ΕΥΡΩΠΑΪΚΟ
ΕΛΕΓΚΤΙΚΟ
ΣΥΝΕΔΡΙΟ

EL

Δελτίο Τύπου

Λουξεμβούργο, 29 Μαρτίου 2022

Τα όργανα της ΕΕ πρέπει να ενισχύσουν την ετοιμότητά τους στον τομέα της κυβερνοασφάλειας

Ο αριθμός των κυβερνοεπιθέσεων στα όργανα της ΕΕ σημειώνει ραγδαία αύξηση. Ο βαθμός ετοιμότητας των οργάνων αυτών στον τομέα της κυβερνοασφάλειας ποικίλλει και συνολικά δεν είναι ανάλογος των εντεινόμενων απειλών. Δεδομένης της ισχυρής αλληλοσύνδεσής τους, υπάρχει το ενδεχόμενο οι αδυναμίες του ενός να εκθέσουν τα άλλα σε απειλές κατά της ασφάλειάς τους. Αυτό είναι το συμπέρασμα ειδικής έκθεσης του Ευρωπαϊκού Ελεγκτικού Συνεδρίου, η οποία εξετάζει τον βαθμό ετοιμότητας των φορέων διακυβέρνησης της ΕΕ κατά των κυβερνοαπειλών. Οι ελεγκτές συνιστούν τη θέσπιση δεσμευτικών κανόνων για την κυβερνοασφάλεια και την αύξηση των πόρων που διατίθενται στην ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT-ΕΕ). Επίσης, σύμφωνα με τους ελεγκτές, η Ευρωπαϊκή Επιτροπή πρέπει να προωθήσει την περαιτέρω συνεργασία μεταξύ των ενωσιακών οργάνων, ενώ η CERT-ΕΕ και ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια πρέπει να αυξήσουν την εστίασή τους σε αυτά που διαθέτουν μικρότερη πείρα στη διαχείριση της κυβερνοασφάλειας.

Τα σημαντικά περιστατικά κυβερνοασφάλειας στα διάφορα όργανα της ΕΕ υπερδεκαπλασιάστηκαν μεταξύ 2018 και 2021· η τηλεργασία αύξησε σημαντικά τον αριθμό των δυνητικών σημείων πρόσβασης για τους επιτιθέμενους. Τα σημαντικά περιστατικά προκαλούνται κατά κανόνα από πολύπλοκες κυβερνοεπιθέσεις, που συνήθως προϋποθέτουν τη χρήση νέων μεθόδων και τεχνολογιών και μπορεί να χρειαστούν εβδομάδες, αν όχι μήνες, για τη διερεύνησή τους και την ανάκαμψη από αυτά. Ενδεικτικό παράδειγμα ήταν η κυβερνοεπίθεση στον Ευρωπαϊκό Οργανισμό Φαρμάκων, όταν διέρρευσαν ευαίσθητα δεδομένα, τα οποία παραποιήθηκαν έτσι ώστε να υπονομευθεί η εμπιστοσύνη των πολιτών στα εμβόλια.

«*Τα θεσμικά και λοιπά όργανα και οι οργανισμοί της ΕΕ αποτελούν ελκυστικούς στόχους για δυνητικούς επιτιθέμενους, ιδίως για ομάδες που είναι ικανές να εκτελούν εξαιρετικά εξελιγμένες αόρατες επιθέσεις στο πλαίσιο κυβερνοκατασκοπείας ή για άλλους κακόβουλους σκοπούς*», δήλωσε η Bettina Jakobsen, Μέλος του ΕΕΣ και επικεφαλής του ελέγχου. «*Επιθέσεις αυτού του είδους μπορεί να έχουν σημαντικές πολιτικές προεκτάσεις, να βλάψουν τη συνολική φήμη της ΕΕ και να υπονομεύσουν την εμπιστοσύνη στους θεσμούς της. Η ΕΕ πρέπει να εντείνει τις προσπάθειές της για την προστασία των οργανισμών της.*»

Σκοπός του παρόντος δελτίου Τύπου είναι η παρουσίαση των κύριων μηνυμάτων της ειδικής έκθεσης του Ευρωπαϊκού Ελεγκτικού Συνεδρίου. Το πλήρες κείμενο της ειδικής έκθεσης διατίθεται στον ιστότοπο eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg

E: press@eca.europa.eu @EUAuditors eca.europa.eu

Κύρια διαπίστωση των ελεγκτών ήταν ότι δεν είναι πάντοτε επαρκής η προστασία των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ από κυβερνοαπειλές. Η κυβερνοασφάλεια δεν προσεγγίζεται με συνέπεια, δεν εφαρμόζονται πάντοτε συναφείς βασικές δικλίδες και ορθές πρακτικές, ενώ δεν παρέχεται συστηματικά σχετική επιμόρφωση. Οι πόροι που διατίθενται για την κυβερνοασφάλεια ποικίλλουν σε μεγάλο βαθμό, καθώς διαπιστώθηκε ότι ορισμένα όργανα δαπανούν πολύ λιγότερο σε σχέση με άλλα παρόμοιου μεγέθους. Μολονότι οι διαφορές στα επίπεδα κυβερνοασφάλειας θα μπορούσαν θεωρητικά να δικαιολογηθούν από τα διαφορετικά προφίλ κινδύνου κάθε οργανισμού και τα ποικίλα επίπεδα ευαισθησίας των δεδομένων που αυτοί χειρίζονται, οι ελεγκτές τονίζουν ότι οι αδυναμίες στον τομέα της κυβερνοασφάλειας ενός ενωσιακού οργάνου μπορούν να εκθέσουν σε κυβερνοαπειλές σειρά άλλων (τα όργανα της ΕΕ όχι μόνο αλληλοσυνδέονται, αλλά συχνά υπάρχει σύνδεση και με δημόσιους και ιδιωτικούς οργανισμούς στα κράτη μέλη).

Η ομάδα αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CCERT-ΕΕ) και ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA) αποτελούν τις δύο βασικές οντότητες που είναι επιφορτισμένες με την παροχή υποστήριξης σε θέματα κυβερνοασφάλειας. Ωστόσο, δεν κατάφεραν να παράσχουν στα όργανα της ΕΕ όλη τη στήριξη που αυτά χρειάζονται, λόγω των περιορισμένων πόρων ή του γεγονότος ότι προτεραιοποιήθηκαν άλλοι τομείς. Σύμφωνα με τους ελεγκτές, αδυναμίες παρουσιάζει επίσης η ανταλλαγή πληροφοριών: παραδείγματος χάριν, δεν προβαίνουν όλα τα όργανα της ΕΕ στην έγκαιρη κοινοποίηση πληροφοριών σχετικά με τα τρωτά σημεία και τα σημαντικά περιστατικά κυβερνοασφάλειας που έχουν πλήξει τα ίδια και ενδέχεται να πλήξουν και άλλα.

Γενικές πληροφορίες

Μέχρι στιγμής, δεν έχει θεσπιστεί νομικό πλαίσιο για την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και στους οργανισμούς της ΕΕ, καθώς αυτά δεν υπόκεινται στην ευρύτερη νομοθεσία της ΕΕ για την κυβερνοασφάλεια, την οδηγία NIS του 2016, ούτε στην προτεινόμενη αναθεώρησή της, την οδηγία NIS2. Επίσης, δεν υπάρχουν ολοκληρωμένες πληροφορίες σχετικά με τα ποσά που αυτά δαπανούν για την κυβερνοασφάλεια. Οι κοινοί κανόνες για την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια για όλα τα όργανα της ΕΕ περιλαμβάνονται στην ανακοίνωση σχετικά με τη στρατηγική της ΕΕ για την Ένωση Ασφάλειας για την περίοδο 2020-2025, την οποία η Επιτροπή δημοσίευσε τον Ιούλιο του 2020. Στη στρατηγική κυβερνοασφάλειας της ΕΕ για την ψηφιακή δεκαετία, η οποία δημοσιεύθηκε τον Δεκέμβριο του 2020, η Επιτροπή ανέλαβε να προτείνει κανονισμό σχετικά με κοινούς κανόνες κυβερνοασφάλειας για όλα τα όργανα και τους οργανισμούς της ΕΕ. Πρότεινε επίσης τη θέσπιση νέας νομικής βάσης για τη CERT-ΕΕ, με σκοπό την ενίσχυση της εντολής και της χρηματοδότησής της.

Η ειδική έκθεση 05/2022, με τίτλο «*Η κυβερνοασφάλεια στα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ - Ο βαθμός ετοιμότητας συνολικά δεν είναι ανάλογος των απειλών*», είναι διαθέσιμη στον ιστότοπο του ΕΕΣ. Το ΕΕΣ είχε επίσης επισημάνει τις προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια σε επισκόπηση του 2019.

Επικοινωνία με τον Τύπο

Γραφείο Τύπου του ΕΕΣ: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu - κιν.: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu - κιν.: (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu - κιν.: (+352) 621 552 224