βλάβη που ενδέχεται να προκύψει, καθώς και τη ζημία για τους καταναλωτές.

(17) Ο κανονισμός (ΕΕ) 2024/1689 θεσπίζει εναρμονισμένους κανόνες για τη διάθεση στην αγορά, τη θέση σε λειτουργία και τη χρήση συστημάτων ΤΝ και μοντέλων ΤΝ γενικού σκοπού στην Ένωση και, σε ορισμένες περιπτώσεις, συστημάτων και μοντέλων παρόχων ΤΝ εγκατεστημένων σε τρίτες χώρες, όταν τα στοιχεία εξόδου του συστήματος ΤΝ χρησιμοποιούνται στην Ένωση ή ορισμένο μοντέλο ΤΝ ενσωματώνεται σε σύστημα που διατίθεται στην αγορά της Ένωσης. Ο ίδιος κανονισμός προβλέπει επίσης ειδικούς κανόνες για μοντέλα που ταξινομούνται ως μοντέλα ΤΝ γενικού σκοπού με συστημικό κίνδυνο, συμπεριλαμβανομένου του αυστηρότερου κανονιστικού καθεστώτος.

(18) Ο κανονισμός (ΕΕ) 2024/2847 εισάγει για τους κατασκευαστές υποχρεωτικές απαιτήσεις κυβερνοασφάλειας που καλύπτουν τον προγραμματισμό, τον σχεδιασμό, την ανάπτυξη και τη συντήρηση προϊόντων υλισμικού και λογισμικού με ψηφιακά στοιχεία τα οποία διατίθενται στην αγορά της Ένωσης. Απαιτεί επίσης από τους κατασκευαστές να χειρίζονται ευπάθειες εκδηλούμενες στη διάρκεια του κύκλου ζωής των προϊόντων τους. Μόλις οι εν λόγω απαιτήσεις τεθούν σε πλήρη εφαρμογή τον Δεκέμβριο του 2027, οι χρηματοοικονομικές οντότητες που διαθέτουν τα συγκεκριμένα προϊόντα στην αγορά της Ένωσης θα πρέπει επίσης να διασφαλίσουν τη συμμόρφωση των προϊόντων με αυτές.

(19) Η σύσταση ΕΣΣΚ/2021/17 συνέστησε στις ευρωπαϊκές εποπτικές αρχές (ΕΕΑ) να αναπτύξουν από κοινού, μέσω της Μεικτής Επιτροπής, και από κοινού με την Ευρωπαϊκή Κεντρική Τράπεζα (ΕΚΤ), το ΕΣΣΚ και τις αρμόδιες εθνικές αρχές, αποτελεσματικό μηχανισμό συντονισμένης απάντησης σε επίπεδο Ένωσης σε περίπτωση σοβαρού διασυνοριακού κυβερνοπεριστατικού ή συναφούς απειλής που θα μπορούσε να έχει συστημικό αντίκτυπο στον χρηματοπιστωτικό τομέα της Ένωσης. Η σύσταση αυτή οδήγησε στη θέσπιση του πανευρωπαϊκού πλαισίου συντονισμού συστημικών κυβερνοπεριστατικών (EU-SCICF), το οποίο παρέχει μια πολύτιμη και λειτουργική πλατφόρμα ανταλλαγής πληροφοριών και συντονισμού των χρηματοπιστωτικών αρχών μεταξύ τους.

(20) Με βάση τα παραπάνω το ΕΣΣΚ εκδίδει προειδοποίηση γενικού χαρακτήρα που εξετάζει τους σημαντικούς κινδύνους που απειλούν τη χρηματοπιστωτική σταθερότητα και ενισχύονται από την ανάπτυξη των FAIM. Η προειδοποίηση λαμβάνει υπόψη την ανάλυση που περιλαμβάνεται στο υπόμνημα του ΕΣΣΚ με τίτλο «Addressing Frontier AI Models with cybercapabilities from a financial stability perspective» (Εξετάζοντας μοντέλα ΤΝ αιχμής με ικανότητες στον κυβερνοχώρο από τη σκοπιά της χρηματοπιστωτικής σταθερότητας), το οποίο δημοσιεύτηκε τον Ιούνιο του 2026 ([9]),

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΠΡΟΕΙΔΟΠΟΙΗΣΗ:

ΤΜΗΜΑ 1

Προειδοποίηση

Νέο τοπίο κινδύνων

Η ταχεία ανάπτυξη μοντέλων ΤΝ αιχμής με ικανότητα στον κυβερνοχώρο επιφέρει ουσιώδεις αλλαγές στο τοπίο κινδύνων για το χρηματοπιστωτικό σύστημα της Ένωσης. Τα διαθέσιμα σήμερα στοιχεία δείχνουν ότι τα FAIM είναι σε θέση να εντοπίζουν ευπάθειες, να επινοούν exploit και να εκτελούν αυτόνομα ολοκληρωμένες κυβερνοεπιθέσεις με ταχύτητα, κλίμακα και επίπεδο ακρίβειας που υπερτερούν κατά πολύ έναντι των πρότερων μοντέλων ΤΝ. Αυτό συνιστά αλλαγή προτύπου στον τομέα της κυβερνοασφάλειας και σημείο καμπής όσον αφορά την ικανότητα ΤΝ.

Το ΕΣΣΚ θεωρεί τις εξελίξεις αυτές πηγή συστημικών κινδύνων για το χρηματοπιστωτικό σύστημα και εν δυνάμει πηγή πρόκλησης σημαντικών δυσμενών επιπτώσεων στην κυβερνοασφάλεια μέσω του ταχύτερου εντοπισμού ευπαθειών, της μείωσης του διαθέσιμου χρόνου απάντησης και αποτελεσματικής άμυνας, της αυξημένης κλίμακας και εξειδίκευσης των κυβερνοεπιθέσεων και της εισαγωγής νέων εξαρτήσεων και κινδύνων συγκέντρωσης εντός του χρηματοπιστωτικού συστήματος. Μολονότι αναγνωρίζεται η αξία τους, οι ενισχυμένες ικανότητες άμυνας που θα προσφέρουν τα FAIM στα χρηματοοικονομικά ιδρύματα είναι πιθανό ότι θα υλοποιηθούν σταδιακά εντός των προσεχών ετών, οπότε τα ιδρύματα αυτά θα διανύσουν υποχρεωτικά μια μεταβατική περίοδο λειτουργίας χαρακτηριζόμενη από αυξημένο κίνδυνο και υψηλό βαθμό αβεβαιότητας σε ένα ταχέως εξελισσόμενο τεχνολογικό τοπίο. Λόγω του εξαιρετικά ψηφιοποιημένου και διασυνδεδεμένου χαρακτήρα του χρηματοπιστωτικού συστήματος οι δυσμενείς αυτές επιπτώσεις στην κυβερνοασφάλεια θα μπορούσαν να διαδοθούν γρήγορα, επηρεάζοντας κρίσιμες και σημαντικές λειτουργίες σε όλα τα χρηματοοικονομικά ιδρύματα και οδηγώντας τελικά σε συστημική διαταραχή και απώλεια εμπιστοσύνης στο χρηματοπιστωτικό σύστημα.

([9]) Διαθέσιμο στον ιστότοπο του ΕΣΣΚ (www.ecb.europa.eu).

Τα αναδυόμενα FAIM αυξάνουν τον εγγενή κίνδυνο ΤΠΕ, οδηγώντας σε αποδυνάμωση της επιχειρησιακής ανθεκτικότητας σε επίπεδο χρηματοπιστωτικού τομέα, ιδίως σε τέσσερα πεδία: α) τον χρόνο, που περιλαμβάνει και την ικανότητα ταχείας ενημέρωσης κώδικα πολύπλοκων συστημάτων χωρίς να προκαλείται λειτουργική αστοχία, λαμβανομένης υπόψη της ραγδαίας σύντμησης των χρονικών περιθωρίων ασφαλείας για τους αμυνόμενους από τον εντοπισμό των ευπαθειών έως τη χρήση των exploit ως όπλων· β) την ικανότητα των αμυνόμενων, συμπεριλαμβανομένης τόσο της ικανότητάς τους να διενεργούν αυτοματοποιημένες και χειροκίνητες δοκιμές ασφάλειας με τη βοήθεια FAIM όσο και της ικανότητάς τους να προστατεύουν, να εντοπίζουν και να αντιμετωπίζουν απειλές που απορρέουν από την αντιπαραθετική χρήση FAIM· γ) τη συγκέντρωση, η οποία αφορά και τις εξαρτήσεις από περιορισμένο αριθμό παρόχων ΤΝ που με τη σειρά τους εξαρτώνται από παρόχους υπολογιστικού νέφους, συστατικά στοιχεία ανοικτού κώδικα και άλλο ευρέως χρησιμοποιούμενο λογισμικό· και δ) την ικανότητα των αρχών, συμπεριλαμβανομένων της εκ μέρους τους βαθμονόμησης των προσδοκιών, των προσομοιώσεων ακραίων καταστάσεων και των μέτρων ετοιμότητας σύμφωνα με την ανάπτυξη FAIM, ώστε οι λειτουργικές αστοχίες να μη μετατρέπονται σε πηγή ευρύτερης αστάθειας.

Επιπλέον, η διασφάλιση και η διατήρηση της προβολής όσον αφορά τη χρήση ΤΝ σε κάθε χρηματοοικονομικό ίδρυμα, η οποία αφορά και την πλήρη κατανόηση του πού και πώς γίνεται η χρήση αυτή, συνιστούν πρόκληση, δεδομένου ότι η ΤΝ χρησιμοποιείται σε διεπαφές πελατών, σε εσωτερικούς παράγοντες, σε επιχειρησιακές διαδικασίες και στη διασύνδεση με τρίτους.

Συστημική αξιολόγηση

Τα περιστατικά που εντοπίζονται ενδέχεται να μεταβάλουν ουσιωδώς τόσο την κλίμακα όσο και τη δομή του κυβερνοκινδύνου, αυξάνοντας όχι μόνο τους άμεσους κινδύνους για τη χρηματοπιστωτική σταθερότητα, αλλά και τους έμμεσους κινδύνους. Οι ικανότητες των FAIM ενδέχεται να ασκήσουν σημαντική πίεση στα υφιστάμενα πλαίσια ανθεκτικότητας, ιδίως εάν τα περιστατικά έχουν ευρεία διάδοση και εκδηλώνονται ταυτόχρονα. Εξάλλου, τα περιστατικά μπορούν να διαδοθούν ταχέως στα χρηματοοικονομικά ιδρύματα και τις αγορές εάν επηρεαστούν κρίσιμοι τρίτοι πάροχοι, κοινά τεχνολογικά οικοσυστήματα ή ευρέως χρησιμοποιούμενες συνιστώσες ανοικτού κώδικα, αυξάνοντας τον κίνδυνο σχετικών διαταραχών με συστημικές επιπτώσεις.

Τα FAIM μεταβάλλουν τρεις πηγές ασυμμετρίας στον χρηματοπιστωτικό τομέα: πρώτον, μεταξύ χωρών, δεύτερον, μεταξύ επιτιθέμενων και αμυνόμενων και, τρίτον, μεταξύ καλύτερα και ανεπαρκέστερα εξοπλισμένων χρηματοοικονομικών ιδρυμάτων από άποψη πόρων.

Πρώτον, η τρέχουσα γεωγραφική συγκέντρωση κορυφαίων παρόχων ΤΝ εκτός της Ένωσης αφήνει την Ένωση εκτεθειμένη σε στρατηγική εξάρτηση και γεωπολιτικό κίνδυνο. Για να μετριαστεί η ασυμμετρία γνώσης και τεχνολογίας μεταξύ χωρών απαιτείται η θέσπιση μέτρων διευκόλυνσης της επαρκούς και αναλογικής πρόσβασης της Ένωσης και των κρατών μελών της σε νέα FAIM. Τα μέτρα αυτά θα πρέπει να είναι έγκαιρα, συνεκτικά και αποτελεσματικά, τόσο σε επίπεδο επιλογών πολιτικής όσο και εφαρμογής, θα πρέπει δε να λαμβάνουν επαρκώς υπόψη τους διαφορετικούς χρηματοοικονομικούς τομείς της Ένωσης, αξιοποιώντας την εμπειρογνωσία των αντίστοιχων ΕΕΑ. Αυτό δεν θα αμβλύνει την ασυμμετρία μόνο μεταξύ χωρών εντός και εκτός Ένωσης, αλλά και μεταξύ χρηματοοικονομικών ιδρυμάτων εγκατεστημένων σε διαφορετικά κράτη μέλη, διαφυλάσσοντας την ισοτιμία των όρων ανταγωνισμού εντός και εκτός Ένωσης και ελαχιστοποιώντας τον συστημικό κίνδυνο. Τυχόν ρυθμίσεις που διευκολύνουν την πρόσβαση ορισμένων μόνο κατηγοριών ιδρυμάτων ή επιλεγμένων χωρών σε FAIM θα συντελέσουν στον κατακερματισμό της ενιαίας αγοράς στον τομέα της χρηματοδότησης, μειώνοντας τη ρευστότητα και το βάθος της.

Δεύτερον, όσον αφορά την ασυμμετρία μεταξύ επιτιθέμενων και αμυνόμενων τα FAIM μειώνουν την τιμή εισόδου για τους επιτιθέμενους. Είναι πιθανό ότι, για την εκτέλεση των συνιστωσών των επιθετικών επιχειρήσεων που είναι τεχνικά πιο προηγμένες και ενέχουν υψηλότερη ένταση εργασίας, οι παράγοντες απειλής θα βασίζονται όλο και περισσότερο στα FAIM, μειώνοντας το κόστος. Αντιθέτως, οι αμυνόμενοι περιορίζονται από επιχειρησιακές απαιτήσεις, εξαρτήσεις και κανονιστικές υποχρεώσεις που μειώνουν τη δυνατότητά τους να αντλήσουν τα οφέλη των FAIM βραχυμεσοπρόθεσμα από άποψη αποτελεσματικότητας και κλίμακας, γεγονός που τελικά απαιτεί μεγαλύτερες περιόδους προσαρμογής.

Τρίτον, υπάρχουν διαφορές στον τρόπο με τον οποίο τα χρηματοοικονομικά ιδρύματα αποκτούν πόρους και εξοπλισμό για την αντιμετώπιση των προκλήσεων που εγείρουν τα FAIM. Οι διαφορές αυτές ενδέχεται να οφείλονται σε έξοδα που είναι σταθερά και όχι κλιμακωτά, καθώς και σε περιορισμούς στους πόρους και στην πρόσβαση σε ειδικούς. Όταν υπάρχει ασυμμετρία στην ικανότητα αντιμετώπισης τέτοιων προκλήσεων, ο πιο αδύναμος κρίκος της αλυσίδας μπορεί να επηρεάσει τη σταθερότητα του συστήματος.

Επιπτώσεις

Είναι σημαντικό να διασφαλιστεί ότι τα συστημικώς σημαντικά συστήματα πληρωμών και διακανονισμού και οι υποδομές των χρηματοοικονομικών αγορών παραμένουν θωρακισμένα έναντι ευπαθειών που προκύπτουν από τη χρήση και ανάπτυξη των FAIM. Δημόσιοι και ιδιωτικοί φορείς θα πρέπει να επανεξετάσουν και να επικαιροποιήσουν διεξοδικά τα οικεία πλαίσια κυβερνοασφάλειας, ώστε να ληφθούν υπόψη οι εν λόγω ευπάθειες. Οι αρχές με αρμοδιότητες εποπτείας ή επίβλεψης θα πρέπει να λαμβάνουν μέτρα για να διασφαλίζουν την επαρκή προστασία των συστημάτων. Η συνεργασία μεταξύ αρχών και ιδιωτικών χρηματοοικονομικών ιδρυμάτων θα πρέπει να επιδιώκεται όποτε παρίσταται ανάγκη ενίσχυσης της ασφάλειας και ανθεκτικότητας του χρηματοπιστωτικού συστήματος της Ένωσης.

Στην έκθεση του 2020 σχετικά με τον συστημικό κίνδυνο στον κυβερνοχώρο ([10]) το ΕΣΣΚ προσδιόρισε την ταχύτητα, την κλίμακα και την κακόβουλη πρόθεση των κυβερνοαπειλών ως πιθανές πηγές διάδοσης του συστημικού κινδύνου. Οι αρχές θα πρέπει να γνωρίζουν ότι, αν και νέα πηγή διάδοσης, τα FAIM ενισχύουν τις υφιστάμενες πηγές που είχαν προσδιοριστεί παλαιότερα, αυτή δε η πτυχή θα πρέπει να ενσωματωθεί στη δράση πολιτικής τους. Λαμβανομένων υπόψη όλων των κινδύνων για τη χρηματοπιστωτική σταθερότητα που απορρέουν από την επιχειρησιακή έκθεση σε κυβερνοκίνδυνο στον χρηματοπιστωτικό τομέα, είναι σημαντικό να διασφαλιστεί ότι οι όποιες ανησυχίες προσδιορίζονται στην παρούσα προειδοποίηση αποτυπώνονται στις εργασίες εποπτείας και επίβλεψης και στις θέσεις πολιτικής που εγκρίνονται από τις αρμόδιες αρχές, στο πλαίσιο των αντίστοιχων εντολών τους.

Εντός των ορίων των αντίστοιχων αρμοδιοτήτων τους, και ειδικότερα βάσει του πλαισίου που θεσπίστηκε με τον κανονισμό (ΕΕ) 2022/2554, οι αρμόδιες αρχές θα πρέπει να γνωρίζουν τις τρεις προαναφερθείσες πηγές ασυμμετρίας που εισήγαγαν τα FAIM στον χρηματοπιστωτικό τομέα. Για να μειωθούν αυτές οι ασυμμετρίες θα πρέπει, παράλληλα με τα υφιστάμενα πλαίσια δοκιμών ([11]), να εξεταστούν και ρυθμίσεις συνεργασίας και τομεακού συντονισμού. Εξάλλου, οι χρηματοπιστωτικές αρχές θα πρέπει να διασφαλίσουν την πλήρη προσήλωση των διοικητικών συμβουλίων των ιδιωτικών χρηματοοικονομικών ιδρυμάτων στον μετριασμό των κυβερνοκινδύνων με γνώμονα τα FAIM, την ύπαρξη σαφών πλαισίων διακυβέρνησης και λογοδοσίας και τον επαρκή σχεδιασμό έγκαιρων απαντήσεων, παράλληλα με τις αντίστοιχες εσωτερικές επενδύσεις.

Η λειτουργία του χρηματοπιστωτικού συστήματος και η εμπιστοσύνη σε αυτό μπορούν εν δυνάμει να επηρεαστούν από ποικίλες πιθανές εξελίξεις που εξετάζονται στην παρούσα προειδοποίηση, όπως ο συστημικός αντίκτυπος, ο γεωπολιτικός κίνδυνος ή η μεταβαλλόμενη ισορροπία μεταξύ επιτιθέμενων και αμυνόμενων. Για τη συνεχή αξιολόγηση των εξελίξεων αυτών το ΕΣΣΚ θα εξετάσει την ανάγκη αποτύπωσής τους στις εκτιμήσεις κινδύνου, στα πλαίσια διενέργειας δοκιμών, στις εποπτικές προσδοκίες και στη μελλοντική ανάπτυξη σεναρίων. Το ΕΣΣΚ θα παρακολουθεί επίσης τη χρήση και ανάπτυξη των FAIM και τον αντίκτυπό τους στον χρηματοπιστωτικό τομέα από άποψη συστημικού κινδύνου. Επιπλέον, θα επαναξιολογεί τις εξελίξεις σε κάθε τριμηνιαία εκτίμηση κινδύνου σε επίπεδο γενικού συμβουλίου και θα εξετάζει περαιτέρω δράσεις, όταν χρειάζεται.

ΤΜΗΜΑ 2

Ορισμοί

Για τους σκοπούς της παρούσας προειδοποίησης ισχύουν οι ακόλουθοι ορισμοί:

1) ως «πάροχος ΤΝ» νοείται πάροχος, όπως ορίζεται στο άρθρο 3 σημείο 3) του κανονισμού (ΕΕ) 2024/1689·

2) ως «μοντέλο ΤΝ αιχμής» νοείται προηγμένο μοντέλο ΤΝ γενικού σκοπού ικανό να επηρεάσει ουσιωδώς επιθετικές ή αμυντικές κυβερνοεπιχειρήσεις·

3) ως «κυβερνοεπίθεση» νοείται κυβερνοεπίθεση, όπως ορίζεται στο άρθρο 1 του κανονισμού (ΕΕ) 2019/796 του Συμβουλίου ([12]), μεταξύ άλλων και όταν προέρχεται από το εσωτερικό της Ένωσης·

4) ως «ευπάθεια» νοείται ευπάθεια, όπως ορίζεται στο άρθρο 3 σημείο 16) του κανονισμού (ΕΕ) 2022/2554·

5) ως «exploit» νοείται εργαλείο, τεχνική ή μέθοδος που χρησιμοποιείται για την εκμετάλλευση μίας ή περισσότερων ευπαθειών με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα, την τροποποίηση ή διατάραξή τους ή, άλλως, για την πρόκληση κινδύνου ΤΠΕ ή συμβάντων που σχετίζονται με τις ΤΠΕ·

6) ως «χρήση exploit ως όπλων» νοείται η εκπόνηση ή προσαρμογή exploit που καθιστά δυνατή τη συστηματική ή κλιμακωτή εκμετάλλευση ευπαθειών·

7) ως «κρίσιμη ή σημαντική λειτουργία» νοείται κρίσιμη ή σημαντική λειτουργία, όπως ορίζεται στο άρθρο 3 σημείο 22) του κανονισμού (ΕΕ) 2022/2554·

8) ως «μοντέλο ΤΝ γενικού σκοπού» νοείται μοντέλο ΤΝ γενικού σκοπού, όπως ορίζεται στο άρθρο 3 σημείο 63) του κανονισμού (ΕΕ) 2024/1689·

9) ως «μοντέλο ΤΝ γενικού σκοπού με συστημικό κίνδυνο» νοείται μοντέλο ΤΝ γενικού σκοπού, το οποίο ταξινομείται ως μοντέλο που παρουσιάζει συστημικό κίνδυνο σύμφωνα με το άρθρο 51 παράγραφος 1 του κανονισμού (ΕΕ) 2024/1689·

10) ως «συμβάν που σχετίζεται με τις ΤΠΕ» νοείται συμβάν, όπως ορίζεται στο άρθρο 3 σημείο 8) του κανονισμού (ΕΕ) 2022/2554·

([10]) Βλέπε έγγραφο με τίτλο «Systemic cyber risk» (Συστημικός κίνδυνος στον κυβερνοχώρο), ΕΣΣΚ, Φεβρουάριος 2020, διαθέσιμο στον ιστότοπο του ΕΣΣΚ (www.esrb.europa.eu).

([11]) Π.χ. δοκιμές ηθικής προσομοίωσης επιθέσεων βάσει πληροφοριών για απειλές (TIBER), δοκιμές παρείσδυσης βάσει απειλών (TLPT), προηγμένες δοκιμές (ART) και προσομοιώσεις ακραίων καταστάσεων για την κυβερνοανθεκτικότητα (CyRST).

([12]) Κανονισμός (ΕΕ) 2019/796 του Συμβουλίου, της 17ης Μαΐου 2019, σχετικά με την επιβολή περιοριστικών μέτρων κατά των κυβερνοεπιθέσεων που απειλούν την Ένωση ή τα κράτη μέλη της (ΕΕ L 129 I της 17.5.2019, σ. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj).

11) ως «κίνδυνος ΤΠΕ» νοείται κίνδυνος, όπως ορίζεται στο άρθρο 3 σημείο 5) του κανονισμού (ΕΕ) 2022/2554·

12) ως «επιχειρησιακή ανθεκτικότητα» νοείται επιχειρησιακή ανθεκτικότητα, όπως ορίζεται στο άρθρο 3 σημείο 1) του κανονισμού (ΕΕ) 2022/2554·

Φρανκφούρτη, 25 Ιουνίου 2026.

Ο Προϊστάμενος της Γραμματείας του ΕΣΣΚ,
εξ ονόματος του γενικού συμβουλίου του ΕΣΣΚ,
Francesco MAZZAFERRO