ΣΥΣΤΑΣΕΙΣ

ΣΥΣΤΑΣΗ (ΕΕ) 2017/1584 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 13ης Σεπτεμβρίου 2017

για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, και ιδίως το άρθρο 292,

Εκτιμώντας τα ακόλουθα:

(1) Η χρήση των τεχνολογιών πληροφοριών και επικοινωνιών και η εξάρτηση από αυτές είναι πλέον θεμελιώδεις πτυχές σε όλους τους τομείς της οικονομικής δραστηριότητας, καθώς οι εταιρείες μας και οι πολίτες είναι πιο διασυνδεδεμένοι και αλληλεξαρτώμενοι από ποτέ, πέρα από τομείς και σύνορα. Τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ πρέπει να έχουν προετοιμασθεί καλά σε περίπτωση περιστατικού στον κυβερνοχώρο που επηρεάζει φορείς σε περισσότερα του ενός κράτη μέλη ή ακόμη και σε ολόκληρη την Ένωση, με ενδεχόμενες σοβαρές διαταραχές στην εσωτερική αγορά και ευρύτερα στα δίκτυα και στα συστήματα πληροφοριών στα οποία στηρίζεται η οικονομία, η δημοκρατία και η κοινωνία της Ένωσης.

(2) Ένα περιστατικό στον κυβερνοχώρο μπορεί να θεωρηθεί ως κρίση σε επίπεδο Ένωσης όταν η διαταραχή που προκαλεί σε ένα κράτος μέλος είναι τόσο εκτεταμένη, που υπερβαίνει τις δυνατότητες του κράτους μέλους αυτού να την αντιμετωπίσει μόνο του ή όταν το περιστατικό πλήττει δύο ή περισσότερα κράτη μέλη με τόσο ευρείες συνέπειες τεχνικής ή πολιτικής σημασίας, ώστε να απαιτείται έγκαιρος συντονισμός και αντιμετώπιση σε ενωσιακό πολιτικό επίπεδο.

(3) Τα περιστατικά στον κυβερνοχώρο μπορούν να οδηγήσουν σε ευρύτερη κρίση με συνέπειες σε τομείς δραστηριότητας πέραν των δικτύων και των συστημάτων πληροφοριών και των δικτύων επικοινωνιών· κάθε ενδεδειγμένη αντιμετώπιση πρέπει να βασίζεται σε ενέργειες μετριασμού εντός και εκτός του κυβερνοχώρου.

(4) Τα περιστατικά στον κυβερνοχώρο είναι απρόβλεπτα, συχνά εμφανίζονται και εξελίσσονται μέσα σε πολύ σύντομο χρονικό διάστημα, και, ως εκ τούτου, οι πληττόμενοι φορείς και οι αρμόδιοι φορείς αντιμετώπισης και μετριασμού των συνεπειών του περιστατικού πρέπει να συντονίζουν τη δράση τους γρήγορα. Πέραν αυτού, τα περιστατικά στον κυβερνοχώρο συχνά δεν περιορίζονται σε κάποια συγκεκριμένη γεωγραφική περιοχή και μπορούν να σημειωθούν ταυτόχρονα ή να εξαπλωθούν αμέσως σε πολλές χώρες.

(5) Η αποτελεσματική αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο σε επίπεδο ΕΕ απαιτεί ταχεία και αποτελεσματική συνεργασία μεταξύ όλων των σχετικών ενδιαφερομένων και εξαρτάται από την ετοιμότητα και τις ικανότητες κάθε κράτους μέλους, καθώς και από τη συντονισμένη και από κοινού δράση με την υποστήριξη των ικανοτήτων της Ένωσης. Η έγκαιρη και αποτελεσματική αντιμετώπιση περιστατικών εξαρτάται επομένως από ήδη υπάρχουσες και, ει δυνατόν, δοκιμασμένες διαδικασίες και μηχανισμούς συνεργασίας όπου έχουν καθορισθεί με σαφήνεια οι ρόλοι και οι ευθύνες των βασικών φορέων σε εθνικό και ενωσιακό επίπεδο.

(6) Στα συμπεράσματά του της 27ης Μαΐου 2011 ([1]) σχετικά με την προστασία των ζωτικής σημασίας υποδομών πληροφοριών το Συμβούλιο κάλεσε τα κράτη μέλη της ΕΕ «να ενισχύσουν τη συνεργασία μεταξύ κρατών μελών και να συμβάλουν, με βάση εθνικές εμπειρίες και τα αποτελέσματα στη διαχείριση κρίσεων και σε συνεργασία με τον ENISA, στην ανάπτυξη ευρωπαϊκών μηχανισμών συνεργασίας για συμβάντα στον κυβερνοχώρο, οι οποίοι να δοκιμαστούν στο πλαίσιο της προσεχούς περιόδου διεξαγωγής του CyberEurope το 2012».

(7) Η ανακοίνωση του 2016 με τίτλο «Ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο» ([2]) παρότρυνε τα κράτη μέλη να αξιοποιήσουν στο μέγιστο τους μηχανισμούς συνεργασίας που προβλέπονται στην οδηγία για την ασφάλεια δικτύων και πληροφοριών ([3]) και να ενισχύσουν τη διασυνοριακή συνεργασία για ετοιμότητα στην αντιμετώπιση περιστατικού μεγάλης κλίμακας στον κυβερνοχώρο. Προσέθετε ότι με τη συντονισμένη προσέγγιση της συνεργασίας σε περίπτωση

([1]) Συμπεράσματα του Συμβουλίου σχετικά με την προστασία κρίσιμων πληροφοριακών υποδομών με τίτλο «Επιτεύγματα και επόμενα βήματα: προς την παγκόσμια ασφάλεια στον κυβερνοχώρο», έγγραφο 10299/11, Βρυξέλλες, 27 Μαΐου 2011.

([2]) COM(2016) 410 final, 5 Ιουλίου 2016.

([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).

κρίσης στο σύνολο των διαφόρων στοιχείων του οικοσυστήματος του κυβερνοχώρου, η οποία θα έχει τη μορφή «προσχεδίου» (blueprint), θα αυξηθεί η ετοιμότητα και ότι το προσχέδιο αυτό θα πρέπει επίσης να διασφαλίζει συνέργειες και συνεκτικότητα με τους υφιστάμενους μηχανισμούς διαχείρισης κρίσεων.

(8) Στα συμπεράσματα του Συμβουλίου ([1]) σχετικά με την προαναφερόμενη ανακοίνωση τα κράτη μέλη κάλεσαν την Επιτροπή να υποβάλει το εν λόγω προσχέδιο προς εξέταση από τα όργανα και άλλα σχετικά ενδιαφερόμενα μέρη. Ωστόσο η οδηγία για την ασφάλεια δικτύων και πληροφοριών δεν προβλέπει ενωσιακό πλαίσιο συνεργασίας σε περιπτώσεις περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

(9) Η Επιτροπή διαβουλεύθηκε με τα κράτη μέλη σε δύο χωριστές ημερίδες διαβούλευσης που πραγματοποιήθηκαν στις Βρυξέλλες στις 5 Απριλίου και στις 4 Ιουλίου 2017 με εκπροσώπους των κρατών μελών από ομάδες παρέμβασης για περιστατικά που αφορούν την ασφάλεια των υπολογιστών (CSIRT), με την ομάδα συνεργασίας που έχει συσταθεί με την οδηγία για την ασφάλεια δικτύων και πληροφοριών και την οριζόντια ομάδα εργασίας του Συμβουλίου για την ασφάλεια στον κυβερνοχώρο, καθώς και με εκπροσώπους της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ), του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), της Ευρωπόλ/EC3 και της Γενικής Γραμματείας του Συμβουλίου (ΓΓΣ).

(10) Το παρόν προσχέδιο συντονισμένης αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο σε επίπεδο Ένωσης, το οποίο επισυνάπτεται στην παρούσα σύσταση, είναι το αποτέλεσμα των προαναφερόμενων διαβουλεύσεων και συμπληρώνει την ανακοίνωση με τίτλο «Ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο».

(11) Το προσχέδιο περιγράφει και καθορίζει τους στόχους και τους τρόπους συνεργασίας μεταξύ των κρατών μελών και των θεσμικών οργάνων, των φορέων και οργανισμών της Ένωσης (εφεξής «όργανα ΕΕ») για την αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο, καθώς και τον τρόπο με τον οποίο οι υπάρχοντες μηχανισμοί διαχείρισης κρίσεων μπορούν να επωφελούνται πλήρως από τους υφιστάμενους φορείς για την ασφάλεια στον κυβερνοχώρο σε επίπεδο ΕΕ.

(12) Για την αντιμετώπιση κρίσης στον κυβερνοχώρο κατά την έννοια της αιτιολογικής σκέψης 2, κατά τον συντονισμό της αντιμετώπισης σε πολιτικό ενωσιακό επίπεδο στο Συμβούλιο θα χρησιμοποιηθούν οι ολοκληρωμένες ρυθμίσεις της ΕΕ για την πολιτική αντιμετώπιση των κρίσεων (IPCR) ([2])· η Επιτροπή θα χρησιμοποιήσει την υψηλού επιπέδου διαδικασία συντονισμού διατομεακών κρίσεων ARGUS ([3]) (ασφαλές γενικό σύστημα έγκαιρης προειδοποίησης). Εάν η κρίση ενέχει σημαντική εξωτερική διάσταση ή διάσταση κοινής πολιτικής ασφαλείας και άμυνας (ΚΠΑΑ), θα ενεργοποιηθεί ο Μηχανισμός Αντιμετώπισης Κρίσεων (CRM) ([3]) της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ).

(13) Σε ορισμένα πεδία, οι τομεακοί μηχανισμοί διαχείρισης κρίσεων σε επίπεδο ΕΕ προβλέπουν συνεργασία σε περίπτωση περιστατικού ή κρίσης στον κυβερνοχώρο. Παραδείγματος χάρη, στο πλαίσιο του Ευρωπαϊκού Οργανισμού για το Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης (GNSS), η απόφαση 2014/496/ΚΕΠΠΑ του Συμβουλίου ([4]) ορίζει ήδη τους αντίστοιχους ρόλους του Συμβουλίου, της Ύπατης Εκπροσώπου, της Επιτροπής, του Ευρωπαϊκού Οργανισμού GNSS και των κρατών μελών μέσα στην αλυσίδα επιχειρησιακών ευθυνών που έχει καθορισθεί για την αντίδραση σε απειλή στην Ένωση, τα κράτη μέλη ή το GNSS, καθώς και σε περίπτωση επιθέσεων στον κυβερνοχώρο. Συνεπώς, η παρούσα σύσταση δεν θα πρέπει να θίξει αυτούς τους μηχανισμούς.

(14) Τα κράτη μέλη έχουν την πρωταρχική ευθύνη αντιμετώπισης εάν πληγούν από περιστατικά ή κρίσεις μεγάλης κλίμακας στον κυβερνοχώρο. Η Επιτροπή, η Ύπατη Εκπρόσωπος και άλλα θεσμικά όργανα ή υπηρεσίες της ΕΕ έχουν ωστόσο ένα σημαντικό ρόλο, ο οποίος απορρέει από το δίκαιο της Ένωσης ή από το γεγονός ότι περιστατικά και κρίσεις στον κυβερνοχώρο μπορούν να έχουν συνέπειες σε όλους τους τομείς της οικονομικής δραστηριότητας στην ενιαία αγορά, στην ασφάλεια και τις διεθνείς σχέσεις της Ένωσης, καθώς και στα ίδια τα θεσμικά όργανα.

(15) Σε επίπεδο Ένωσης, στους βασικούς παράγοντες που εμπλέκονται στην αντιμετώπιση κρίσεων στον κυβερνοχώρο περιλαμβάνονται οι δομές και οι μηχανισμοί της οδηγίας για την ασφάλεια δικτύων και πληροφοριών που συστάθηκαν πρόσφατα, και συγκεκριμένα οι ομάδες παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT), όπως και οι σχετικοί οργανισμοί και φορείς, ήτοι ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο στο πλαίσιο της Ευρωπόλ (Ευρωπόλ/EC3), το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (INTCEN), η Διεύθυνση Πληροφοριών του Στρατιωτικού Επιτελείου της ΕΕ (EUMS INT) και την Αίθουσα Διαχείρισης Κρίσεων (SITROOM), που συνεργάζονται στο πλαίσιο της SIAC (Ενιαία Ικανότητα Ανάλυσης Πληροφοριών), η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ (με έδρα το INTCEN), η ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα της ΕΕ (CERT-ΕΕ) και το Κέντρο Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών στην Ευρωπαϊκή Επιτροπή.

(16) Η συνεργασία μεταξύ των κρατών μελών σε τεχνικό επίπεδο στην αντιμετώπιση περιστατικών στον κυβερνοχώρο προβλέπεται μέσω του δικτύου CSIRT που έχει συσταθεί με την οδηγία για την ασφάλεια δικτύων και πληροφοριών. Ο

([1]) Έγγραφο 14540/16, 15 Νοεμβρίου 2016.
([2]) Για περισσότερες πληροφορίες, μπορείτε να ανατρέξετε στο τμήμα 3.1 του προσαρτήματος σχετικά με τη διαχείριση κρίσεων, τους μηχανισμούς συνεργασίας και παράγοντες σε επίπεδο ΕΕ.
([3]) Ομοίως.
([4]) Απόφαση 2014/496/ΚΕΠΠΑ του Συμβουλίου, της 22ας Ιουλίου 2014, σχετικά με ορισμένες πτυχές της εγκατάστασης, λειτουργίας και χρήσης του ευρωπαϊκού παγκόσμιου δορυφορικού συστήματος πλοήγησης που επηρεάζουν την ασφάλεια της Ευρωπαϊκής Ένωσης και την κατάργηση της κοινής δράσης 2004/552/ΚΕΠΠΑ (ΕΕ L 219 της 25.7.2014, σ. 53).

ENISA καλύπτει τη γραμματειακή υποστήριξη του δικτύου και υποστηρίζει δραστήρια τη συνεργασία μεταξύ των CSIRT. Οι εθνικές CSIRT και η CERT-ΕΕ συνεργάζονται και ανταλλάσσουν πληροφορίες σε εθελοντική βάση και, όταν είναι αναγκαίο, σε περίπτωση περιστατικών στον κυβερνοχώρο που πλήττουν ένα ή περισσότερα κράτη μέλη. Μετά από αίτημα αντιπροσώπου CSIRT κράτους μέλους, συζητούν και, ει δυνατόν, καθορίζουν συντονισμένη αντιμετώπιση περιστατικού που έχει εντοπισθεί εντός της δικαιοδοσίας του συγκεκριμένου κράτους μέλους. Σχετικές διαδικασίες θα καθοριστούν στις τυποποιημένες επιχειρησιακές διαδικασίες λειτουργίας του δικτύου της CSIRT (SOP) ([1]).

(17) Το δίκτυο CSIRT έχει επιφορτισθεί επίσης με τη συζήτηση, τη διερεύνηση και τον καθορισμό και άλλων μορφών επιχειρησιακής συνεργασίας, μεταξύ άλλων σχετικά με τις κατηγορίες κινδύνων και περιστατικών, την έγκαιρη προειδοποίηση, την αμοιβαία συνδρομή, τις αρχές και τους τρόπους συντονισμού, όταν τα κράτη μέλη αντιμετωπίζουν διασυνοριακούς κινδύνους και περιστατικά.

(18) Η ομάδα συνεργασίας που έχει συσταθεί με το άρθρο 11 της οδηγίας για την ασφάλεια δικτύων και πληροφοριών έχει αναλάβει να παρέχει στρατηγική καθοδήγηση για τις δραστηριότητες του δικτύου CSIRT και να συζητεί τις ικανότητες και την ετοιμότητα των κρατών μελών και, σε εθελούσια βάση, να αξιολογεί τις εθνικές στρατηγικές για την ασφάλεια συστημάτων δικτύων και πληροφοριών και την αποτελεσματικότητα των CSIRT, και να προσδιορίζει βέλτιστες πρακτικές.

(19) Ειδικός άξονας εργασίας της ομάδας συνεργασίας είναι η εκπόνηση κατευθυντήριων γραμμών για την κοινοποίηση περιστατικών, δυνάμει του άρθρου 14 παράγραφος 7 της οδηγίας για την ασφάλεια δικτύων και πληροφοριών, σχετικά με τις συνθήκες υπό τις οποίες οι φορείς εκμετάλλευσης βασικών υπηρεσιών είναι υποχρεωμένοι να κοινοποιούν περιστατικά σύμφωνα με το άρθρο 14 παράγραφος 3 και με τη μορφή και τη διαδικασία των εν λόγω κοινοποιήσεων ([2]).

(20) Η επίγνωση και η κατανόηση της κατάστασης σε πραγματικό χρόνο, του σημείου του κινδύνου και των απειλών, που έχουν αποκτηθεί με την υποβολή εκθέσεων, τις αξιολογήσεις, την έρευνα, τη διερεύνηση και την ανάλυση, είναι ζωτικής σημασίας για να καταστεί δυνατή η λήψη εμπεριστατωμένων αποφάσεων. Η εν λόγω «επίγνωση της κατάστασης» —από όλα τα ενδιαφερόμενα μέρη— είναι ουσιώδους σημασίας για αποτελεσματική και συντονισμένη αντιμετώπιση. Η επίγνωση της κατάστασης περιλαμβάνει στοιχεία σχετικά με τα αίτια, καθώς και με τις συνέπειες και την προέλευση του περιστατικού. Αναγνωρίζεται ότι αυτό εξαρτάται από την ανταλλαγή και τη γνωστοποίηση πληροφοριών σε κατάλληλο μορφότυπο μεταξύ των ενδιαφερόμενων μερών, με τη χρήση κοινής ταξονομίας για την περιγραφή του περιστατικού με τον ενδεδειγμένο ασφαλή τρόπο.

(21) Η αντιμετώπιση περιστατικών στον κυβερνοχώρο μπορεί να λάβει πολλές μορφές, από τον καθορισμό τεχνικών μέτρων στα οποία ενδεχομένως συμμετέχουν δύο ή περισσότερες οντότητες για την από κοινού διερεύνηση των τεχνικών αιτίων του περιστατικού (π.χ. ανάλυση κακόβουλου λογισμικού) ή για τον προσδιορισμό των τρόπων με τους οποίους οι οργανισμοί μπορούν να αξιολογούν αν έχουν πληγεί (π.χ. δείκτες συμβιβασμού) έως αποφάσεις επιχειρησιακού χαρακτήρα με αντικείμενο την εφαρμογή αυτών των μέτρων και, σε πολιτικό επίπεδο, λήψη απόφασης σχετικά με τη χρήση άλλων μέσων, όπως το πλαίσιο κοινής αντιμετώπισης κακόβουλων δραστηριοτήτων στον κυβερνοχώρο ([3]) ή το επιχειρησιακό πρωτόκολλο για την αντιμετώπιση υβριδικών απειλών ([4]), αναλόγως του περιστατικού.

(22) Η εμπιστοσύνη των ευρωπαίων πολιτών και των ευρωπαϊκών επιχειρήσεων στις ψηφιακές υπηρεσίες έχει ζωτική σημασία για μια ακμάζουσα ψηφιακή ενιαία αγορά. Συνεπώς, η επικοινωνία σε καταστάσεις κρίσης διαδραματίζει ιδιαίτερα σημαντικό ρόλο στον μετριασμό των αρνητικών συνεπειών των περιστατικών και κρίσεων στον κυβερνοχώρο. Η επικοινωνία μπορεί επίσης να χρησιμοποιείται στο πλαίσιο για κοινή διπλωματική αντίδραση ως μέσο επίδρασης στη συμπεριφορά των (εν δυνάμει) δραστών που ενεργούν από τρίτες χώρες. Η ευθυγράμμιση της επικοινωνίας με το κοινό για τον μετριασμό των αρνητικών συνεπειών περιστατικών και κρίσεων στον κυβερνοχώρο και της επικοινωνίας με το κοινό για να επηρεασθεί η συμπεριφορά των δραστών είναι απαραίτητη ώστε να είναι αποτελεσματική η αντιμετώπιση από πλευράς πολιτικής.

(23) Η παροχή πληροφοριών στο κοινό σχετικά με τον τρόπο που είναι δυνατόν να μετριασθούν οι συνέπειες περιστατικού σε επίπεδο χρήστη και οργάνωσης [π.χ. με λογισμικό ενημέρωσης (και διόρθωσης) ή συμπληρωματικές δράσεις για την αποτροπή απειλής κ.λπ.] θα μπορούσε να είναι αποτελεσματικό μέτρο για τον μετριασμό περιστατικού και κρίσης μεγάλης κλίμακας στον κυβερνοχώρο.

(24) Η Επιτροπή, μέσω της υποδομής ψηφιακών υπηρεσιών για την ασφάλεια στον κυβερνοχώρο του μηχανισμού «Συνδέοντας την Ευρώπη» (ΔΣΕ), αναπτύσσει έναν μηχανισμό συνεργασίας στη βασική πλατφόρμα υπηρεσιών, γνωστό ως MeliCERTes, μεταξύ των ομάδων CSIRT κρατών μελών που συμμετέχουν, για να βελτιώσουν το επίπεδο των ικανοτήτων τους στην ετοιμότητα, τη συνεργασία και την αντιμετώπιση αναδυόμενων απειλών και περιστατικών στον κυβερνοχώρο. Η Επιτροπή, μέσω ανταγωνιστικών προσκλήσεων υποβολής προτάσεων για επιχορηγήσεις στο πλαίσιο της ΔΣΕ συγχρηματοδοτεί τις CSIRT στα κράτη μέλη με σκοπό να βελτιωθεί η επιχειρησιακή τους ικανότητα σε εθνικό επίπεδο.

([1]) Υπό εκπόνηση· αναμένεται να εγκριθούν έως τα τέλη του 2017.
([2]) Οι κατευθυντήριες γραμμές πρόκειται να οριστικοποιηθούν έως τα τέλη του 2017.
([3]) Συμπεράσματα του Συμβουλίου σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»), έγγρ. 9916/17.
([4]) Κοινό έγγραφο εργασίας των υπηρεσιών με τίτλο κοινό ενωσιακό επιχειρησιακό πρωτόκολλο αντιμετώπισης υβριδικών απειλών, «Εγχειρίδιο ΕΕ», SWD(2016) 227 final, 5 Ιουλίου 2016.

(25) Οι ασκήσεις ασφάλειας στον κυβερνοχώρο σε επίπεδο ΕΕ είναι ζωτικής σημασίας για την προσομοίωση και τη βελτίωση της συνεργασίας μεταξύ των κρατών μελών και του ιδιωτικού τομέα. Προς τον σκοπό αυτό, από το 2010 ο ENISA διοργανώνει τακτικές πανευρωπαϊκές ασκήσεις ασφάλειας στον κυβερνοχώρο («Cyber Europe»).

(26) Το Συμβούλιο στα συμπεράσματά του ([1]) σχετικά με την εφαρμογή της κοινής δήλωσης του προέδρου του Ευρωπαϊκού Συμβουλίου, του προέδρου της Ευρωπαϊκής Επιτροπής και του γενικού γραμματέα του Οργανισμού του Βορειοατλαντικού Συμφώνου κάνει έκκληση για ενίσχυση της συνεργασίας σε ασκήσεις στον κυβερνοχώρο με τη συμμετοχή των μελών του προσωπικού των προαναφερόμενων σε αντίστοιχες ασκήσεις, όπως ιδίως και στη Cyber Coalition και τη Cyber Europe.

(27) Το συνεχώς εξελισσόμενο τοπίο των απειλών και τα πρόσφατα περιστατικά στον κυβερνοχώρο αποτελούν ένδειξη ότι αυξάνεται ο κίνδυνος που αντιμετωπίζει η Ένωση, και τα κράτη μέλη θα πρέπει να λάβουν μέτρα με βάση την παρούσα σύσταση χωρίς περαιτέρω καθυστέρηση και ούτως ή άλλως μέχρι τα τέλη του 2018,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΣΤΑΣΗ:

1) Τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ πρέπει να καθορίσουν ένα πλαίσιο της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο, το οποίο θα περιέχει τους στόχους και τους τρόπους συνεργασίας που παρουσιάζονται στο προσχέδιο σύμφωνα με τις κατευθυντήριες αρχές που περιγράφονται στο εν λόγω προσχέδιο.

2) Συγκεκριμένα, το πλαίσιο της ΕΕ για την αντιμετώπιση κρίσεων στον κυβερνοχώρο πρέπει να προσδιορίζει τους σχετικούς παράγοντες, τα θεσμικά όργανα της ΕΕ και τις αρχές των κρατών μελών, σε όλα τα απαραίτητα επίπεδα —τεχνικό, επιχειρησιακό, στρατηγικό/πολιτικό—, και να αναπτύσσει, εφόσον απαιτείται, τυποποιημένες διαδικασίες λειτουργίας που καθορίζουν τον τρόπο συνδυασμού τους με τους μηχανισμούς διαχείρισης κρίσεων της ΕΕ. Πρέπει να δοθεί έμφαση στην ενθάρρυνση της ανταλλαγής πληροφοριών χωρίς αδικαιολόγητη καθυστέρηση και στον συντονισμό της αντιμετώπισης περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο.

3) Προς τον σκοπό αυτό, οι αρμόδιες αρχές των κρατών μελών θα πρέπει να εργασθούν από κοινού για την περαιτέρω εξειδίκευση πρωτοκόλλων ανταλλαγής πληροφοριών και συνεργασίας. Η ομάδα συνεργασίας θα πρέπει να ανταλλάσσει εμπειρίες στα θέματα αυτά με τα σχετικά θεσμικά όργανα της ΕΕ.

4) Τα κράτη μέλη θα πρέπει να διασφαλίσουν ότι οι εθνικοί τους μηχανισμοί διαχείρισης κρίσεων παρέχουν επαρκή αντιμετώπιση περιστατικών στον κυβερνοχώρο, όπως και ότι προβλέπουν τις αναγκαίες διαδικασίες συνεργασίας σε επίπεδο ΕΕ εντός του πλαισίου της ΕΕ.

5) Όσον αφορά τους υπάρχοντες μηχανισμούς διαχείρισης κρίσεων της ΕΕ, σύμφωνα με το προσχέδιο, τα κράτη μέλη θα πρέπει, μαζί με τις υπηρεσίες της Επιτροπής και την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ), να ορίσουν πρακτικές κατευθυντήριες γραμμές εφαρμογής όσον αφορά την ένταξη των εθνικών τους φορέων διαχείρισης κρίσεων και της ασφάλειας στον κυβερνοχώρο και των διαδικασιών τους στους υπάρχοντες μηχανισμούς διαχείρισης κρίσεων της ΕΕ, και συγκεκριμένα στις IPCR και ΕΥΕΔ CRM. Ειδικότερα, τα κράτη μέλη θα πρέπει να μεριμνήσουν για τη θέση σε εφαρμογή κατάλληλων δομών που να επιτρέπουν την αποτελεσματική ροή πληροφοριών μεταξύ των εθνικών τους αρχών διαχείρισης κρίσεων και των αντιπροσώπων τους σε επίπεδο ΕΕ στους ευρωπαϊκούς μηχανισμούς αντιμετώπισης κρίσεων.

6) Τα κράτη μέλη θα πρέπει να αξιοποιήσουν πλήρως τις δυνατότητες που προσφέρει το πρόγραμμα της υποδομής ψηφιακών υπηρεσιών για την ασφάλεια στον κυβερνοχώρο (DSI) του μηχανισμού «Συνδέοντας την Ευρώπη» (ΔΣΕ) και να συνεργάζονται με την Επιτροπή ώστε να διασφαλισθεί ότι ο μηχανισμός συνεργασίας στη βασική πλατφόρμα υπηρεσιών που διαθέτει έχει τις απαραίτητες λειτουργίες και πληροί τις σχετικές απαιτήσεις συνεργασίας ακόμη και κατά τη διάρκεια κρίσεων στον κυβερνοχώρο.

7) Τα κράτη μέλη, με τη συνδρομή του ENISA και στηριζόμενα σε προηγούμενες εργασίες στο πεδίο αυτό, πρέπει να συνεργάζονται για την κατάρτιση και τον καθορισμό κοινής ταξονομίας και μορφότυπου υποβολής περιπτωσιολογικών αναφορών που θα περιγράφουν τα τεχνικά αίτια και τις συνέπειες περιστατικών στον κυβερνοχώρο, για περαιτέρω ενίσχυση της τεχνικής και επιχειρησιακής συνεργασίας κατά τη διάρκεια κρίσεων. Εν προκειμένω, τα κράτη μέλη θα πρέπει να λάβουν υπόψη τις εργασίες της ομάδας συνεργασίας σχετικά με κατευθυντήριες γραμμές κοινοποίησης περιστατικών, και ιδίως τις πτυχές που σχετίζονται με τον μορφότυπο των εθνικών κοινοποιήσεων.

8) Οι διαδικασίες που καθορίζονται στο πλαίσιο θα πρέπει να τίθενται σε δοκιμή και, όταν χρειάζεται, να αναθεωρούνται με βάση τα διδάγματα που αντλούνται από τη συμμετοχή των κρατών μελών στις εθνικές, περιφερειακές και ενωσιακές ασκήσεις ασφάλειας στον κυβερνοχώρο, όπως και στις ασκήσεις ασφάλειας στον κυβερνοχώρο της διπλωματίας και του ΝΑΤΟ. Ειδικότερα, θα πρέπει να τεθούν σε δοκιμή στις ασκήσεις CyberEurope που οργανώνει ο ENISA. Η CyberEurope 2018 παρουσιάζει μια πρώτη τέτοια ευκαιρία.

([1]) Έγγραφο ST 15283/16, 6 Δεκεμβρίου 2016.

9) Τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ πρέπει να εξετάζουν τακτικά στην πράξη την αντιμετώπιση κρίσεων μεγάλης κλίμακας περιστατικών στον κυβερνοχώρο, σε εθνικό και ευρωπαϊκό επίπεδο, καθώς και την πολιτική αντίδρασή τους, εφόσον είναι απαραίτητο και με τη συμμετοχή του ιδιωτικού τομέα αν ενδείκνυται.

Βρυξέλλες, 13 Σεπτεμβρίου 2017.

Για την Επιτροπή
Mariya GABRIEL
Μέλος της Επιτροπής

ΠΑΡΑΡΤΗΜΑ

Προσχέδιο συντονισμένης αντιμετώπισης διασυνοριακών περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο

ΕΙΣΑΓΩΓΗ

Το παρόν προσχέδιο (blueprint) αφορά περιστατικά στον κυβερνοχώρο τα οποία προκαλούν διαταραχή εξαιρετικά εκτεταμένη σε κάποιο κράτος μέλος για να μπορεί να την αντιμετωπίσει μόνο του ή τα οποία πλήττουν δύο ή περισσότερα κράτη μέλη ή θεσμικά όργανα της ΕΕ με τόσο ευρείες συνέπειες τεχνικής ή πολιτικής σημασίας, ώστε να απαιτείται έγκαιρος συντονισμός της πολιτικής και αντιμετώπιση σε ενωσιακό πολιτικό επίπεδο.

Αυτά τα περιστατικά μεγάλης κλίμακας στον κυβερνοχώρο θεωρούνται ως «κρίση» ασφάλειας στον κυβερνοχώρο.

Σε περίπτωση κρίσης ενωσιακής εμβέλειας που ενέχει στοιχεία σχετικά με τον κυβερνοχώρο, ο συντονισμός της αντιμετώπισης σε ενωσιακό πολιτικό επίπεδο διενεργείται από το Συμβούλιο, με χρήση ολοκληρωμένων ρυθμίσεων για την αντιμετώπιση πολιτικών κρίσεων (IPCR).

Εντός της Επιτροπής, ο συντονισμός θα πραγματοποιείται σύμφωνα με το σύστημα έγκαιρης προειδοποίησης ARGUS.

Εάν η κρίση ενέχει σημαντική εξωτερική διάσταση ή διάσταση κοινής πολιτικής ασφαλείας και άμυνας (ΚΠΑΑ), ενεργοποιείται ο μηχανισμός αντιμετώπισης κρίσεων της ΕΥΕΔ.

Το προσχέδιο περιγράφει τον τρόπο με τον οποίο οι παγιωμένοι μηχανισμοί διαχείρισης κρίσεων θα πρέπει να αξιοποιούν πλήρως τους υφιστάμενους φορείς για την ασφάλεια στον κυβερνοχώρο σε επίπεδο ΕΕ, καθώς και τους μηχανισμούς συνεργασίας μεταξύ των κρατών μελών.

Προς τον σκοπό αυτό, το προσχέδιο λαμβάνει υπόψη ένα σύνολο κατευθυντήριων αρχών (αναλογικότητα, επικουρικότητα, συμπληρωματικότητα και εμπιστευτικότητα των πληροφοριών), παρουσιάζει τους βασικούς στόχους της συνεργασίας (αποτελεσματική αντίδραση, κοινή επίγνωση της κατάστασης, μηνύματα επικοινωνίας με το κοινό) σε τρία επίπεδα (στρατηγικό/πολιτικό, επιχειρησιακό και τεχνικό), τους σχετικούς μηχανισμούς και τους εμπλεκόμενους παράγοντες, καθώς και τις δραστηριότητες για την επίτευξη των εν λόγω βασικών στόχων.

Το προσχέδιο δεν καλύπτει ολόκληρο το φάσμα του κύκλου ζωής της διαχείρισης κρίσεων (πρόληψη/μετριασμός, ετοιμότητα, αντιμετώπιση, αποκατάσταση), αλλά επικεντρώνεται στην αντιμετώπιση. Παρ' όλα αυτά, καλύπτει και ορισμένες δραστηριότητες όπως, ιδίως, εκείνες που συνδέονται με την επίτευξη κοινής επίγνωσης της κατάστασης.

Είναι επίσης σημαντικό να σημειωθεί ότι τα περιστατικά στον κυβερνοχώρο μπορεί να αποτελέσουν πηγή ή μέρος ευρύτερης κρίσης, με επιπτώσεις σε άλλους τομείς. Δεδομένου ότι οι περισσότερες κρίσεις στον κυβερνοχώρο αναμένεται να έχουν επιπτώσεις στον υλικό κόσμο, κάθε ενδεδειγμένη αντιμετώπιση πρέπει να βασίζεται σε δραστηριότητες μετριασμού τόσο εντός όσο και εκτός του κυβερνοχώρου. Οι δραστηριότητες αντιμετώπισης κρίσεων στον κυβερνοχώρο θα πρέπει να συντονίζονται με άλλους μηχανισμούς διαχείρισης κρίσεων σε ενωσιακό, εθνικό ή τομεακό επίπεδο.

Τέλος, το προσχέδιο δεν αντικαθιστά ούτε πρέπει να θίγει υφιστάμενους ειδικούς ανά τομέα ή πολιτική μηχανισμούς, ρυθμίσεις ή μέσα, όπως εκείνο που συστάθηκε για το πρόγραμμα του ευρωπαϊκού παγκόσμιου δορυφορικού συστήματος πλοήγησης (GNSS) ([1]).

Κατευθυντήριες αρχές

Για τον καθορισμό των στόχων, τον προσδιορισμό των αναγκαίων δραστηριοτήτων και την ανάθεση των ρόλων και αρμοδιοτήτων στους αντίστοιχους παράγοντες ή μηχανισμούς, εφαρμόστηκαν οι ακόλουθες *κατευθυντήριες αρχές*, οι οποίες θα πρέπει επίσης να τηρηθούν για την κατάρτιση μελλοντικών κατευθυντήριων γραμμών εφαρμογής.

Αναλογικότητα: στη μεγάλη πλειονότητά τους τα περιστατικά στον κυβερνοχώρο που πλήττουν τα κράτη μέλη κάθε άλλο παρά εθνική «κρίση» —και πόσο μάλλον ευρωπαϊκή— μπορούν να θεωρηθούν. Το δίκτυο ομάδων παρέμβασης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT), το οποίο συστάθηκε με την οδηγία NIS ([2]), αποτελεί τη βάση της συνεργασίας μεταξύ των κρατών μελών για την αντιμετώπιση των εν λόγω περιστατικών. Οι εθνικές ομάδες CSIRT συνεργάζονται και ανταλλάσσουν οικειοθελώς πληροφορίες σε καθημερινή βάση, μεταξύ άλλων, όταν είναι αναγκαίο, για την αντιμετώπιση περιστατικών στον κυβερνοχώρο που πλήττουν ένα ή περισσότερα κράτη μέλη σύμφωνα με τις τυποποιημένες επιχειρησιακές διαδικασίες (SOP) του δικτύου CSIRT. Κατά συνέπεια, το προσχέδιο θα πρέπει να κάνει πλήρη χρήση των εν λόγω τυποποιημένων επιχειρησιακών διαδικασιών, τις οποίες και θα συμπληρώσει με όλα τα πρόσθετα ειδικά καθήκοντα αντιμετώπισης κρίσης στον κυβερνοχώρο.

([1]) Απόφαση 2014/496/ΚΕΠΠΑ.
([2]) Οδηγία (ΕΕ) 2016/1148.

Επικουρικότητα: καθοριστική σημασία έχει η αρχή της επικουρικότητας. Τα κράτη μέλη έχουν την πρωταρχική ευθύνη αντιμετώπισης εάν πληγούν από περιστατικά ή κρίσεις μεγάλης κλίμακας στον κυβερνοχώρο. Ωστόσο, σημαντικός είναι και ο ρόλος της Επιτροπής, της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης και άλλων θεσμικών και λοιπών οργάνων, υπηρεσιών και οργανισμών της ΕΕ. Ο ρόλος αυτός καθορίζεται με σαφήνεια στις ολοκληρωμένες ρυθμίσεις ΕΕ για την αντιμετώπιση πολιτικών κρίσεων, αλλά απορρέει επίσης από το ενωσιακό δίκαιο ή απλώς από το γεγονός ότι τα περιστατικά και οι κρίσεις στον κυβερνοχώρο ενδέχεται να επηρεάσουν όλους τους τομείς της οικονομικής δραστηριότητας εντός της ενιαίας αγοράς, την ασφάλεια και τις διεθνείς σχέσεις της Ένωσης, καθώς και τα ίδια τα θεσμικά όργανα.

Συμπληρωματικότητα: το προσχέδιο λαμβάνει πλήρως υπόψη τους υφιστάμενους μηχανισμούς διαχείρισης κρίσεων σε επίπεδο ΕΕ, και συγκεκριμένα τις ολοκληρωμένες ρυθμίσεις για την αντιμετώπιση πολιτικών κρίσεων (IPCR), το ARGUS και τον μηχανισμό αντιμετώπισης κρίσεων της ΕΥΕΔ, ενσωματώνει τις δομές και τους μηχανισμούς της νέας οδηγίας NIS, δηλαδή το δίκτυο των CSIRT, καθώς και τα σχετικά όργανα και οργανισμούς, ήτοι τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο, στο πλαίσιο της Ευρωπόλ (Ευρωπόλ/EC3), το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (INTCEN), τη Διεύθυνση Πληροφοριών του Στρατιωτικού Επιτελείου της ΕΕ (EUMS INT) και την Αίθουσα Διαχείρισης Κρίσεων (SITROOM) στο INTCEN, που συνεργάζονται στο πλαίσιο της SIAC (Ενιαία Ικανότητα Ανάλυσης Πληροφοριών)· τη Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ (με έδρα στο INTCEN)· και την ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ (CERT-EU). Στο πλαίσιο αυτό, το προσχέδιο θα πρέπει επίσης να εξασφαλίζει ότι επιτυγχάνεται μέγιστη συμπληρωματικότητα και ελάχιστη επικάλυψη στην αλληλεπίδραση και τη συνεργασία μεταξύ των μηχανισμών αυτών.

Εμπιστευτικότητα των πληροφοριών: όλες οι ανταλλαγές πληροφοριών στο πλαίσιο του προσχεδίου πρέπει να συμμορφώνονται με τους εφαρμοστέους κανόνες για την ασφάλεια ([1]), την προστασία των δεδομένων προσωπικού χαρακτήρα και το πρωτόκολλο για την ανταλλαγή πληροφοριών «Traffic Light» ([2]). Για την ανταλλαγή διαβαθμισμένων πληροφοριών, ανεξάρτητα από το εφαρμοζόμενο σύστημα διαβάθμισης, πρέπει να χρησιμοποιούνται διαθέσιμα διαπιστευμένα εργαλεία ([3]). Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα τηρεί τους εφαρμοστέους κανόνες της ΕΕ, ιδίως τον γενικό κανονισμό για την προστασία δεδομένων ([4]), την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ([5]), καθώς και τον κανονισμό ([6])«για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και τα λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών».

Βασικοί στόχοι

Η συνεργασία στο πλαίσιο του προσχεδίου ακολουθεί την προαναφερόμενη προσέγγιση τριών επιπέδων: πολιτικό, επιχειρησιακό και τεχνικό. Σε κάθε επίπεδο η συνεργασία μπορεί να περιλαμβάνει την ανταλλαγή πληροφοριών, καθώς και κοινές δράσεις, και αποσκοπεί στην επίτευξη των εξής βασικών στόχων.

— Παροχή δυνατότητας αποτελεσματικής αντίδρασης: η αντιμετώπιση μπορεί να λάβει πολλές μορφές, από τον καθορισμό τεχνικών μέτρων στα οποία ενδεχομένως συμμετέχουν δύο ή περισσότερες οντότητες για την από κοινού διερεύνηση των τεχνικών αιτίων του περιστατικού (π.χ. ανάλυση κακόβουλου λογισμικού) ή για τον προσδιορισμό των τρόπων με τους οποίους οι οργανισμοί μπορούν να αξιολογούν αν έχουν πληγεί (π.χ. δείκτες συμβιβασμού) έως αποφάσεις επιχειρησιακού χαρακτήρα με αντικείμενο την εφαρμογή των τεχνικών αυτών μέτρων και, σε πολιτικό επίπεδο, λήψη απόφασης για την ενεργοποίηση άλλων μέσων, όπως η διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο») ή το επιχειρησιακό πρωτόκολλο της ΕΕ για την αντιμετώπιση υβριδικών απειλών, αναλόγως του περιστατικού.

— Κοινή επίγνωση της κατάστασης: ουσιώδη σημασία για να υπάρξει συντονισμένη αντιμετώπιση έχει η επαρκώς καλή κατανόηση των γεγονότων καθώς εκτυλίσσονται από όλα τα ενδιαφερόμενα μέρη και στα τρία επίπεδα (τεχνικό, επιχειρησιακό, πολιτικό). Στην επίγνωση της κατάστασης μπορεί να περιλαμβάνονται τεχνολογικά στοιχεία σχετικά με τα αίτια, καθώς και τον αντίκτυπο και την πηγή του περιστατικού. Δεδομένου ότι τα περιστατικά στον κυβερνοχώρο μπορεί να επηρεάσουν ένα ευρύ φάσμα τομέων (χρηματοοικονομικά, ενέργεια, μεταφορές, υγεία κ.λπ.), είναι επιτακτική ανάγκη οι κατάλληλες πληροφορίες, στην κατάλληλη μορφή, να περιέρχονται εγκαίρως σε όλα τα σχετικά ενδιαφερόμενα μέρη.

([1]) Απόφαση (ΕΕ, Ευρατόμ) 2015/443 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με την ασφάλεια στην Επιτροπή (ΕΕ L 72 της 17.3.2015, σ. 41) και απόφαση (ΕΕ, Ευρατόμ) 2015/444 της Επιτροπής, της 13ης Μαρτίου 2015, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 72 της 17.3.2015, σ. 53)· απόφαση της Ύπατης Εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφάλειας, της 19ης Απριλίου 2013, σχετικά με τους κανόνες ασφάλειας για την Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΕ C 190 της 29.6.2013, σ. 1)· απόφαση 2013/488/ΕΕ του Συμβουλίου, της 23ης Σεπτεμβρίου 2013, σχετικά με τους κανόνες ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών της ΕΕ (ΕΕ L 274 της 15.10.2013, σ. 1).

([2]) https://www.first.org/tlp/

([3]) Τον Ιούνιο του 2016 αυτοί οι δίαυλοι μετάδοσης περιλάμβαναν το CIMS (Classified Information Management System — Σύστημα διαχείρισης διαβαθμισμένων πληροφοριών), τον ACID (αλγόριθμο κρυπτογράφησης), το RUE (ασφαλές σύστημα για τη δημιουργία, την ανταλλαγή και την αποθήκευση εγγράφων με διαβάθμιση RESTREINT UE / EU RESTRICTED) και το SOLAN. Άλλα μέσα διαβίβασης διαβαθμισμένων πληροφοριών είναι π.χ. το PGP ή το S/MIME.

([4]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

([5]) Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

([6]) Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1) —υπό επανεξέταση.

— Συμφωνία σχετικά με βασικά μηνύματα επικοινωνίας με το κοινό ([1]): η επικοινωνία σε καταστάσεις κρίσης διαδραματίζει σημαντικό ρόλο στον μετριασμό των αρνητικών συνεπειών των περιστατικών και κρίσεων στον κυβερνοχώρο, αλλά μπορεί επίσης να χρησιμοποιηθεί ως μέσο επίδρασης στη συμπεριφορά των (εν δυνάμει) δραστών. Με ένα κατάλληλο μήνυμα, που είναι σαφές ως προς τις πιθανές συνέπειες της διπλωματικής αντίδρασης μπορεί επίσης να επηρεαστεί η συμπεριφορά των δραστών. Η ευθυγράμμιση της επικοινωνίας με το κοινό για τον μετριασμό των αρνητικών συνεπειών περιστατικών και κρίσεων στον κυβερνοχώρο και της επικοινωνίας με το κοινό για να επηρεαστεί η συμπεριφορά των δραστών είναι απαραίτητη ώστε να είναι αποτελεσματική η αντιμετώπιση από πλευράς πολιτικής. Ιδιαίτερα σημαντική στον τομέα της ασφάλειας στον κυβερνοχώρο είναι η διάδοση ακριβών και αξιοποιήσιμων πληροφοριών για τον τρόπο με τον οποίο μπορεί το κοινό να μετριάσει τις συνέπειες ενός περιστατικού (π.χ. με εφαρμογή προγράμματος διόρθωσης, λήψη συμπληρωματικών μέτρων για την αποτροπή απειλής κ.λπ.).

ΣΥΝΕΡΓΑΣΙΑ ΜΕΤΑΞΥ ΚΡΑΤΩΝ ΜΕΛΩΝ, ΚΑΙ ΜΕΤΑΞΥ ΚΡΑΤΩΝ ΜΕΛΩΝ ΚΑΙ ΦΟΡΕΩΝ ΤΗΣ ΕΕ ΣΕ ΤΕΧΝΙΚΟ, ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΚΑΙ ΣΤΡΑΤΗΓΙΚΟ/ΠΟΛΙΤΙΚΟ ΕΠΙΠΕΔΟ

Η αποτελεσματική αντιμετώπιση μεγάλης κλίμακας περιστατικών ασφάλειας ή κρίσεων στον κυβερνοχώρο σε επίπεδο ΕΕ εξαρτάται από την αποτελεσματική τεχνική, επιχειρησιακή και στρατηγική/πολιτική συνεργασία.

Σε κάθε επίπεδο οι εμπλεκόμενοι παράγοντες θα πρέπει να εκτελούν συγκεκριμένες δραστηριότητες με σκοπό την επίτευξη τριών βασικών στόχων:

— Συντονισμένη αντιμετώπιση

— Κοινή επίγνωση της κατάστασης

— Επικοινωνία με το κοινό

Καθ' όλη τη διάρκεια ενός περιστατικού ή μιας κρίσης τα χαμηλότερα επίπεδα συνεργασίας θα ειδοποιούν, θα ενημερώνουν και θα υποστηρίζουν τα υψηλότερα επίπεδα, ενώ τα υψηλότερα επίπεδα θα παρέχουν καθοδήγηση ([2]) και αποφάσεις στα χαμηλότερα επίπεδα, κατά περίπτωση.

Συνεργασία σε τεχνικό επίπεδο

Πεδίο δραστηριοτήτων:

— Χειρισμός περιστατικών ([3]) κατά τη διάρκεια κρίσης ασφάλειας στον κυβερνοχώρο

— Παρακολούθηση και επιτήρηση περιστατικού, συμπεριλαμβανομένης της συνεχούς ανάλυσης των απειλών και κινδύνων.

Δυνητικοί φορείς

Σε τεχνικό επίπεδο, ο κεντρικός μηχανισμός για τη συνεργασία στο προσχέδιο είναι το δίκτυο CSIRT, του οποίου προεδρεύει η Προεδρία με γραμματεία που παρέχεται από τον ENISA.

— Κράτη μέλη:

  — Οι αρμόδιες αρχές και τα ενιαία σημεία επαφής που συγκροτήθηκαν με την οδηγία NIS.

  — Οι CSIRT.

— Όργανα/Υπηρεσίες/Οργανισμοί της ΕΕ:

  — Ο ENISA.

  — Η Ευρωπόλ/EC3.

  — Η CERT-ΕΕ.

([1]) Εν προκειμένω είναι σημαντικό να σημειωθεί ότι η επικοινωνία με το κοινό μπορεί να αφορά τόσο την επικοινωνία με το ευρύ κοινό σχετικά με το περιστατικό όσο και την επικοινωνία σχετικά με πληροφορίες πιο τεχνικού ή επιχειρησιακού χαρακτήρα με κρίσιμους τομείς και/ή τα θιγόμενα μέρη. Αυτό ενδέχεται να απαιτήσει τη χρήση εμπιστευτικών διαύλων διάδοσης και τη χρήση ειδικών τεχνικών εργαλείων/πλατφορμών. Και στις δύο περιπτώσεις η επικοινωνία με τους φορείς και το ευρύτερο κοινό εντός οποιουδήποτε κράτους μέλους αποτελεί αρμοδιότητα και ευθύνη κάθε κράτους μέλους. Ως εκ τούτου, σύμφωνα με την αρχή της επικουρικότητας που παρουσιάστηκε ανωτέρω, τα κράτη μέλη και οι εθνικές ομάδες CSIRT έχουν την τελική ευθύνη για τις πληροφορίες που διαδίδονται εντός της επικράτειάς τους και της περιοχής ευθύνης τους, αντίστοιχα.

([2]) «Άδειες ανάληψης δράσης» — σε περίπτωση κρίσης ασφάλειας στον κυβερνοχώρο οι σύντομοι χρόνοι αντίδρασης είναι ζωτικής σημασίας για την εφαρμογή κατάλληλων δράσεων μετριασμού. Για να εξασφαλίζονται αυτοί οι σύντομοι χρόνοι αντίδρασης, μπορούν να εκδίδονται από ένα κράτος μέλος σε άλλο «άδειες ανάληψης δράσης» σε προαιρετική βάση, με τις οποίες παρέχεται σε ένα κράτος μέλος η άδεια να αναλάβει δράση αμέσως, χωρίς να διαβουλευθεί με τα υψηλότερα επίπεδα ή με τα θεσμικά όργανα της ΕΕ ούτε να περάσει από όλους τους επίσημους διαύλους που απαιτούνται συνήθως, εάν αυτό απαιτείται σε ένα συγκεκριμένο περιστατικό (π.χ. μια CSIRT δεν θα πρέπει να υποχρεούται να διαβουλευθεί με τα υψηλότερα επίπεδα προκειμένου να διαβιβάσει πολύτιμες πληροφορίες σε μια CSIRT σε άλλο κράτος μέλος).

([3]) Ως «χειρισμός περιστατικών» νοείται το σύνολο των διαδικασιών που υποστηρίζουν τον εντοπισμό, την ανάλυση και την ανάσχεση ενός περιστατικού και την παρέμβαση για την αντιμετώπισή του.

— Ευρωπαϊκή Επιτροπή:

  — Το ΚΣΑΕΑ (υπηρεσία συνεχούς λειτουργίας 24/7 στην ΓΔ ECHO) και η οριζόμενη επικεφαλής υπηρεσία (η οποία θα επιλέγεται μεταξύ της ΓΔ CNECT και της ΓΔ HOME ανάλογα με τη συγκεκριμένη φύση του περιστατικού), η Γενική Γραμματεία (γραμματεία του ARGUS), η ΓΔ HR (Διεύθυνση Ασφαλείας), η ΓΔ DIGIT (Επιχειρήσεις ασφάλειας των ΤΠ).

  — Για άλλους οργανισμούς της ΕΕ ([1]) η αντίστοιχη αρμόδια ΓΔ της Επιτροπής ή η ΕΥΕΔ (πρώτο σημείο επαφής).

— ΕΥΕΔ:

  — Η SIAC (Ενιαία Ικανότητα Ανάλυσης Πληροφοριών: INTCEN της ΕΕ και EUMS INT).

  — Η Αίθουσα Διαχείρισης Κρίσεων της ΕΕ και η οριοθείσα γεωγραφική ή θεματική υπηρεσία.

  — Η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ (μέρος της INTCEN της ΕΕ — ασφάλεια στον κυβερνοχώρο σε υβριδικό περιβάλλον).

Κοινή επίγνωση της κατάστασης:

— Ως μέρος της τακτικής συνεργασίας σε τεχνικό επίπεδο για την υποστήριξη της επίγνωσης της κατάστασης από την Ένωση, ο ENISA θα πρέπει να καταρτίζει σε τακτική βάση την τεχνική έκθεση για την κατάσταση στην ΕΕ σχετικά με τα περιστατικά και τις απειλές που θέτουν σε κίνδυνο την ασφάλεια στον κυβερνοχώρο, βάσει δημόσια διαθέσιμων πληροφοριών, της δικής του ανάλυσης και εκθέσεων που εκπονούνται από κοινού με τις CSIRT των κρατών μελών (σε εθελοντική βάση) ή με τα ενιαία σημεία επαφής που συγκροτήθηκαν με την οδηγία NIS, το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) της Ευρωπόλ και την CERT-ΕΕ, και, κατά περίπτωση, το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (INTCEN) της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ). Η έκθεση θα πρέπει να διατίθεται στις αρμόδιες υπηρεσίες του Συμβουλίου, της Επιτροπής, της ΥΕ/ΑΠ και στο δίκτυο CSIRT.

— Σε περίπτωση μείζονος περιστατικού, η Προεδρία του δικτύου CSIRT, με τη συνδρομή του ENISA, καταρτίζει έκθεση για την κατάσταση στην ΕΕ σχετικά με τα περιστατικά που θέτουν σε κίνδυνο την ασφάλεια στον κυβερνοχώρο ([2]) και την υποβάλλει στην Προεδρία, στην Επιτροπή και στην ΥΕ/ΑΠ μέσω της CSIRT της εκ περιτροπής Προεδρίας.

— *Όλοι οι άλλοι οργανισμοί της ΕΕ* υποβάλλουν έκθεση στις αντίστοιχες αρμόδιες ΓΔ, οι οποίες με τη σειρά τους υποβάλλουν έκθεση στην επικεφαλής υπηρεσία της Επιτροπής.

— Η *CERT-ΕΕ* παρέχει τεχνικές εκθέσεις στο δίκτυο CSIRT, στα θεσμικά όργανα και τους οργανισμούς της ΕΕ (κατά περίπτωση) και στο σύστημα ARGUS (εάν ενεργοποιηθεί).

— Η *Ευρωπόλ/EC3* ([3]) *και η CERT-ΕΕ* παρέχουν εξειδικευμένη εγκληματολογική ανάλυση των τεχνικών τεχνουργημάτων και άλλων τεχνικών πληροφοριών στο δίκτυο CSIRT.

— SIAC της ΕΥΕΔ: Η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ υποβάλλει εκθέσεις στις υπηρεσίες της ΕΥΕΔ εξ ονόματος του INTCEN.

Αντιμετώπιση:

— *Το δίκτυο CSIRT* προβαίνει σε ανταλλαγές τεχνικών λεπτομερειών και αναλύσεων σχετικά με το περιστατικό, όπως διευθύνσεις IP, δείκτες έκθεσης σε κίνδυνο ([4]) κ.λπ. Οι εν λόγω πληροφορίες θα πρέπει να παρέχονται αμελλητί στον ENISA και το αργότερο εντός 24 ωρών από τη στιγμή που θα διαπιστωθεί το περιστατικό.

— Σύμφωνα με τις τυποποιημένες επιχειρησιακές διαδικασίες του δικτύου CSIRT, τα μέλη του συνεργάζονται στην προσπάθειά τους να αναλύσουν τα διαθέσιμα τεχνικά τεχνουργήματα και άλλες τεχνικές πληροφορίες σχετικά με το περιστατικό με σκοπό τον προσδιορισμό των αιτίων και πιθανών τεχνικών μέτρων μετριασμού.

— Ο ENISA βοηθά τις CSIRT στις τεχνικές τους δραστηριότητες βασιζόμενος στην εμπειρογνωσία που διαθέτει και σύμφωνα με την εντολή που του έχει δοθεί ([5]).

([1]) Ανάλογα με τον χαρακτήρα και τις συνέπειες του περιστατικού σε διάφορους τομείς δραστηριοτήτων (οικονομικά, μεταφορές, ενέργεια, ιατροφαρμακευτική περίθαλψη κ.λπ.) θα εμπλέκονται τα σχετικά όργανα ή οργανισμοί της ΕΕ.

([2]) Η έκθεση για την κατάσταση στην ΕΕ σχετικά με τα περιστατικά που θέτουν σε κίνδυνο την ασφάλεια στον κυβερνοχώρο αποτελεί συμπίληση εκθέσεων που υποβάλλουν οι εθνικές CSIRT. Ο μορφότυπος της έκθεσης πρέπει να περιγράφεται στις τυποποιημένες επιχειρησιακές διαδικασίες SOP του δικτύου CSIRT.

([3]) Σύμφωνα με τους όρους και τις διαδικασίες που καθορίζονται στο νομικό πλαίσιο του EC3.

([4]) Δείκτης έκθεσης σε κίνδυνο — στην ηλεκτρονική εγκληματολογική ανάλυση είναι ένα τεχνούργημα που παρατηρείται σε δίκτυο ή σε λειτουργικό σύστημα και αποτελεί αξιόπιστη ένδειξη διείσδυσης σε υπολογιστή. Συνήθεις δείκτες έκθεσης σε κίνδυνο είναι οι υπογραφές ιών και οι διευθύνσεις IP, κωδικοί κατακερματισμού (hashes) MD5 αρχείων κακόβουλου λογισμικού, ή URL ή ονόματα χώρου διακομιστών διοίκησης και ελέγχου κακόβουλου λογισμικού (botnet).

([5]) Πρόταση κανονισμού σχετικά με τον ENISA, τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια στον Κυβερνοχώρο και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα των τεχνολογιών της πληροφορίας και των επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»), 13 Σεπτεμβρίου 2017.

— Οι CSIRT των κρατών μελών συντονίζουν τις δραστηριότητες τεχνικής παρέμβασης με τη συνδρομή του ENISA και της Επιτροπής.

— SIAC της ΕΥΕΔ: Εξ ονόματος του INTCEN, η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ καθορίζει τη διαδικασία συλλογής με σκοπό τη συγκέντρωση αρχικών αποδεικτικών στοιχείων.

Επικοινωνία με το κοινό:

— Οι CSIRT καταρτίζουν τεχνικές συμβουλές ([1]) και ειδοποιήσεις τρωτότητας ([2]) και τις διαδίδουν στις σχετικές τους κοινότητες και το κοινό σύμφωνα με τις διαδικασίες χορήγησης άδειας που ισχύουν σε κάθε περίπτωση.

— Ο ENISA διευκολύνει την κατάρτιση και διάδοση κοινών επικοινωνιών του δικτύου CSIRT.

— Ο ENISA συντονίζει τις δικές του δραστηριότητες επικοινωνίας με το κοινό με το δίκτυο CSIRT και την υπηρεσία Τύπου της Επιτροπής.

— Ο ENISA και το EC3 συντονίζουν τις δραστηριότητες επικοινωνίας τους με το κοινό με βάση την κοινή επίγνωση της κατάστασης, όπως έχει συμφωνηθεί μεταξύ των κρατών μελών. Και οι δύο συντονίζουν τις δραστηριότητες επικοινωνίας τους με το κοινό με την υπηρεσία Τύπου της Επιτροπής.

— Εάν η κρίση έχει εξωτερική διάσταση ή διάσταση σχετική με την κοινή πολιτική ασφαλείας και άμυνας (ΚΠΑΑ), η επικοινωνία με το κοινό θα πρέπει να συντονίζεται με την ΕΥΕΔ και την υπηρεσία εκπροσώπου Τύπου της ΥΕ/ΑΠ.

Συνεργασία σε επιχειρησιακό επίπεδο

Πεδίο δραστηριοτήτων:

— Προετοιμασία της λήψης αποφάσεων σε πολιτικό επίπεδο.

— Συντονισμός της διαχείρισης της κρίσης ασφάλειας στον κυβερνοχώρο (ανάλογα με την περίπτωση).

— Αξιολόγηση των συνεπειών και των επιπτώσεων σε επίπεδο ΕΕ και πρόταση για τυχόν δράσεις μετριασμού.

Δυνητικοί φορείς

— Κράτη μέλη:

  — Οι αρμόδιες αρχές και τα ενιαία σημεία επαφής που συγκροτήθηκαν με την οδηγία NIS.

  — Οργανισμοί για την ασφάλεια στον κυβερνοχώρο, εθνικές CSIRT.

  — Άλλες εθνικές τομεακές αρχές (σε περίπτωση πολυτομεακών περιστατικών ή κρίσεων).

— Όργανα/Υπηρεσίες/Οργανισμοί της ΕΕ:

  — Ο ENISA.

  — Η Ευρωπόλ/EC3.

  — Η CERT-ΕΕ.

— Ευρωπαϊκή Επιτροπή:

  — Ο (αναπληρωτής) γενικός γραμματέας (ΓΓ) (διαδικασία ARGUS).

  — Η ΓΔ CNECT/HOME.

  — Η Αρχή Ασφαλείας της Επιτροπής.

  — Άλλες ΓΔ (σε περίπτωση πολυτομεακών περιστατικών ή κρίσεων).

([1]) Συμβουλές τεχνικής φύσης για τα αίτια του περιστατικού και τις πιθανές δράσεις μετριασμού.
([2]) Πληροφορίες σχετικά με την τεχνική τρωτότητα η οποία χρησιμοποιείται για να επηρεαστούν αρνητικά τα συστήματα ΤΠ.

— ΕΥΕΔ:

  — Ο (αναπληρωτής) γενικός γραμματέας για την αντιμετώπιση κρίσεων και την Ενιαία Ικανότητα Ανάλυσης Πληροφοριών (SIAC) [Κέντρο Ανάλυσης Πληροφοριών (INTCEN) της ΕΕ και Τμήμα Πληροφοριών του ΣΕΕΕ].

  — Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ.

— Συμβούλιο:

  — η Προεδρία [ο πρόεδρος της οριζόντιας ομάδας εργασίας για θέματα κυβερνοχώρου ή η ΕΜΑ ([1])] με την υποστήριξη της ΓΓΣ ή της ΕΠΑ ([2]) και —εάν ενεργοποιηθούν— με την υποστήριξη των ρυθμίσεων IPCR.

Επίγνωση της κατάστασης:

— Υποστήριξη της εκπόνησης εκθέσεων για την επικρατούσα πολιτικο/στρατηγική κατάσταση (π.χ. από την ISAA σε περίπτωση ενεργοποίησης των IPCR).

— Η *οριζόντια ομάδα εργασίας για θέματα κυβερνοχώρου του Συμβουλίου* προετοιμάζει τη συνεδρίαση της ΕΜΑ ή της ΕΠΑ, κατά περίπτωση.

— Σε περίπτωση ενεργοποίησης των IPCR,

  — η Προεδρία μπορεί να συγκαλέσει συνεδριάσεις στρογγυλής τραπέζης για τη στήριξη της προετοιμασίας για την ΕΜΑ ή την ΕΠΑ, συγκεντρώνοντας σχετικούς ενδιαφερόμενους φορείς από τα κράτη μέλη, τα θεσμικά όργανα, τους οργανισμούς, καθώς και τρίτα μέρη, όπως τρίτες χώρες και διεθνείς οργανισμούς. Πρόκειται για συνεδριάσεις κρίσεων με σκοπό τον προσδιορισμό των σημείων συμφόρησης και τη διατύπωση προτάσεων για ενέργειες σχετικές με οριζόντια θέματα,

  — η *επικεφαλής υπηρεσία της Επιτροπής στην ΕΥΕΔ* ως επικεφαλής για τη διαδικασία ISAA καταρτίζει την έκθεση ISAA με συνεισφορές από τον ENISA, το δίκτυο CSIRT, την Ευρωπόλ/EC3, το EUMS INT, το INTCEN και όλους τους άλλους σχετικούς φορείς. Η έκθεση ISAA αποτελεί πανευρωπαϊκή αξιολόγηση βασισμένη στη συσχέτιση των τεχνικών περιστατικών και στην αξιολόγηση κρίσεων (ανάλυση απειλών, αξιολόγηση κινδύνου, μη τεχνικές συνέπειες και επιπτώσεις, πτυχές των περιστατικών ή κρίσεων που δεν συνδέονται με τον κυβερνοχώρο κ.λπ.) που είναι προσαρμοσμένη στις ανάγκες του επιχειρησιακού και πολιτικού επιπέδου.

— Σε περίπτωση ενεργοποίησης του συστήματος ARGUS,

  — η CERT-EU και το EC3 ([3]) συμβάλλουν άμεσα στην ανταλλαγή πληροφοριών εντός της Επιτροπής.

— Σε περίπτωση ενεργοποίησης του μηχανισμού αντιμετώπισης κρίσεων της ΕΥΕΔ,

  — η SIAC θα εντείνει τις προσπάθειές της όσον αφορά τη συλλογή πληροφοριών, θα συγκεντρώσει τις πληροφορίες από όλες τις πηγές και θα καταρτίσει ανάλυση και αξιολόγηση σχετικά με το περιστατικό.

Αντιμετώπιση (κατόπιν αιτήματος από το πολιτικό επίπεδο):

— Διασυνοριακή συνεργασία με τα ενιαία σημεία επαφής και τις εθνικές αρμόδιες αρχές (οδηγία ΑΔΠ) για τον μετριασμό των συνεπειών και των αποτελεσμάτων.

— Ενεργοποίηση όλων των τεχνικών μέτρων μετριασμού και συντονισμός των τεχνικών ικανοτήτων που απαιτούνται προκειμένου να σταματήσει ή να μειωθεί ο αντίκτυπος των επιθέσεων εναντίον των στοχευμένων συστημάτων πληροφορικής.

— Συνεργασία και, αν αποφασιστεί, συντονισμός της ανάπτυξης τεχνικών ικανοτήτων με σκοπό μια κοινή ή συνεργατική αντιμετώπιση σύμφωνα με τις ***τυποποιημένες επιχειρησιακές διαδικασίες του δικτύου CSIRT***.

— Αξιολόγηση της ανάγκης για συνεργασία με εμπλεκόμενα τρίτα μέρη.

— (εφόσον ενεργοποιηθεί) Λήψη αποφάσεων στο πλαίσιο της διαδικασίας ARGUS.

— (εφόσον ενεργοποιηθούν) Προετοιμασία αποφάσεων και συντονισμός στο πλαίσιο των ρυθμίσεων IPCR.

— (εφόσον ενεργοποιηθεί) Υποστήριξη της λήψης αποφάσεων της ΕΥΕΔ μέσω του μηχανισμού αντιμετώπισης κρίσεων της ΕΥΕΔ, μεταξύ άλλων όσον αφορά τις επαφές με τρίτες χώρες και διεθνείς οργανισμούς, καθώς και κάθε μέτρο που αποσκοπεί στην προστασία των αποστολών και επιχειρήσεων ΚΠΑΑ και των αντιπροσωπειών της ΕΕ.

([1]) Η Επιτροπή Μονίμων Αντιπροσώπων ή ΕΜΑ (άρθρο 240 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης — ΣΛΕΕ) είναι αρμόδια για την προετοιμασία των εργασιών του Συμβουλίου της Ευρωπαϊκής Ένωσης.

([2]) Η Επιτροπή Πολιτικής και Ασφάλειας είναι μια επιτροπή του Συμβουλίου της Ευρωπαϊκής Ένωσης η οποία ασχολείται με την κοινή εξωτερική πολιτική και πολιτική ασφαλείας (ΚΕΠΠΑ) που αναφέρεται στο άρθρο 38 της Συνθήκης για την Ευρωπαϊκή Ένωση.

([3]) Σύμφωνα με και υπό τους όρους και τις διαδικασίες που καθορίζονται στο νομικό πλαίσιο του EC3.

Επικοινωνία με το κοινό:

— Συμφωνία όσον αφορά τα μηνύματα επικοινωνίας με το κοινό σχετικά με το περιστατικό.

— Εάν η κρίση έχει εξωτερική διάσταση ή διάσταση σχετική με την κοινή πολιτική ασφαλείας και άμυνας (ΚΠΑΑ), η επικοινωνία με το κοινό θα πρέπει να συντονίζεται με την ΕΥΕΔ και την υπηρεσία εκπροσώπου Τύπου της ΥΕ/ΑΠ.

Συνεργασία στο στρατηγικό/πολιτικό επίπεδο

Δυνητικοί φορείς

— Για τα κράτη μέλη, οι αρμόδιοι υπουργοί για την ασφάλεια στον κυβερνοχώρο.

— Για το Ευρωπαϊκό Συμβούλιο, ο πρόεδρος.

— Για το Συμβούλιο, η εκ περιτροπής Προεδρία.

— Όταν πρόκειται για μέτρα στο πλαίσιο της «διπλωματικής εργαλειοθήκης για τον κυβερνοχώρο», η ΕΠΑ και η οριζόντια ομάδα εργασίας.

— Για την Ευρωπαϊκή Επιτροπή, ο πρόεδρος ή ο εξουσιοδοτημένος αντιπρόεδρος/Επίτροπος.

— Η Ύπατη Εκπρόσωπος της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας / αντιπρόεδρος της Επιτροπής.

Πεδίο δραστηριοτήτων: Στρατηγική και πολιτική διαχείριση τόσο των πτυχών της κρίσης που αφορούν τον κυβερνοχώρο όσο και αυτών που δεν συνδέονται με τον κυβερνοχώρο, συμπεριλαμβανομένων των μέτρων που εμπίπτουν στο πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.

Κοινή επίγνωση της κατάστασης:

— Προσδιορισμός των επιπτώσεων των διαταραχών που προκαλεί η κρίση στη λειτουργία της Ένωσης.

Αντιμετώπιση:

— Ενεργοποίηση πρόσθετων μηχανισμών/μέσων διαχείρισης κρίσεων ανάλογα με τη φύση και τις επιπτώσεις του περιστατικού. Μπορούν να περιλαμβάνουν, για παράδειγμα, τον μηχανισμό πολιτικής προστασίας.

— Λήψη μέτρων εντός του πλαισίου για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.

— Εξασφάλιση διαθεσιμότητας υποστήριξης έκτακτης ανάγκης για τα πληττόμενα κράτη μέλη, π.χ. με ενεργοποίηση του Αποθεματικού Ταμείου Αντιμετώπισης Επειγουσών Καταστάσεων για την Ασφάλεια στον Κυβερνοχώρο ([1]) μόλις αρχίσει να εφαρμόζεται.

— Συνεργασία και συντονισμός με διεθνείς οργανισμούς κατά περίπτωση, όπως τα Ηνωμένα Έθνη (ΟΗΕ), ο Οργανισμός για την Ασφάλεια και τη Συνεργασία στην Ευρώπη (ΟΑΣΕ) και, ιδίως, το ΝΑΤΟ.

— Αξιολόγηση των συνεπειών που αφορούν την εθνική ασφάλεια και άμυνα.

Επικοινωνία με το κοινό:

Λήψη απόφασης για τον καθορισμό μιας κοινής στρατηγικής επικοινωνίας με το κοινό.

ΑΝΤΙΜΕΤΩΠΙΣΗ, ΣΕ ΣΥΝΤΟΝΙΣΜΟ ΜΕ ΤΑ ΚΡΑΤΗ ΜΕΛΗ, ΣΕ ΕΠΙΠΕΔΟ ΕΕ ΣΤΟ ΠΛΑΙΣΙΟ ΤΩΝ ΡΥΘΜΙΣΕΩΝ IPCR

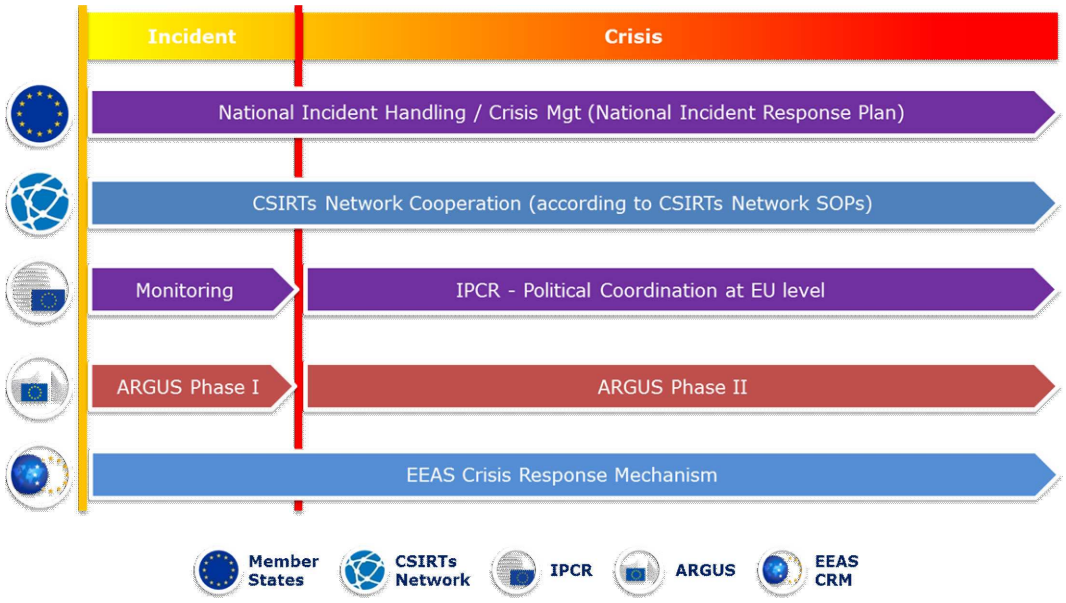
Σύμφωνα με την αρχή της συμπληρωματικότητας σε επίπεδο ΕΕ, η παρούσα ενότητα παρουσιάζει και επικεντρώνεται ιδίως στον κεντρικό στόχο, στις αρμοδιότητες και στις δραστηριότητες των αρχών των κρατών μελών, του δικτύου CSIRT, του ENISA, της CERT-EU, της Ευρωπόλ/EC3, του INTCEN, της Μονάδας Ανάλυσης Υβριδικών Απειλών της ΕΕ και της οριζόντιας ομάδας εργασίας του Συμβουλίου για θέματα κυβερνοχώρου στο πλαίσιο της διαδικασίας IPCR. Οι φορείς θεωρείται ότι ενεργούν σύμφωνα με τις διαδικασίες που θεσπίζονται σε επίπεδο ΕΕ ή σε εθνικό επίπεδο.

Είναι σημαντικό να σημειωθεί ότι, όπως φαίνεται και από το διάγραμμα 1, ανεξάρτητα από την ενεργοποίηση των μηχανισμών διαχείρισης κρίσεων της ΕΕ, λαμβάνουν χώρα δραστηριότητες σε εθνικό επίπεδο και υπάρχει συνεργασία στο πλαίσιο του δικτύου CSIRT (εφόσον απαιτείται) καθ' όλη τη διάρκεια κάθε περιστατικού/κρίσης σύμφωνα με τις αρχές της επικουρικότητας και της αναλογικότητας.

([1]) Το Αποθεματικό Ταμείο Αντιμετώπισης Επειγουσών Καταστάσεων για την Ασφάλεια στον Κυβερνοχώρο είναι προτεινόμενη δράση στο πλαίσιο της κοινής ανακοίνωσης με τίτλο «Ανθεκτικότητα, αποτροπή και άμυνα: Οικοδόμηση ισχυρής ασφάλειας στον κυβερνοχώρο για την ΕΕ», JOIN(2017) 450/1.

Διάγραμμα 1

Αντιμετώπιση περιστατικών/κρίσεων στον κυβερνοχώρο σε επίπεδο ΕΕ



Όλες οι δραστηριότητες που περιγράφονται παρακάτω πρέπει να πραγματοποιούνται σύμφωνα με τις τυποποιημένες επιχειρησιακές διαδικασίες και τους τυποποιημένους επιχειρησιακούς κανόνες των σχετικών μηχανισμών συνεργασίας και σύμφωνα με τις καθορισμένες εντολές και αρμοδιότητες των διαφόρων φορέων και θεσμικών οργάνων. Οι εν λόγω διαδικασίες/κανόνες μπορεί να χρειάζονται ορισμένες προσθήκες ή τροποποιήσεις προκειμένου να επιτευχθεί η καλύτερη δυνατή συνεργασία και η αποτελεσματική αντιμετώπιση μεγάλης κλίμακας περιστατικών και κρίσεων στον κυβερνοχώρο.

Μπορεί να μην κληθούν όλοι οι φορείς που παρουσιάζονται στη συνέχεια να αναλάβουν δράση κατά τη διάρκεια ενός συγκεκριμένου περιστατικού. Ωστόσο το σχέδιο στρατηγικής και οι σχετικές τυποποιημένες διαδικασίες λειτουργίας των μηχανισμών συνεργασίας θα πρέπει να προβλέπουν το ενδεχόμενο συμμετοχής τους.

Λόγω του διαφορετικού αντικτύπου που μπορεί να έχει στην κοινωνία ένα περιστατικό ή μια κρίση στον κυβερνοχώρο, ο υψηλός βαθμός ευελιξίας όσον αφορά τη συμμετοχή των τομεακών φορέων σε όλα τα επίπεδα, καθώς και κάθε κατάλληλη αντίδραση θα βασίζονται στις δραστηριότητες μετριασμού τόσο στον κυβερνοχώρο όσο και εκτός κυβερνοχώρου.

Διαχείριση κρίσεων ασφάλειας στον κυβερνοχώρο — ενσωμάτωση της ασφάλειας στον κυβερνοχώρο στη διαδικασία IPCR

Οι ρυθμίσεις IPCR, που περιγράφονται στις τυποποιημένες επιχειρησιακές διαδικασίες IPCR ([1]), ακολουθούν διαδοχικά τα βήματα που περιγράφονται παρακάτω (η πραγματοποίηση ορισμένων από τα εν λόγω βήματα θα εξαρτάται από την εκάστοτε κατάσταση).

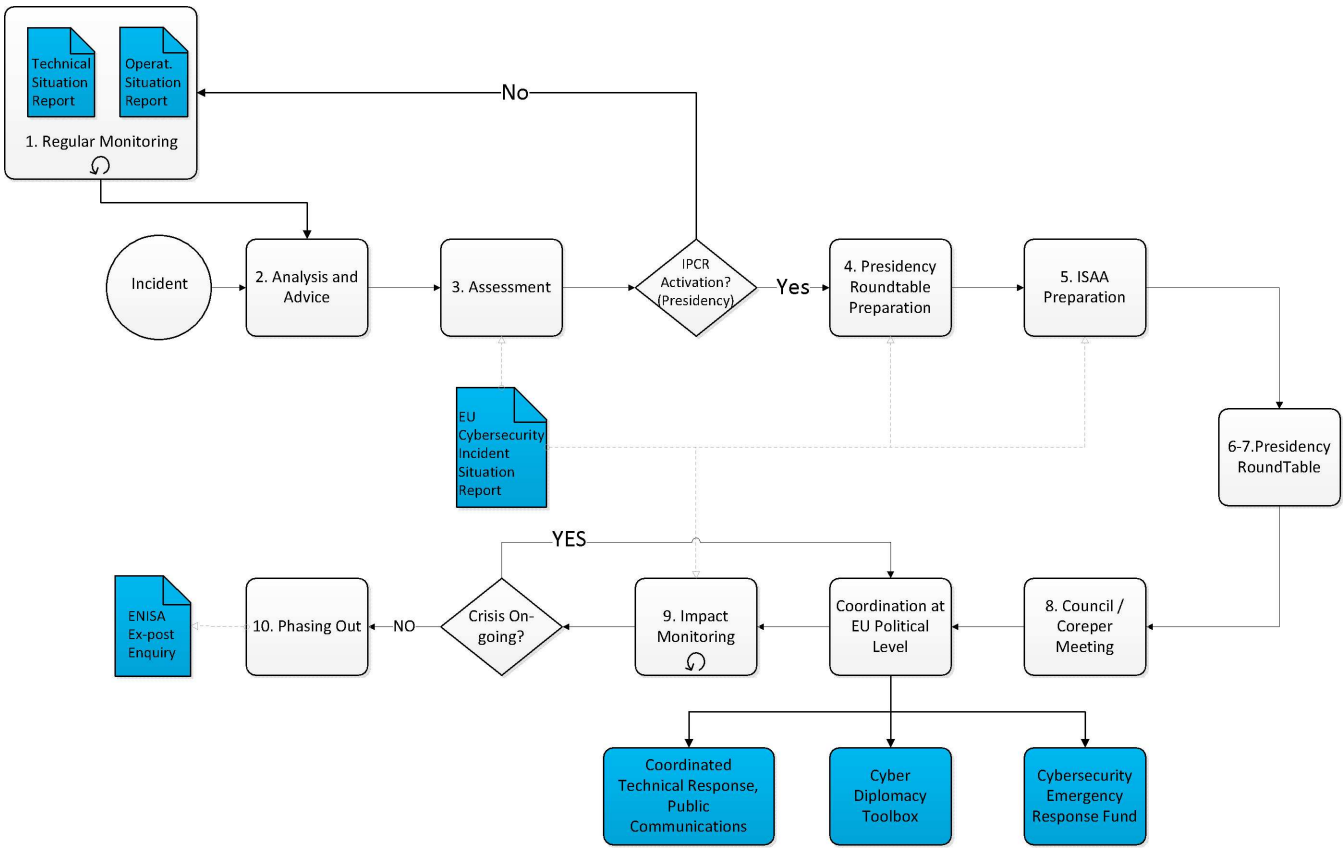
Σε κάθε βήμα προσδιορίζουμε δραστηριότητες και φορείς που συνδέονται ειδικά με την ασφάλεια στον κυβερνοχώρο. Προς διευκόλυνση του αναγνώστη, σε κάθε βήμα παρατίθεται το κείμενο από τις τυποποιημένες επιχειρησιακές διαδικασίες IPCR και εν συνεχεία οι ειδικές δραστηριότητες του σχεδίου στρατηγικής. Η προσέγγιση ανά βήμα επιτρέπει επίσης τον σαφή εντοπισμό των **κενών** που υπάρχουν στις απαιτούμενες ικανότητες και διαδικασίες, τα οποία εμποδίζουν την αποτελεσματική αντίδραση σε κρίσεις ασφάλειας στον κυβερνοχώρο.

Το διάγραμμα 2 [παρακάτω ([2])] αποτελεί γραφική παράσταση της διαδικασίας IPCR —τα νέα στοιχεία που εισάγονται επισημαίνονται με μπλε χρώμα.

([1]) Από το έγγραφο 12607/15 «IPCR Standard Operating Procedures», επί του οποίου συμφώνησε η Ομάδα Φίλων της Προεδρίας και το οποίο έλαβε υπόψη της η ΕΜΑ τον Οκτώβριο του 2015.
([2]) Εκτενέστερη εκδοχή του διαγράμματος επισυνάπτεται στο προσάρτημα.

Διάγραμμα 2

Ειδικά στοιχεία ασφάλειας στον κυβερνοχώρο στο IPCR



Σημείωση: Δεδομένης της φύσης των υβριδικών απειλών στον κυβερνοχώρο που έχουν σχεδιαστεί έτσι ώστε να παραμένουν κάτω από το όριο της αναγνωρίσιμης κρίσης, η ΕΕ πρέπει να λάβει μέτρα πρόληψης και ετοιμότητας. Η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ έχει την υποχρέωση να αναλύει γρήγορα σχετικά περιστατικά και να ενημερώνει τις κατάλληλες δομές συντονισμού. Η τακτική υποβολή εκθέσεων από την εν λόγω μονάδα μπορεί να συμβάλει στη διαμόρφωση της πολιτικής σε επιμέρους τομείς για την ενίσχυση της ετοιμότητας.

— **Βήμα 1 — Τακτική τομεακή παρακολούθηση και προειδοποίηση:** οι υφιστάμενες, τακτικές τομεακές εκθέσεις για την επικρατούσα κατάσταση και οι υφιστάμενες προειδοποιήσεις παρέχουν ενδείξεις στην Προεδρία του Συμβουλίου σχετικά με μία εξελισσόμενη κρίση καθώς και με την πιθανή εξέλιξή της.

  — **Κενό που εντοπίστηκε:** Δεν υπάρχουν επί του παρόντος τακτικές και συντονισμένες εκθέσεις για την επικρατούσα κατάσταση και προειδοποιήσεις για την ασφάλεια στον κυβερνοχώρο σχετικά με περιστατικά (και απειλές) που αφορούν την ασφάλεια στον κυβερνοχώρο σε επίπεδο ΕΕ.

  — **Προσχέδιο: Παρακολούθηση της κατάστασης / υποβολή εκθέσεων για την ασφάλεια στον κυβερνοχώρο στην ΕΕ**

    — **Ο ENISA θα εκπονεί σε τακτά διαστήματα τεχνική έκθεση** σχετικά με την επικρατούσα κατάσταση στην ΕΕ όσον αφορά την ασφάλεια στον κυβερνοχώρο σχετικά με περιστατικά και απειλές, βάσει των δημόσια διαθέσιμων πληροφοριών, της δικής του ανάλυσης και των εκθέσεων που του διαβιβάζουν οι CSIRT (σε προαιρετική βάση) ή τα ενιαία κέντρα επαφής των κρατών μελών βάσει της οδηγίας για την ασφάλεια δικτύων και πληροφοριών, το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3) της Ευρωπόλ, η CERT-EU και το Κέντρο Ανάλυσης Πληροφοριών της Ευρωπαϊκής Ένωσης (INTCEN) της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης (ΕΥΕΔ). Η έκθεση θα πρέπει να διατίθεται στις αρμόδιες υπηρεσίες του Συμβουλίου, της Επιτροπής και του δικτύου CSIRT.

    — Για λογαριασμό της SIAC, η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ θα πρέπει να εκπονεί **έκθεση επιχειρησιακής κατάστασης για θέματα ασφάλειας του κυβερνοχώρου στην ΕΕ.** Επίσης, η έκθεση υποστηρίζει το πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο.

    — Και οι δύο εκθέσεις θα διαχέονται προς τους ενδιαφερόμενους σε ευρωπαϊκό και εθνικό επίπεδο, ώστε να συμβάλλουν στην επίγνωση των δικών τους δυνατοτήτων, να αποτελούν βάση για τη λήψη αποφάσεων και να διευκολύνουν τη διασυνοριακή περιφερειακή συνεργασία.

Μετά τον εντοπισμό περιστατικού

— **Βήμα 2 — Ανάλυση και παροχή συμβουλών:** με βάση τα διαθέσιμα στοιχεία παρακολούθησης και τις προειδοποιήσεις, οι υπηρεσίες της Επιτροπής, η ΕΥΕΔ και η Γενική Γραμματεία του Συμβουλίου αλληλοενημερώνονται για τις πιθανές εξελίξεις, προκειμένου να είναι σε θέση να συμβουλεύουν την Προεδρία για πιθανή ενεργοποίηση της IPCR (πλήρη ή απλώς σε λειτουργία ανταλλαγής πληροφοριών).

  — **Προσχέδιο:**

    — Για την Επιτροπή, ΓΔ CNECT, ΓΔ HOME, ΓΔ HR.DS και ΓΔ DIGIT με την υποστήριξη του ENISA, του EC3 και της CERT-EU.

    — ΕΥΕΔ. Με βάση τις εργασίες του SITROOM και πηγές πληροφοριών, η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ παρέχει επίγνωση της κατάστασης όσον αφορά υφιστάμενες και δυνητικές υβριδικές απειλές κατά της ΕΕ και των εταίρων της, συμπεριλαμβανομένων των απειλών στον κυβερνοχώρο. Ως εκ τούτου, όταν η ανάλυση και αξιολόγηση της Μονάδας Ανάλυσης Υβριδικών Απειλών της ΕΕ υποδεικνύει την ύπαρξη ενδεχόμενων απειλών κατά ενός κράτους μέλους, χωρών-εταίρων ή οργανισμού, το INTCEN θα ενημερώνει (σε πρώτο βαθμό) σε επιχειρησιακό επίπεδο, σύμφωνα με τις καθιερωμένες διαδικασίες. Το επιχειρησιακό επίπεδο θα καταρτίζει στη συνέχεια συστάσεις για το επίπεδο πολιτικής στρατηγικής, συμπεριλαμβανομένης της ενδεχόμενης ενεργοποίησης των ρυθμίσεων διαχείρισης κρίσεων, σε λειτουργία παρακολούθησης (π.χ. μηχανισμός αντιμετώπισης κρίσεων της ΕΥΕΔ ή ιστοσελίδα παρακολούθησης IPCR).

    — Ο πρόεδρος του δικτύου CSIRT, επικουρούμενος από τον ENISA, καταρτίζει έκθεση για την κατάσταση σε σχέση με περιστατικά ασφάλειας του κυβερνοχώρου στην ΕΕ ([1]), η οποία παρουσιάζεται στην Προεδρία, στην Επιτροπή και στην Ύπατο Εκπρόσωπο / Αντιπρόεδρο της Επιτροπής μέσω των CSIRT της εκ περιτροπής Προεδρίας.

— **Βήμα 3 — Αξιολόγηση/απόφαση σχετικά με την ενεργοποίηση IPCR**: η Προεδρία αξιολογεί κατά πόσον υπάρχει ανάγκη για πολιτικό συντονισμό, ανταλλαγή πληροφοριών ή λήψη αποφάσεων σε επίπεδο ΕΕ. Προς τον σκοπό αυτό, η Προεδρία μπορεί να συγκαλεί άτυπη συνάντηση στρογγυλής τραπέζης. Η Προεδρία προβαίνει σε αρχικό προσδιορισμό των τομέων που απαιτούν συμμετοχή της ΕΜΑ ή του Συμβουλίου. Τούτο θα αποτελέσει τη βάση των κατευθυντήριων οδηγιών για την κατάρτιση ολοκληρωμένων εκθέσεων επίγνωσης των δυνατοτήτων και ανάλυσης της κατάστασης (ISAA). Η Προεδρία θα αποφασίζει, με βάση τα χαρακτηριστικά και τις πιθανές συνέπειες της κρίσης, καθώς και τις συναφείς πολιτικές ανάγκες, κατά πόσον ενδείκνυται σύγκληση συνεδριάσεων των αρμόδιων ομάδων εργασίας του Συμβουλίου και/ή της ΕΜΑ και/ή της ΕΠΑ.

  — **Προσχέδιο:**

    — Συμμετέχοντες στη συζήτηση στρογγυλής τραπέζης:

      — οι υπηρεσίες της Επιτροπής και η ΕΥΕΔ θα παρέχουν συμβουλές στην Προεδρία σχετικά με τους αντίστοιχους τομείς αρμοδιοτήτων τους,

      — οι εκπρόσωποι των κρατών μελών στο πλαίσιο της οριζόντιας ομάδας εργασίας για θέματα κυβερνοχώρου, με την υποστήριξη εμπειρογνωμόνων από τις πρωτεύουσες (CSIRT, αρμόδιες αρχές για την ασφάλεια στον κυβερνοχώρο κ.ά.),

      — πολιτική/στρατηγική καθοδήγηση για τις εκθέσεις ISAA βάσει των πλέον πρόσφατων εκθέσεων για την κατάσταση σε σχέση με περιστατικά ασφάλειας του κυβερνοχώρου στην ΕΕ, καθώς και συμπληρωματικών πληροφοριών που παρέχουν οι συμμετέχοντες στη συζήτηση στρογγυλής τραπέζης,

      — σχετικές ομάδες εργασίας και επιτροπές:

        — οριζόντια ομάδα εργασίας για θέματα κυβερνοχώρου.

  Η Επιτροπή, η ΕΥΕΔ και η ΓΓΣ, σε πλήρη συμφωνία και με σύμπραξη της Προεδρίας, μπορούν επίσης να αποφασίζουν την ενεργοποίηση των IPCR σε λειτουργία ανταλλαγής πληροφοριών, δημιουργώντας μια ιστοσελίδα κρίσης, ώστε να προετοιμαστεί το έδαφος για ενδεχόμενη πλήρη ενεργοποίηση.

— **Βήμα 4 — Ενεργοποίηση IPCR / Συλλογή και ανταλλαγή πληροφοριών**: με την ενεργοποίηση (είτε στον τρόπο λειτουργίας που περιλαμβάνει μόνο την ανταλλαγή πληροφοριών είτε στην πλήρη ενεργοποίηση) δημιουργείται, στη διαδικτυακή πλατφόρμα IPCR, σελίδα κρίσης που επιτρέπει να πραγματοποιούνται ειδικές ανταλλαγές πληροφοριών οι οποίες επικεντρώνονται σε πτυχές που μπορούν να αξιοποιηθούν στην ISAA και συμβάλλουν στην προετοιμασία του διαλόγου σε πολιτικό επίπεδο. Το ποια είναι η επικεφαλής υπηρεσία ISAA (μία από τις υπηρεσίες της Επιτροπής ή η ΕΥΕΔ) εξαρτάται από τις περιστάσεις της υπόθεσης.

— **Βήμα 5 — Εκπόνηση της ISAA**: ξεκινά η εκπόνηση των εκθέσεων ISAA. Η Επιτροπή / Η ΕΥΕΔ εκδίδουν τις εκθέσεις ISAA, όπως περιγράφεται συνοπτικά στις τυποποιημένες επιχειρησιακές διαδικασίες ISAA, και μπορούν περαιτέρω να

([1]) Η έκθεση για την κατάσταση στην ΕΕ σχετικά με τα περιστατικά που θέτουν σε κίνδυνο την ασφάλεια στον κυβερνοχώρο αποτελεί συμπίληση εκθέσεων που υποβάλλουν οι εθνικές CSIRT. Ο μορφότυπος της έκθεσης πρέπει να περιγράφεται στις τυποποιημένες επιχειρησιακές διαδικασίες SOP του δικτύου CSIRT.

προωθούν την ανταλλαγή πληροφοριών στη διαδικτυακή πλατφόρμα IPCR ή να υποβάλλουν ειδικά αιτήματα για πληροφορίες. Οι εκθέσεις ISAA προσαρμόζονται στις ανάγκες που υπάρχουν σε πολιτικό επίπεδο (δηλαδή στην ΕΜΑ ή στο Συμβούλιο), όπως καθορίζονται από την Προεδρία και καταρτίζονται υπό την καθοδήγησή της, καθιστώντας έτσι δυνατή τη στρατηγική επισκόπηση της κατάστασης και τον εμπεριστατωμένο διάλογο επί των σημείων της ημερήσιας διάταξης που καθορίζει η Προεδρία. Σύμφωνα με τις τυποποιημένες επιχειρησιακές διαδικασίες ISAA, ο χαρακτήρας μιας κρίσης στον κυβερνοχώρο είναι αυτός που καθορίζει κατά πόσον η έκθεση ISAA εκπονείται από μία από τις υπηρεσίες της Επιτροπής (ΓΔ CNECT, ΓΔ HOME) ή από την ΕΥΕΔ.

Κατόπιν της ενεργοποίησης της διαδικασίας IPCR, η Προεδρία σκιαγραφεί τους ειδικούς τομείς ενδιαφέροντος για την ISAA, ώστε αυτή να υποστηρίξει τον πολιτικό συντονισμό και/ή τη διαδικασία λήψης απόφασης στο Συμβούλιο. Η Προεδρία προσδιορίζει επίσης τον χρόνο υποβολής της έκθεσης, μετά από διαβουλεύσεις με τις υπηρεσίες της Επιτροπής / την ΕΥΕΔ.

— **Προσχέδιο:**

— Η έκθεση ISAA περιλαμβάνει συνεισφορές από τις συναφείς υπηρεσίες, στις οποίες συγκαταλέγονται:

— το δίκτυο CSIRT, που συνεισφέρει μέσω έκθεσης της ΕΕ σχετικά με περιστατικά που θέτουν σε κίνδυνο την ασφάλεια στον κυβερνοχώρο,

— το EC3, το SITROOM, η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ, η CERT-EU. Η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ παρέχει στήριξη και συνεισφορές στην επικεφαλής υπηρεσία ISAA και στη συζήτηση στρογγυλής τραπέζης IPCR, κατά περίπτωση,

— τα όργανα και οι οργανισμοί της ΕΕ ανά τομέα, ανάλογα με τους τομείς που επηρεάζονται,

— οι αρχές των κρατών μελών (πέραν των CSIRT).

— Συγκέντρωση των συνεισφορών ISAA ([1]):

— Η Επιτροπή και οργανισμοί της ΕΕ: το πληροφοριακό σύστημα ARGUS αποτελεί το εσωτερικό δίκτυο κορμού για την ISAA. Τα όργανα της ΕΕ αποστέλλουν τις συνεισφορές τους στις αντίστοιχες αρμόδιες ΓΔ, οι οποίες με τη σειρά τους τροφοδοτούν τις σχετικές πληροφορίες στο σύστημα ARGUS. Οι υπηρεσίες και τα όργανα της Επιτροπής συγκεντρώνουν πληροφορίες από υπάρχοντα τομεακά δίκτυα με κράτη μέλη και διεθνείς οργανισμούς και από άλλες σχετικές πηγές.

— Για την ΕΥΕΔ: η Αίθουσα Διαχείρισης Κρίσεων της ΕΕ, που υποστηρίζεται από άλλες σχετικές υπηρεσίες της ΕΥΕΔ, αποτελεί το εσωτερικό δίκτυο κορμού και το ενιαίο σημείο επαφής για την ISAA. Η ΕΥΕΔ συλλέγει πληροφορίες από τρίτες χώρες και σχετικούς διεθνείς οργανισμούς.

— **Βήμα 6 — Προετοιμασία της άτυπης συνάντησης στρογγυλής τραπέζης της Προεδρίας**: η Προεδρία, επικουρούμενη από τη Γενική Γραμματεία του Συμβουλίου, καθορίζει το χρονοδιάγραμμα, την ημερήσια διάταξη, τους συμμετέχοντες και τα αναμενόμενα αποτελέσματα (πιθανά παραδοτέα) της άτυπης συνάντησης στρογγυλής τραπέζης της Προεδρίας. Η ΓΣ κοινοποιεί τις σχετικές πληροφορίες στη διαδικτυακή πλατφόρμα IPCR εξ ονόματος της Προεδρίας και, κυρίως, συγκαλεί τη συνεδρίαση.

— **Βήμα 7 — Στρογγυλή τράπεζα της Προεδρίας / προπαρασκευαστικά μέτρα για τον πολιτικό συντονισμό / τη λήψη αποφάσεων της ΕΕ**: η Προεδρία συγκαλεί άτυπη συνάντηση στρογγυλής τραπέζης για την εξέταση της κατάστασης και για την προετοιμασία και επανεξέταση των στοιχείων που πρέπει να επισημανθούν στην ΕΜΑ ή στο Συμβούλιο. Η άτυπη συζήτηση στρογγυλής τραπέζης της Προεδρίας αποτελεί επίσης το φόρουμ όπου εκπονούνται, επανεξετάζονται και συζητώνται όλες οι προτάσεις για δράση που υποβάλλονται στην ΕΜΑ / στο Συμβούλιο.

— **Προσχέδιο:**

— Η οριζόντια ομάδα εργασίας του Συμβουλίου για θέματα του κυβερνοχώρου αναλαμβάνει να προετοιμάσει την ΕΠΑ ή την ΕΜΑ.

— **Βήμα 8 — Πολιτικός συντονισμός και λήψη αποφάσεων στην ΕΜΑ / στο Συμβούλιο**: τα αποτελέσματα των συνεδριάσεων της ΕΜΑ / του Συμβουλίου αφορούν τον συντονισμό των δραστηριοτήτων αντίδρασης σε όλα τα επίπεδα, τις αποφάσεις σχετικά με έκτακτα μέτρα, τις πολιτικές δηλώσεις κ.λπ. Οι αποφάσεις αυτές αποτελούν επίσης επικαιροποιημένη πολιτική/στρατηγική καθοδήγηση για την περαιτέρω εκπόνηση εκθέσεων ISAA.

— **Προσχέδιο:**

— Η πολιτική απόφαση για τον συντονισμό της αντίδρασης σε περίπτωση κρίσης στον κυβερνοχώρο υλοποιείται μέσω των δραστηριοτήτων (που εκτελούνται από τους αντίστοιχους φορείς) που περιγράφονται ανωτέρω στο τμήμα 1 «Συνεργασία σε στρατηγικό/πολιτικό, επιχειρησιακό και τεχνικό επίπεδο» όσον αφορά την **αντίδραση** και την **επικοινωνία με το κοινό**.

— Η εκπόνηση έκθεσης ISAA εξακολουθεί να βασίζεται στη συνεργασία σε τεχνικό, επιχειρησιακό και πολιτικό/στρατηγικό επίπεδο όσον αφορά την **επίγνωση της κατάστασης**, που επίσης περιγράφονται στο τμήμα 1 ανωτέρω.

([1]) Τυποποιημένες επιχειρησιακές διαδικασίες ISAA.

— **Βήμα 9 — Παρακολούθηση των επιπτώσεων**: η επικεφαλής υπηρεσία ISAA παρέχει, με την υποστήριξη όσων συνεισφέρουν στην ISAA, πληροφορίες για την εξέλιξη της κρίσης και για τις επιπτώσεις των πολιτικών αποφάσεων που ελήφθησαν. Αυτή η ανατροφοδότηση υποστηρίζει μια διαδικασία εν εξελίξει και στηρίζει την απόφαση της Προεδρίας για τη συνέχιση της συμμετοχής της ΕΕ σε πολιτικό επίπεδο ή για την αποκλιμάκωση των IPCR.

— **Βήμα 10 — Αποκλιμάκωση:** ακολουθώντας την ίδια διαδικασία με την ενεργοποίηση, η Προεδρία δύναται να συγκαλεί άτυπη συνάντηση στρογγυλής τραπέζης για να αξιολογείται αν οι IPCR πρέπει να διατηρηθούν ενεργές ή όχι. Η Προεδρία δύναται να αποφασίσει να περατώσει ή να υποβαθμίσει την ενεργοποίηση.

— **Προσχέδιο:**

— Ο ENISA μπορεί να προσκαλείται να συνεισφέρει ή να προβεί σε εκ των υστέρων τεχνική έρευνα του περιστατικού, σύμφωνα με τις διατάξεις της εντολής του.

ΠΡΟΣΑΡΤΗΜΑ

1. ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ, ΜΗΧΑΝΙΣΜΟΙ ΣΥΝΕΡΓΑΣΙΑΣ ΚΑΙ ΦΟΡΕΙΣ ΣΕ ΕΠΙΠΕΔΟ ΕΕ

Μηχανισμοί διαχείρισης κρίσεων

Ολοκληρωμένες ρυθμίσεις για την πολιτική αντιμετώπιση των κρίσεων (IPCR): οι ολοκληρωμένες ρυθμίσεις για την πολιτική αντιμετώπιση των κρίσεων (IPCR) που ενέκρινε το Συμβούλιο στις 25 Ιουνίου 2013 [1] είναι σχεδιασμένες ώστε να διευκολύνουν τον έγκαιρο συντονισμό και την αντίδραση σε πολιτικό επίπεδο της ΕΕ σε περίπτωση μείζονος κρίσης. Οι IPCR στηρίζουν επίσης τον συντονισμό σε πολιτικό επίπεδο της αντίδρασης σε περίπτωση επίκλησης της ρήτρας αλληλεγγύης (άρθρο 222 της ΣΛΕΕ), όπως ορίζεται στην απόφαση 2014/415/ΕΕ του Συμβουλίου σχετικά με την εφαρμογή από την Ένωση της ρήτρας αλληλεγγύης, που εκδόθηκε στις 24 Ιουνίου 2014. Στις τυποποιημένες επιχειρησιακές διαδικασίες (SOP) των IPCR [2] καθορίζεται η διαδικασία ενεργοποίησης και οι επόμενες δράσεις που πρέπει να αναληφθούν.

ARGUS: το σύστημα συντονισμού σε περίπτωση κρίσεων που δημιουργήθηκε από την Ευρωπαϊκή Επιτροπή το 2005 για να παρέχει ειδική διαδικασία συντονισμού σε περίπτωση μείζονος πολυτομεακής κρίσης. Υποστηρίζεται από γενικό σύστημα έγκαιρης προειδοποίησης (εργαλείο ΤΠ) με το ίδιο όνομα. Το ARGUS προβλέπει δύο φάσεις· στη φάση ΙΙ (σε περίπτωση μείζονος πολυτομεακής κρίσης) δρομολογούνται συνεδριάσεις της Επιτροπής Συντονισμού Κρίσεων (CCC) υπό τον πρόεδρο της Επιτροπής ή τον επίτροπο στον οποίο έχει ανατεθεί η εν λόγω αρμοδιότητα. Η CCC απαρτίζεται από εκπροσώπους των αρμόδιων ΓΔ της Επιτροπής, των γραφείων των επιτρόπων και άλλων υπηρεσιών της ΕΕ, και έχει ως στόχο να κατευθύνει και να συντονίσει την αντίδραση της Επιτροπής στην κρίση. Με πρόεδρο τον αναπληρωτή γενικό γραμματέα, η CCC αξιολογεί την κατάσταση, εξετάζει τις διαθέσιμες επιλογές και λαμβάνει αποφάσεις που είναι δυνατό να αποτελέσουν αντικείμενο προσφυγής όσον αφορά τα εργαλεία και τα μέσα της ΕΕ υπό την ευθύνη της Επιτροπής, διασφαλίζοντας την εφαρμογή των αποφάσεων [3] [4].

Μηχανισμός αντιμετώπισης κρίσεων της ΕΥΕΔ: ο μηχανισμός αντιμετώπισης κρίσεων της ΕΥΕΔ είναι ένα διαρθρωμένο σύστημα της ΕΥΕΔ για την αντιμετώπιση κρίσεων και καταστάσεων έκτακτης ανάγκης με εξωτερικό χαρακτήρα ή σημαντική εξωτερική διάσταση —συμπεριλαμβανομένων των υβριδικών απειλών— που επηρεάζουν, δυνητικά ή πραγματικά, τα συμφέροντα της ΕΕ ή οποιωνδήποτε κρατών μελών. Με την εξασφάλιση της συμμετοχής αρμόδιων υπαλλήλων της Επιτροπής καθώς και της Γραμματείας του Συμβουλίου στις συνεδριάσεις του, ο μηχανισμός αντιμετώπισης κρίσεων διευκολύνει τη συνέργεια μεταξύ προσπαθειών στο επίπεδο της διπλωματίας, της ασφάλειας και της άμυνας και χρηματοπιστωτικών, εμπορικών και συνεργατικών μέσων που διαχειρίζεται η Επιτροπή. Η μονάδα αντιμετώπισης κρίσεων μπορεί να ενεργοποιείται για όσο διάστημα διαρκεί η κρίση.

Μηχανισμοί συνεργασίας

Δίκτυο CSIRT: το δίκτυο ομάδων παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών συγκεντρώνει το σύνολο των εθνικών και κυβερνητικών CSIRT και CERT-ΕΕ. Σκοπός του δικτύου είναι να καταστεί δυνατή και να ενισχυθεί η ανταλλαγή πληροφοριών μεταξύ των CSIRT για απειλές και συμβάντα που αφορούν την ασφάλεια στον κυβερνοχώρο, καθώς και η συνεργασία για την αντιμετώπιση περιστατικών και κρίσεων που αφορούν την ασφάλεια στον κυβερνοχώρο.

Οριζόντια ομάδα εργασίας του Συμβουλίου για θέματα κυβερνοχώρου: η ομάδα εργασίας συστάθηκε για να διασφαλιστεί ο στρατηγικός και οριζόντιος συντονισμός όσον αφορά ζητήματα πολιτικής του κυβερνοχώρου στο Συμβούλιο και μπορεί να συμμετέχει σε νομοθετικές και μη νομοθετικές δραστηριότητες.

Παράγοντες

ENISA: ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών ιδρύθηκε το 2004. Ο Οργανισμός συνεργάζεται στενά με τα κράτη μέλη και τον ιδιωτικό τομέα για να παρέχει συμβουλές και λύσεις σχετικά με ζητήματα όπως οι πανευρωπαϊκές ασκήσεις ασφάλειας στον κυβερνοχώρο, η χάραξη εθνικών στρατηγικών για την ασφάλεια στον κυβερνοχώρο, η συνεργασία των CSIRT και η ανάπτυξη ικανοτήτων. Ο ENISA συνεργάζεται απευθείας με τις CSIRT ανά την ΕΕ και αποτελεί τη γραμματεία του δικτύου CSIRT.

ΚΣΑΕΑ: το Κέντρο Συντονισμού Αντιμετώπισης Εκτάκτων Αναγκών της Επιτροπής (στη Γενική Διεύθυνση Ανθρωπιστικής Βοήθειας και Πολιτικής Προστασίας — ΓΔ ECHO) στηρίζει και συντονίζει ευρύ φάσμα δραστηριοτήτων πρόληψης, ετοιμότητας και αντιμετώπισης σε 24ωρη και καθημερινή βάση. Εγκαινιάστηκε το 2013 και ενεργεί ως κόμβος της Επιτροπής για την αντιμετώπιση κρίσεων (συνδέεται με άλλες αίθουσες διαχείρισης κρίσεων της ΕΕ), καθώς και ως το κεντρικό, σε 24ωρη και καθημερινή βάση, σημείο επαφής των IPCR.

---

[1] 10708/13 για την «Ολοκλήρωση της διαδικασίας επανεξέτασης των ρυθμίσεων της ΕΕ για τον συντονισμό σε καταστάσεις έκτακτης ανάγκης και κρίσεις», που εγκρίθηκε από το Συμβούλιο στις 24 Ιουνίου 2013.

[2] 12607/15 «Τυποποιημένες επιχειρησιακές διαδικασίες IPCR», που συμφωνήθηκαν από την ομάδα «Φίλοι της Προεδρίας» και τις οποίες έλαβε υπόψη η ΕΜΑ τον Οκτώβριο του 2015.

[3] Διατάξεις της Επιτροπής σχετικά με το γενικό σύστημα έγκαιρης προειδοποίησης «ARGUS», COM(2005) 662 τελικό, 23 Δεκεμβρίου 2005.

[4] Απόφαση 2006/25/ΕΚ, Ευρατόμ της Επιτροπής, της 23ης Δεκεμβρίου 2005, που τροποποιεί τον εσωτερικό της κανονισμό (ΕΕ L 19 της 24.1.2006, σ. 20) για τη θέσπιση του γενικού συστήματος έγκαιρης προειδοποίησης «ARGUS».

Ευρωπόλ/EC3: το Ευρωπαϊκό Κέντρο για τα Εγκλήματα στον Κυβερνοχώρο (EC3), που συστάθηκε το 2013 στο πλαίσιο της Ευρωπόλ, στηρίζει την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο στην ΕΕ από την πλευρά των αρχών επιβολής του νόμου. Το EC3 παρέχει επιχειρησιακή και αναλυτική στήριξη σε έρευνες των κρατών μελών και λειτουργεί ως κεντρικός κόμβος για εγκληματολογικές πληροφορίες και στοιχεία που στηρίζουν επιχειρήσεις και έρευνες των κρατών μελών με επιχειρησιακή ανάλυση, συντονισμό και εμπειρογνωμοσύνη, καθώς και άκρως εξειδικευμένες τεχνικές ικανότητες και ικανότητες ψηφιακής εγκληματολογικής στήριξης.

CERT-ΕΕ: η ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ έχει αποστολή να βελτιώσει την προστασία των θεσμικών οργάνων και οργανισμών της ΕΕ έναντι των απειλών στον κυβερνοχώρο. Είναι μέλος του δικτύου CSIRT. Η CERT-ΕΕ έχει συνάψει τεχνικές συμφωνίες για την ανταλλαγή πληροφοριών σχετικά με απειλές στον κυβερνοχώρο με την ομάδα CIRC (ομάδα αντιμετώπισης συμβάντων πληροφορικής) του ΝΑΤΟ, με ορισμένες τρίτες χώρες και με κύριους εμπορικούς παράγοντες στον τομέα της ασφάλειας στον κυβερνοχώρο.

Η κοινότητα των υπηρεσιών πληροφοριών της ΕΕ περιλαμβάνει το Κέντρο Ανάλυσης Πληροφοριών της ΕΕ (**INTCEN**) και τη Διεύθυνση Πληροφοριών του Στρατιωτικού Επιτελείου της ΕΕ (EUMS INT), στο πλαίσιο της συμφωνίας της **Ενιαίας Ικανότητας Ανάλυσης Πληροφοριών** (SIAC). Αποστολή της SIAC είναι η παροχή αναλύσεων πληροφοριών, έγκαιρης προειδοποίησης και επίγνωσης της κατάστασης στην Ύπατη Εκπρόσωπο της Ευρωπαϊκής Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας και στην Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ). Η SIAC παρέχει τις υπηρεσίες της στα διάφορα όργανα λήψης αποφάσεων της ΕΕ στους τομείς της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας (ΚΕΠΠΑ), της κοινής πολιτικής ασφαλείας και άμυνας (ΚΠΑΑ) και της καταπολέμησης της τρομοκρατίας (CT), καθώς και στα κράτη μέλη. Το INTCEN της ΕΕ και η EUMS INT δεν αποτελούν επιχειρησιακούς οργανισμούς και δεν έχουν καμία δυνατότητα συλλογής στοιχείων. Το επιχειρησιακό επίπεδο των υπηρεσιών πληροφοριών αποτελεί ευθύνη των κρατών μελών. Η SIAC ασχολείται μόνο με τη στρατηγική ανάλυση.

Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ: με την κοινή ανακοίνωση του Απριλίου 2016 για την αντιμετώπιση υβριδικών απειλών η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ (HFC της ΕΕ) ορίζεται ως το σημείο αναφοράς για κάθε ανάλυση πηγής σχετικά με υβριδικές απειλές στην ΕΕ· η εντολή της εγκρίθηκε τον Δεκέμβριο του 2016 από την Επιτροπή μέσω διαβούλευσης μεταξύ των υπηρεσιών. Με έδρα στο INTCEN, η Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ αποτελεί μέρος της SIAC και, ως εκ τούτου, συνεργάζεται με την EUMS INT και διαθέτει μόνιμο στρατιωτικό υπάλληλο. Ο υβριδικός χαρακτήρας αναφέρεται στην εσκεμμένη χρήση, από κράτος ή μη κρατικό φορέα, ενός συνδυασμού πολλαπλών συγκεκαλυμμένων/εμφανών, στρατιωτικών/πολιτικών εργαλείων και μηχανισμών, όπως επιθέσεις στον κυβερνοχώρο, εκστρατείες παραπληροφόρησης, κατασκοπία, οικονομική πίεση, χρήση ενδιάμεσων δυνάμεων ή άλλη ανατρεπτική δραστηριότητα. Η HFC της ΕΕ συνεργάζεται με εκτεταμένο δίκτυο σημείων επαφής (PoCs), τόσο εντός της Επιτροπής όσο και εντός των κρατών μελών, για να παρέχει την ολοκληρωμένη αντίδραση / το σύνολο της κρατικής προσέγγισης που απαιτείται για την αντιμετώπιση ποικίλων προκλήσεων.

Αίθουσα Διαχείρισης Κρίσεων της ΕΕ: η Αίθουσα Διαχείρισης Κρίσεων της ΕΕ αποτελεί μέρος του Κέντρου Ανάλυσης Πληροφοριών της ΕΕ (INTCEN) και παρέχει στην ΕΥΕΔ την επιχειρησιακή ικανότητα να εξασφαλίζει άμεση και αποτελεσματική αντίδραση σε κρίσεις. Πρόκειται για μόνιμο πολιτικοστρατιωτικό όργανο επιφυλακής που παρέχει παγκόσμια παρακολούθηση και επίγνωση καταστάσεων με ικανότητα 24ωρης και καθημερινής λειτουργίας.

Συναφή μέσα

Πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο: το πλαίσιο, που συμφωνήθηκε τον Ιούνιο του 2017, αποτελεί μέρος της προσέγγισης της ΕΕ για τη διπλωματία στον κυβερνοχώρο, η οποία συμβάλλει στην πρόληψη συγκρούσεων, στον μετριασμό απειλών για την ασφάλεια στον κυβερνοχώρο και στη βελτίωση της σταθερότητας στις διεθνείς σχέσεις. Το πλαίσιο αξιοποιεί πλήρως μέτρα βάσει της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας, καθώς και, εφόσον είναι αναγκαίο, περιοριστικά μέτρα. Η χρήση των μέτρων εντός του πλαισίου αναμένεται να ενθαρρύνει τη συνεργασία, να διευκολύνει τον μετριασμό άμεσων και μακροπρόθεσμων απειλών και να επηρεάσει τη συμπεριφορά των δραστών και εν δυνάμει δραστών μακροπρόθεσμα.

2. ΣΥΝΤΟΝΙΣΜΟΣ ΣΕ ΚΑΤΑΣΤΑΣΕΙΣ ΚΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΣΥΜΦΩΝΑ ΜΕ ΤΙΣ ΡΥΘΜΙΣΕΙΣ IPCR — ΟΡΙΖΟΝΤΙΟ ΕΠΙΠΕΔΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΑΙ ΠΟΛΙΤΙΚΗ ΚΛΙΜΑΚΩΣΗ

Οι ρυθμίσεις IPCR μπορούν να χρησιμοποιηθούν (και έχουν χρησιμοποιηθεί) για την αντιμετώπιση τεχνικών και επιχειρησιακών ζητημάτων, αλλά πάντοτε από πολιτική/στρατηγική άποψη.

Όσον αφορά την κλιμάκωση, οι IPCR μπορούν να χρησιμοποιηθούν ανάλογα με το επίπεδο της κρίσης με τη μετάβαση από «λειτουργία παρακολούθησης» σε «λειτουργία ανταλλαγής πληροφοριών», που αποτελεί το πρώτο επίπεδο ενεργοποίησης των IPCR, και σε «πλήρη ενεργοποίηση των IPCR».

Η πλήρης ενεργοποίηση αποφασίζεται από την εκ περιτροπής Προεδρία του Συμβουλίου της ΕΕ. Η Επιτροπή, η ΕΥΕΔ και η ΓΓΣ μπορούν να ενεργοποιήσουν τις IPCR σε κατάσταση λειτουργίας ανταλλαγής πληροφοριών. Η παρακολούθηση και η ανταλλαγή

πληροφοριών ενεργοποιούν διάφορα επίπεδα ανταλλαγής πληροφοριών, ενώ η ανταλλαγή πληροφοριών ενεργοποιεί αίτημα για την εκπόνηση εκθέσεων ISAA. Η πλήρης ενεργοποίηση προσθέτει συνεδριάσεις στρογγυλής τραπέζης στο πλαίσιο των IPCR στα διαθέσιμα εργαλεία, φέρνοντας στο τραπέζι την Προεδρία (κατά κανόνα το προεδρείο της ΕΜΑ ΙΙ ή εμπειρογνώμονα επί του θέματος σε επίπεδο Συμβούλου Μόνιμης Αντιπροσωπείας, αλλά, κατ' εξαίρεση, πραγματοποιούνται συζητήσεις στρογγυλής τραπέζης σε υπουργικό επίπεδο).

Παράγοντες

Η εκ περιτροπής Προεδρία (κατά κανόνα το προεδρείο της ΕΜΑ) έχει ηγετικό ρόλο.

Για το Ευρωπαϊκό Συμβούλιο, το Γραφείο του Προέδρου.

Για την Ευρωπαϊκή Επιτροπή, επίπεδο αναπληρωτή ΓΓ/ΓΔ και/ή εμπειρογνώμονες επί του θέματος.

Για την ΕΥΕΔ, επίπεδο αναπληρωτή ΓΓ/ΕΔ και/ή εμπειρογνώμονες επί του θέματος.

Για τη ΓΓΣ, το Γραφείο του ΓΓ, η ομάδα IPCR και οι αρμόδιες ΓΔ.

Πεδίο δραστηριοτήτων: Δημιουργία κοινής ολοκληρωμένης εικόνας της κατάστασης και κλιμάκωση της επίγνωσης σχετικά με προβλήματα ή ελλείψεις σε καθένα από τα τρία επίπεδα για την αντιμετώπισή τους σε πολιτικό επίπεδο, λήψη αποφάσεων κατά τις συνεδριάσεις, αν οι αποφάσεις αυτές εμπίπτουν στην αρμοδιότητα των συμμετεχόντων, ή δημιουργία προτάσεων για τη λήψη μέτρων που απευθύνονται στην ΕΜΑ ΙΙ και μέχρι και το Συμβούλιο.

Κοινή επίγνωση της κατάστασης:

(Μη ενεργή): είναι δυνατή η δημιουργία σελίδων παρακολούθησης των IPCR για την παρακολούθηση εξελισσόμενων καταστάσεων οι οποίες ενδέχεται να κλιμακωθούν σε κρίση με επιπτώσεις για την ΕΕ.

(Ανταλλαγή πληροφοριών των IPCR): οι εκθέσεις ISAA θα συντάσσονται από τον επικεφαλής της ISAA με βάση στοιχεία από τις υπηρεσίες της Επιτροπής, την ΕΥΕΔ και τα κράτη μέλη (μέσω των ερωτηματολογίων IPCR).

(Πλήρης ενεργοποίηση των IPCR): πέραν των εκθέσεων ISAA, οι άτυπες συνεδριάσεις στρογγυλής τραπέζης στο πλαίσιο των IPCR συγκεντρώνουν διάφορους ενδιαφερόμενους φορείς από τα κράτη μέλη, την Επιτροπή, την ΕΥΕΔ, τους αρμόδιους οργανισμούς κ.λπ., για να συζητήσουν τις ελλείψεις και τα προβλήματα.

Συνεργασία και αντιμετώπιση:

Ενεργοποίηση/συγχρονισμός πρόσθετων μηχανισμών/μέσων διαχείρισης κρίσεων ανάλογα με τη φύση και τον αντίκτυπο του περιστατικού. Σε αυτούς τους μηχανισμούς / τα μέσα είναι δυνατό να περιλαμβάνονται, για παράδειγμα, ο μηχανισμός πολιτικής προστασίας, το πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο ή το «κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών».

Επικοινωνίες σε καταστάσεις κρίσης:

Το δίκτυο αρμόδιων επικοινωνίας σε καταστάσεις κρίσης στο πλαίσιο των IPCR μπορεί να ενεργοποιηθεί από την Προεδρία, ύστερα από διαβούλευση με τις αρμόδιες υπηρεσίες της Επιτροπής, της ΓΓΣ και της ΕΥΕΔ, ώστε να υποστηριχθεί η δημιουργία κοινών μηνυμάτων ή να αναζητηθούν τα πλέον αποτελεσματικά μέσα επικοινωνίας.

3. ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ARGUS — ΑΝΤΑΛΛΑΓΗ ΠΛΗΡΟΦΟΡΙΩΝ ΕΝΤΟΣ ΤΗΕΥΡΩΠΑΪΚΗΣ ΕΠΙΤΡΟΠΗΣ

Αντιμέτωπη με απρόβλεπτες κρίσεις που απαιτούσαν δράση σε ευρωπαϊκό επίπεδο, όπως οι τρομοκρατικές επιθέσεις στη Μαδρίτη (Μάρτιος 2004), το τσουνάμι στη Νοτιοανατολική Ασία (Δεκέμβριος 2004) και οι τρομοκρατικές επιθέσεις στο Λονδίνο (Ιούλιος 2005), το 2005 η Επιτροπή θέσπισε το σύστημα συντονισμού ARGUS, το οποίο υποστηρίζεται από το ομώνυμο γενικό σύστημα έγκαιρης προειδοποίησης ([1]) ([2]). Στόχος του είναι να παρέχει μια ειδική **διαδικασία συντονισμού κρίσεων** σε περίπτωση μείζονος κρίσης που θίγει πολλαπλούς τομείς, ώστε να είναι δυνατή η ανταλλαγή σχετικών με την κρίση πληροφοριών σε πραγματικό χρόνο και να διασφαλίζεται η ταχεία λήψη αποφάσεων.

Το ARGUS ορίζει δύο φάσεις, ανάλογα με τη σοβαρότητα του συμβάντος:

Φάση Ι: χρησιμοποιείται για «ανταλλαγή πληροφοριών» σε κρίσεις περιορισμένης κλίμακας

([1]) Επιτροπή των Ευρωπαϊκών Κοινοτήτων, 23 Δεκεμβρίου 2005, Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή των Περιφερειών: Διατάξεις της Επιτροπής για το γενικό σύστημα έγκαιρης προειδοποίησης «ARGUS», COM(2005) 662 final.

([2]) Απόφαση 2006/25/ΕΚ, Ευρατόμ.

Στα παραδείγματα πρόσφατα αναφερθέντων συμβάντων της φάσης Ι περιλαμβάνονται οι δασικές πυρκαγιές στην Πορτογαλία και το Ισραήλ, η επίθεση στο Βερολίνο το 2016, οι πλημμύρες στην Αλβανία, ο τυφώνας Matthew στην Αϊτή και η ξηρασία στη Βολιβία. Οποιαδήποτε ΓΔ μπορεί να κινήσει τη διαδικασία για συμβάν της φάσης Ι όταν κρίνει ότι μια κατάσταση που υπάγεται στον τομέα αρμοδιότητάς της είναι αρκούντως σοβαρή ώστε να δικαιολογεί την ανταλλαγή πληροφοριών ή να επωφελείται από αυτή. Για παράδειγμα, η ΓΔ CNECT ή η ΓΔ HOME μπορεί να κινήσει τη διαδικασία για συμβάν της φάσης Ι όταν κρίνει ότι μια κατάσταση που υπάγεται στον τομέα αρμοδιότητάς της είναι αρκούντως σοβαρή ώστε να δικαιολογείται η ανταλλαγή πληροφοριών ή η αξιοποίηση αυτών.

Φάση ΙΙ: ενεργοποιείται σε περίπτωση σοβαρής κρίσης που θίγει πολλαπλούς τομείς ή προβλεπόμενης ή επικείμενης απειλής κατά της Ένωσης.

Η φάση ΙΙ ενεργοποιεί μια ειδική διαδικασία συντονισμού που επιτρέπει στην Επιτροπή να λαμβάνει αποφάσεις και να διαχειρίζεται ταχεία, συντονισμένη και συνεκτική αντιμετώπιση, στο υψηλότερο επίπεδο εντός του πεδίου αρμοδιότητάς της και σε συνεργασία με τα άλλα όργανα. Η φάση ΙΙ προορίζεται για μείζονες κρίσεις που θίγουν πολλαπλούς τομείς ή για προβλεπόμενες ή επικείμενες απειλές που προκύπτουν από αυτές. Στα παραδείγματα πραγματικών συμβάντων της φάσης ΙΙ περιλαμβάνονται η μεταναστευτική/προσφυγική κρίση (2015 — σήμερα), η τριπλή καταστροφή στη Φουκουσίμα (2011) και η έκρηξη του ηφαιστείου *Eyjafjallajökull* στην Ισλανδία (2010).

Η φάση ΙΙ ενεργοποιείται από τον πρόεδρο με δική του πρωτοβουλία ή κατόπιν αιτήματος μέλους της Επιτροπής. Ο πρόεδρος μπορεί να αναθέσει την πολιτική ευθύνη για την αντιμετώπιση της κρίσης εκ μέρους της Επιτροπής στον επίτροπο που προΐσταται της υπηρεσίας την οποία αφορά περισσότερο η εκάστοτε κρίση, ή μπορεί να αποφασίσει να την επωμιστεί ο ίδιος.

Προβλέπει επείγουσες συνεδριάσεις της επιτροπής συντονισμού κρίσεων (ΕΣΚ). Οι εν λόγω συνεδριάσεις συγκαλούνται υπό την εποπτεία του προέδρου ή του επιτρόπου στον οποίο έχει ανατεθεί η ευθύνη. Οι συνεδριάσεις συγκαλούνται από τη ΓΓ μέσω του εργαλείου ΤΠ του ARGUS. Η επιτροπή συντονισμού κρίσεων είναι ειδική επιχειρησιακή δομή διαχείρισης κρίσεων που έχει θεσπιστεί για να κατευθύνει και να συντονίζει την αντιμετώπιση κρίσεων από την Επιτροπή και στην οποία συμμετέχουν εκπρόσωποι όλων των σχετικών γενικών διευθύνσεων, των γραφείων των επιτρόπων και άλλων υπηρεσιών της Επιτροπής. Υπό την προεδρία του αναπληρωτή γενικού γραμματέα, η **ΕΣΚ αξιολογεί την κατάσταση, εξετάζει επιλογές και λαμβάνει αποφάσεις, ενώ ταυτόχρονα διασφαλίζει ότι οι αποφάσεις και οι δράσεις υλοποιούνται,** διασφαλίζοντας παράλληλα τη συνεκτικότητα και τη συνοχή της αντιμετώπισης. Η ΓΓ παρέχει στήριξη στην ΕΣΚ.

4. ΜΗΧΑΝΙΣΜΟΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΡΙΣΕΩΝ ΤΗΣ ΕΥΕΔ

Ο μηχανισμός αντιμετώπισης κρίσεων (CRM) ενεργοποιείται όταν ανακύπτει σοβαρή κατάσταση ή έκτακτη ανάγκη που αφορά ή εμπλέκει με οποιονδήποτε τρόπο την εξωτερική διάσταση της ΕΕ. Ο CRM ενεργοποιείται από τον αναπληρωτή ΓΓ για την αντιμετώπιση κρίσεων, κατόπιν διαβούλευσης με την ΥΕ/ΑΠ ή τον γενικό γραμματέα. Η εκκίνηση του μηχανισμού αντιμετώπισης κρίσεων μπορεί επίσης να ζητηθεί στον αναπληρωτή ΓΓ για την αντιμετώπιση κρίσεων και από την ΥΕ/ΑΠ, τον ΓΓ ή άλλο αναπληρωτή ΓΓ ή ΕΔ.

Ο CRM συμβάλλει στη συνεκτικότητα της ΕΕ στην αντιμετώπιση κρίσεων στο πλαίσιο της στρατηγικής ασφαλείας. Ειδικότερα, ο CRM διευκολύνει συνέργειες μεταξύ των προσπαθειών στους τομείς της διπλωματίας, της ασφάλειας και της άμυνας, αφενός, και των χρηματοδοτικών, εμπορικών μέσων και μέσων συνεργασίας τα οποία διαχειρίζεται η Επιτροπή, αφετέρου.

Ο CRM συνδέεται με το γενικό σύστημα αντιμετώπισης καταστάσεων έκτακτης ανάγκης της Επιτροπής (ARGUS) και με τις ολοκληρωμένες ρυθμίσεις της ΕΕ για την αντιμετώπιση πολιτικών κρίσεων (IPCR) ώστε να αξιοποιούνται οι συνέργειες σε περίπτωση ταυτόχρονης ενεργοποίησης. Η Αίθουσα Διαχείρισης Κρίσεων στην ΕΥΕΔ ενεργεί ως κόμβος επικοινωνίας μεταξύ της ΕΥΕΔ και των συστημάτων αντιμετώπισης καταστάσεων έκτακτης ανάγκης στο Συμβούλιο και στην Επιτροπή.

Κατά κανόνα, η πρώτη δράση που σχετίζεται με την εφαρμογή του CRM είναι η σύγκληση **συνεδρίασης κρίσης** με τη συμμετοχή ανώτερων διοικητικών στελεχών της ΕΥΕΔ, της Επιτροπής και του Συμβουλίου που επηρεάζονται άμεσα από την εν λόγω κρίση. Η συνεδρίαση κρίσης αξιολογεί τις βραχυπρόθεσμες επιπτώσεις της κρίσης και μπορεί να συμφωνήσει ως προς την ανάληψη άμεσης δράσης ή την ενεργοποίηση του πυρήνα αντιμετώπισης κρίσεων ή τη σύγκληση πλατφόρμας κρίσεων. Οι διαδικασίες αυτές μπορούν να εφαρμοστούν με οποιαδήποτε χρονική ακολουθία.

Η **μονάδα αντιμετώπισης κρίσεων** είναι μια μικρής κλίμακας αίθουσα επιχειρήσεων, όπου συγκεντρώνονται εκπρόσωποι των υπηρεσιών της ΕΥΕΔ, της Επιτροπής και του Συμβουλίου οι οποίες εμπλέκονται στην αντιμετώπιση της κρίσης, για να παρακολουθούν συνεχώς την κατάσταση, ώστε να παρέχουν στήριξη στους υπευθύνους λήψης αποφάσεων στην κεντρική υπηρεσία της ΕΥΕΔ. Εφόσον ενεργοποιηθεί, η μονάδα αντιμετώπισης κρίσεων λειτουργεί 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα.

Στην **πλατφόρμα κρίσεων** συγκεντρώνονται οι σχετικές υπηρεσίες της ΕΥΕΔ, της Επιτροπής και του Συμβουλίου για να παρέχουν αξιολόγηση των μεσοπρόθεσμων και μακροπρόθεσμων επιπτώσεων της κρίσης και για να συμφωνήσουν τα μέτρα που πρέπει να ληφθούν. Η πλατφόρμα προεδρεύεται από την ΥΕ/ΑΠ ή τον γενικό γραμματέα ή τον αναπληρωτή ΓΓ για την αντιμετώπιση κρίσεων. Η πλατφόρμα κρίσεων αξιολογεί την αποτελεσματικότητα της δράσης της ΕΕ στις χώρες ή περιοχές σε κρίση, αποφασίζει τροποποιήσεις των πρόσθετων μέτρων και συζητά προτάσεις για δράση του Συμβουλίου. Η πλατφόρμα κρίσεων είναι μια ad hoc συνεδρίαση· ως εκ τούτου, δεν είναι μονίμως ενεργοποιημένη.

Η **επιχειρησιακή ομάδα** απαρτίζεται από εκπροσώπους των υπηρεσιών που εμπλέκονται στην αντιμετώπιση και μπορεί να ενεργοποιηθεί για να παρακολουθεί και να διευκολύνει την εφαρμογή της αντιμετώπισης εκ μέρους της ΕΕ. Αξιολογεί τον αντίκτυπο της δράσης της ΕΕ, καταρτίζει έγγραφα πολιτικής και έγγραφα επιλογών, συμβάλλει στην προετοιμασία του πολιτικού πλαισίου προσέγγισης των κρίσεων (PFCA), συμβάλλει στην επικοινωνιακή στρατηγική και προβαίνει σε ρυθμίσεις που μπορούν να διευκολύνουν την υλοποίηση της αντιμετώπισης εκ μέρους της ΕΕ.

5. ΕΓΓΡΑΦΑ ΑΝΑΦΟΡΑΣ

Ακολουθεί κατάλογος εγγράφων αναφοράς που ελήφθησαν υπόψη για την κατάρτιση του προσχεδίου:

— The European Cyber Crises Cooperation Framework, έκδοση 1, 17 Οκτωβρίου 2012

— Report on Cyber Crisis Cooperation and Management, ENISA, 2014

— Actionable Information for Security Incident Response, ENISA, 2014

— Common practices of EU-level crisis management and applicability to cyber crises, ENISA, 2015

— Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, 2016

— Τυποποιημένες Επιχειρησιακές Διαδικασίες της ΕΕ για τον κυβερνοχώρο, ENISA, 2016

— A good practice guide of using taxonomies in incident prevention and detection, ENISA, 2017

— Ανακοίνωση για την ενίσχυση του συστήματος κυβερνοανθεκτικότητας της Ευρώπης και προώθηση ανταγωνιστικού και καινοτόμου κλάδου ασφάλειας στον κυβερνοχώρο, COM(2016) 410 final, 5 Ιουλίου 2016

— Συμπεράσματα του Συμβουλίου σχετικά με την ενίσχυση του ευρωπαϊκού συστήματος ανθεκτικότητας στον κυβερνοχώρο και την προώθηση ενός ανταγωνιστικού και καινοτόμου κλάδου κυβερνοασφάλειας — Συμπεράσματα του Συμβουλίου (15 Νοεμβρίου 2016), 14540/16

— Απόφαση 2014/415/ΕΕ του Συμβουλίου, της 24ης Ιουνίου 2014, σχετικά με τις ρυθμίσεις για την εφαρμογή από την Ένωση της ρήτρας αλληλεγγύης (ΕΕ L 192 της 1.7.2014, σ. 53)

— Ολοκλήρωση της διαδικασίας επανεξέτασης των ρυθμίσεων της ΕΕ για το συντονισμό σε καταστάσεις έκτακτης ανάγκης και κρίσεις (CCA): οι ρυθμίσεις της ΕΕ για την ολοκληρωμένη αντιμετώπιση πολιτικών κρίσεων (IPCR), 10708/13, 7 Ιουνίου 2013

— Ολοκληρωμένη επίγνωση και ανάλυση καταστάσεων (ISAA) — Τυποποιημένες επιχειρησιακές διαδικασίες, DS 1570/15, 22 Οκτωβρίου 2015

— Διατάξεις της Επιτροπής για το γενικό σύστημα έγκαιρης προειδοποίησης «ARGUS», COM(2005) 662 final, 23 Δεκεμβρίου 2005

— Απόφαση 2006/25/ΕΚ, Ευρατόμ της Επιτροπής, της 23ης Δεκεμβρίου 2005, που τροποποιεί τον εσωτερικό της κανονισμό (ΕΕ L 19 της 24.1.2006, σ. 20)

— ARGUS Modus Operandi, Ευρωπαϊκή Επιτροπή, 23 Οκτωβρίου 2013

— Συμπεράσματα του Συμβουλίου σχετικά με ένα πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο («εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο»), έγγρ. 9916/17

— Επιχειρησιακό πρωτόκολλο της ΕΕ για την αντιμετώπιση υβριδικών απειλών «Σενάριο της ΕΕ», έγγραφο SWD(2016) 227

— Μηχανισμός αντιμετώπισης κρίσεων της ΕΥΕΔ, 8 Νοεμβρίου 2016 [Ares(2017)880661.Κοινό υπηρεσιακό έγγραφο εργασίας Επιχειρησιακό πρωτόκολλο της ΕΕ για την αντιμετώπιση υβριδικών απειλών «Σενάριο της ΕΕ», έγγραφο SWD(2016) 227 final, 5 Ιουλίου 2016

— Κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Κοινό πλαίσιο για την αντιμετώπιση υβριδικών απειλών. Απόκριση της Ευρωπαϊκής Ένωσης JOIN/2016/018 final, 6 Απριλίου 2016

— ΕΥΕΔ (2016) 1674 — Έγγραφο εργασίας της Ευρωπαϊκής Υπηρεσίας Εξωτερικής Δράσης — Μονάδα Ανάλυσης Υβριδικών Απειλών της ΕΕ — Εντολή

6. ΕΙΔΙΚΑ ΣΤΟΙΧΕΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΣΤΗ ΔΙΑΔΙΚΑΣΙΑ IPCR