Ισχυρότεροι μαζί: Ο ENISA δημοσιεύει τη ‘μετά τη δράση’ έκθεση για τη Cyber Europe 2014:

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) δημοσιεύει σήμερα τη δημόσια έκδοση της ‘μετά τη δράση’ έκθεσης για την πανευρωπαϊκή άσκηση στον κυβερνοχώρο CyberEurope 2014 (CE2014). Αυτή η έκθεση, η οποία έχει εγκριθεί από τα κράτη μέλη, δίνει μια υψηλού επιπέδου επισκόπηση της περίπλοκης άσκησης ασφάλειας στον κυβερνοχώρο που διενεργήθηκε το 2014.

Κύριος στόχος της CyberEurope 2014 ήταν να εκπαιδεύσει τα κράτη μέλη ώστε να συνεργάζονται στη διάρκεια μιας κρίσης στον κυβερνοχώρο. Η τριών φάσεων άσκηση έδωσε ευκαιρίες να αξιολογηθεί η αποτελεσματικότητα των διαδικασιών συνεργασίας και κλιμάκωσης στη διάρκεια διασυνοριακών περιστατικών στον κυβερνοχώρο, που επηρεάζουν την ασφάλεια ζωτικών υπηρεσιών και υποδομών, ενώ συγχρόνως να δοκιμαστούν οι εθνικές ικανότητες και τα έκτακτα σχέδια στα οποία συμμετέχουν οργανώσεις τόσο από το δημόσιο όσο και από τον ιδιωτικό τομέα.

Η άσκηση, την οποία οργανώνει ο ENISA κάθε δύο χρόνια, σχεδιάστηκε από κοινού με εκπροσώπους από τις συμμετέχουσες χώρες και απαίτησε έξι (6) συνέδρια σχεδιασμού σε ολόκληρη την Ευρώπη. Αυτή η άσκηση, η οποία συγκέντρωσε περισσότερους από **1.500 συμμετέχοντες** από **29 κράτη μέλη της ΕΕ και της ΕΖΕΣ,** κάλυψε **για πρώτη φορά και τις τρεις (3) φάσεις** της αντιμετώπισης περιστατικών στον κυβερνοχώρο – **τεχνική, επιχειρησιακή** και **στρατηγική** –, οι οποίες κλιμακώνονται μία-μία μέχρι να εξελιχθούν στην επόμενη φάση, και περιελάμβανε:

- Φάση 1 – Τεχνικό επίπεδο (28-30 Απριλίου 2014, **49 ώρες**): Ανίχνευση, ανάλυση και μετριασμό περιστατικών, ανταλλαγές πληροφοριών.
- Φάση 2 – Επιχειρησιακό επίπεδο (30 Οκτωβρίου 2014, **10 ώρες**): Προειδοποίηση, συνεργασία, βραχυπρόθεσμο μετριασμό κρίσης, ανάπτυξη μιας κοινής εικόνας της κατάστασης.
- Φάση 3 – Στρατηγικό επίπεδο – **δοκιμάστηκε για πρώτη φορά** – (25 Φεβρουαρίου 2015): Λήψη αποφάσεων βάσει της κοινής εικόνας της κατάστασης, συζητήσεις πολιτικής σε υψηλό επίπεδο για το μακροπρόθεσμο στρατηγικό μετριασμό της κρίσης.

Η έκθεση δείχνει ότι στην Ευρώπη η κοινή ικανότητα μετριασμού των μεγάλης κλίμακας περιστατικών ασφάλειας στον κυβερνοχώρο έχει εξελιχθεί σημαντικά από το 2010, οπότε και διενεργήθηκε για πρώτη φορά η άσκηση CyberEurope. Η ανταλλαγή πληροφοριών σε πραγματικό χρόνο μεταξύ των χωρών αποδεικνύεται πολύτιμη για την ταχεία λήψη αποφάσεων. Οι **Τυποποιημένες διαδικασίες λειτουργίας της ΕΕ** (ΕΕ-ΤΔΛ) που ακολουθούνται για να υποστηρίξουν αυτές τις δραστηριότητες συνεργασίας, παρέχουν στα κράτη μέλη κατευθυντήριες γραμμές, τις οποίες μπορούν να χρησιμοποιήσουν σε περίπτωση μεγάλης κλίμακας περιστατικών ασφάλειας στον κυβερνοχώρο. Αυτές θα βελτιωθούν περαιτέρω για να λάβουν υπόψη τους το εξελισσόμενο πλαίσιο πολιτικής στην Ευρώπη για την ασφάλεια στον κυβερνοχώρο.

Η συνεργασία επισημάνθηκε ως βασικό στοιχείο που συμβάλλει στην αυξημένη κατανόηση, την οικοδόμηση εμπιστοσύνης και την ταχύτερη αντίδραση. Η **Πλατφόρμα για την άσκηση στον κυβερνοχώρο (ΠΑΚ)** που ανέπτυξε ο ENISA για το σχεδιασμό, τη διεξαγωγή και την αξιολόγηση της άσκησης αποδείχθηκε ισχυρό εργαλείο. Ο ENISA αναπτύσσει επί του παρόντος περαιτέρω την ΠΑΚ, προκειμένου να φιλοξενήσει μελλοντικές ασκήσεις στον κυβερνοχώρο και τεχνικά σενάρια. Το ενενήντα

οκτώ τοις εκατό (**98%**) των συμμετεχόντων στην τεχνική φάση εξέφρασε ενδιαφέρον να συμμετάσχει στην επόμενη άσκηση.

Ο εκτελεστικός διευθυντής του ENISA Udo Helmbrecht δήλωσε: ***«Τα διδάγματα της CyberEurope 2014 είναι πολλά και παρέχουν τη βάση για πρωτοποριακό έργο στον τομέα της συνεργασίας σε θέματα κρίσης στον κυβερνοχώρο, ένα αναδυόμενο πεδίο όπου η ΕΕ και ο ENISA κατέχουν ηγετική θέση. Έχουμε δεσμευτεί να εφαρμόσουμε το σχέδιο δράσης, με την υποστήριξη των κρατών μελών, για να βελτιώσουμε περαιτέρω την ετοιμότητα σε σχέση με την κρίση στον κυβερνοχώρο, τόσο σε εθνικό επίπεδο όσο και σε επίπεδο ΕΕ».***

Το σενάριο

Το σενάριο της CyberEurope 2014 είχε ως κεντρικό άξονα μια κανονιστική πρόταση της ΕΕ σχετικά με τους **ενεργειακούς πόρους**. Κατά την τεχνική φάση της άσκησης, τα κράτη μέλη και τα θεσμικά όργανα της ΕΕ είχαν να αντιμετωπίσουν **περιστατικά στον κυβερνοχώρο** όπως **διαρροή πληροφοριών,** πληροφορίες ανοικτής πηγής, ανάλυση **κακόβουλου λογισμικού** κινητών τηλεφώνων, επιθέσεις **άρνησης υπηρεσίας** και **προηγμένες επίμονες απειλές**. Ακολούθησε η επιχειρησιακή φάση της CyberEurope 2014, με την κλιμάκωση της κατάστασης που οδήγησε σε μια σειρά **επιθέσεων μεγάλης κλίμακας στον κυβερνοχώρο** κατά διαφόρων υποδομών ζωτικής σημασίας και αναρίθμητων online υπηρεσιών. Τέλος, η στρατηγική φάση της CyberEurope 2014 κλιμάκωσε περαιτέρω την κρίση, με αποτέλεσμα να πληγούν σοβαρά εν μέσω ενός δριμύτατου χειμώνα αρκετές ενεργειακές υποδομές, να παραβιαστούν βασικές τεχνολογίες και να αυξηθεί η ανησυχία της κοινής γνώμης.

Για την πλήρη έκθεση

Για μια γρήγορη ματιά στα ενδότερα της CyberEurope, δείτε το ακόλουθο βίντεο του ENISA:

https://www.enisa.europa.eu/media/news-items/preparing-for-the-unknown-a-peek-into-cyber-europe

Για συνεντεύξεις και ερωτήματα από τον Τύπο:

Επικοινωνήστε με τη **Συνεργασία για την κρίση στον κυβερνοχώρο**: c3@enisa.europa.eu