23 Νοεμβρίου 2026

Ο Γ.Γ Προστασίας Κρίσιμων Οντοτήτων Σ. Παπαγεωργίου, τόνισε την ανάγκη συνεχούς επιτήρησης και ενίσχυσης της ανθεκτικότητας των κρίσιμων υποδομών

/ Γενικά Θέματα



Οι κυβερνοεπιθέσεις είναι πλέον από τις σημαντικότερες απειλές για την ασφάλεια των κρατών, καθώς μπορούν να πλήξουν κρίσιμες υποδομές και υπηρεσίες από τις οποίες εξαρτάται η καθημερινότητα των πολιτών.

Η αξιοποίηση της τεχνητής νοημοσύνης διευκολύνει πλέον τον εντοπισμό ευπαθειών και επιταχύνει τη δράση των επιτιθέμενων, εντείνοντας τις ανησυχίες για την προστασία συστημάτων όπως η ηλεκτροδότηση, οι μεταφορές, η υγεία και η τροφοδοσία με τρόφιμα.

«Ό,τι είναι ευάλωτο αυτή τη στιγμή θα χτυπηθεί γρήγορα», προειδοποίησε ο Γενικός Γραμματέας Προστασίας Κρίσιμων Οντοτήτων, Σπύρος Παπαγεωργίου, μιλώντας στο EPTnews για την αυξανόμενη απειλή των κυβερνοεπιθέσεων και τις προκλήσεις που δημιουργεί η χρήση της τεχνητής νοημοσύνης.

Όπως εξήγησε, η τεχνητή νοημοσύνη έχει αλλάξει σημαντικά τα δεδομένα στον τομέα της κυβερνοασφάλειας, καθώς επιτρέπει στους επιτιθέμενους να εντοπίζουν ευκολότερα αδυναμίες στα συστήματα και να αυτοματοποιούν τις επιθέσεις τους.

Παράλληλα, υπογράμμισε ότι δεν υπάρχει απόλυτη ασφάλεια, ενώ τόνισε την ανάγκη συνεχούς επιτήρησης και ενίσχυσης της ανθεκτικότητας των κρίσιμων υποδομών.

Ο κ. Παπαγεωργίου διαχώρισε τους επιτιθέμενους σε δύο βασικές κατηγορίες, τους κυβερνοεγκληματίες, που επιδιώκουν οικονομικό όφελος, και τους κρατικούς δρώντες, τους οποίους χαρακτήρισε ως την πιο επικίνδυνη απειλή.

Όπως ανέφερε, οι δεύτεροι χρησιμοποιούν αντίστοιχες τακτικές και εργαλεία, αλλά επιδιώκουν διαφορετικούς στόχους: να αποκτήσουν πρόσβαση σε συστήματα, να διατηρήσουν τον έλεγχό τους, να υποκλέψουν πληροφορίες ή ακόμη και να τα θέσουν εκτός λειτουργίας όταν το απαιτήσουν οι συνθήκες, ιδίως σε περιόδους κρίσης ή πολέμου.

«Δεν εντοπίζονται εύκολα», σημείωσε, εξηγώντας ότι για την αντιμετώπισή τους απαιτείται το λεγόμενο «κυνήγι της κυβερνοαπειλής». Πρόκειται για τη συστηματική αναζήτηση επιτιθέμενων που ενδέχεται να έχουν ήδη παραβιάσει ένα σύστημα και να παραμένουν στο εσωτερικό του χωρίς να γίνονται αντιληπτοί.

Ερωτηθείς εάν οι κυβερνοεπιθέσεις συνδέονται με τις πολεμικές συγκρούσεις, επισήμανε ότι «συνήθως η κυβερνοεπίθεση προηγείται του πολέμου». Όπως εξήγησε, οι επιτιθέμενοι στοχεύουν κρίσιμες οντότητες και υπηρεσίες που στηρίζουν την πολεμική προσπάθεια, ενώ ακόμη και τα οπλικά συστήματα, λόγω της εξάρτησής τους από το λογισμικό και την τεχνολογία, είναι ευάλωτα σε τέτοιου είδους επιθέσεις.

Περιγράφοντας τη μεθοδολογία των επιτιθέμενων, ο Γενικός Γραμματέας εξήγησε ότι μια κυβερνοεπίθεση δεν πραγματοποιείται συνήθως αιφνιδιαστικά, αλλά προηγείται συστηματική προετοιμασία.

Ο επιτιθέμενος εντοπίζει τα εκτεθειμένα συστήματα, καταγράφει τα λογισμικά που χρησιμοποιούνται, αναζητά ευπάθειες με τη βοήθεια της τεχνητής νοημοσύνης και σχεδιάζει τον τρόπο με τον οποίο θα αποκτήσει αρχικά πρόσβαση και στη συνέχεια βαθύτερο έλεγχο.

«Αν θέλουμε να το αντιμετωπίσουμε, πρέπει να σκεφτόμαστε όπως οι επιτιθέμενοι», ανέφερε ο κ. Παπαγεωργίου. Αυτό, όπως διευκρίνισε, σημαίνει ότι οι αρμόδιοι πρέπει να εντοπίζουν εγκαίρως τα ευάλωτα συστήματα, να προχωρούν σε αναβαθμίσεις ή αντικαταστάσεις, να περιορίζουν την έκθεσή τους και να διασφαλίζουν τη συνεχή επιτήρησή τους.

Αναφερόμενος στις ανησυχίες για πιθανή στοχοποίηση συστημάτων ψύξης σε

σούπερ μάρκετ, ο Γενικός Γραμματέας επιβεβαίωσε ότι «η ανησυχία υπάρχει».

Επισήμανε, μάλιστα, ότι δεν μπορεί να υπάρξει απόλυτη ασφάλεια, καθώς «αν υπήρχε, δεν θα μιλάγαμε τώρα».

Σχετικά με τον τρόπο προστασίας τέτοιων συστημάτων, εξήγησε ότι το πρώτο βήμα είναι να εντοπιστεί πώς πραγματοποιήθηκε η επίθεση. Στην περίπτωση των ψυγείων, η βασική αδυναμία ήταν η απομακρυσμένη πρόσβαση, μέσω της οποίας ο επιτιθέμενος μπορούσε να ελέγχει το σύστημα.

Ο ίδιος υπογράμμισε την ανάγκη περιορισμού της έκθεσης των εφαρμογών και καθορισμού συγκεκριμένων δικαιωμάτων πρόσβασης. Έφερε, επίσης, ως παράδειγμα τη χρήση ενός «code of the day», δηλαδή ενός νέου κωδικού πρόσβασης που δημιουργείται με βάση την ημερομηνία, εφόσον ο συντηρητής δεν θυμάται τον υπάρχοντα. Όπως σημείωσε, ακόμη και σε αυτές τις περιπτώσεις πρέπει να προβλέπονται αυστηρά καθορισμένα δικαιώματα.

Καθοριστικό ρόλο, σύμφωνα με τον κ. Παπαγεωργίου, έχει η επιτήρηση της λειτουργίας των συστημάτων, ώστε να εντοπίζεται εγκαίρως οποιαδήποτε ύποπτη δραστηριότητα.

«Η κυβερνοασφάλεια δεν είναι απλώς συγκεκριμένα μέτρα», τόνισε, προσθέτοντας ότι προϋποθέτει ένα σύνολο παρεμβάσεων, με τη συνεχή επιτήρηση να αποτελεί βασικό στοιχείο τους.

Ο Γενικός Γραμματέας περιέγραψε δύο βασικούς άξονες για την αντιμετώπιση των κυβερνοεπιθέσεων, την πρόληψη και την ανθεκτικότητα.

Η πρόληψη αφορά τα μέτρα που λαμβάνονται ώστε να αποτραπεί μια επίθεση. Η ανθεκτικότητα, από την άλλη, βασίζεται στην παραδοχή ότι μια επίθεση μπορεί τελικά να πετύχει τον στόχο της. Σε αυτή την περίπτωση, απαιτείται οργανωμένο σχέδιο διαχείρισης, ώστε οι υπηρεσίες να συνεχίσουν να λειτουργούν παράλληλα με τις προσπάθειες αντιμετώπισης και αποκατάστασης της ζημιάς.

«Αν αντέξει ο οργανισμός, αντέχει και η χώρα», ανέφερε χαρακτηριστικά. Σχετικά με το εάν η Ελλάδα διαθέτει το απαραίτητο ανθρώπινο δυναμικό και την τεχνογνωσία, απάντησε καταφατικά, υποστηρίζοντας ότι η χώρα είναι «καλά οργανωμένη» στον τομέα της ανθεκτικότητας.

Εξηγώντας τον ρόλο της Γενικής Γραμματείας Προστασίας Κρίσιμων Οντοτήτων, ο κ. Παπαγεωργίου ανέφερε ότι αρχικά προσδιορίστηκαν οι βασικές υπηρεσίες από τις οποίες εξαρτάται η καθημερινότητα των πολιτών, όπως η ηλεκτροδότηση, η

υδροδότηση, οι μεταφορές, το σύστημα υγείας και η τροφοδοσία με τρόφιμα.

Στη συνέχεια, προσδιορίστηκαν οι οργανισμοί που παρέχουν αυτές τις υπηρεσίες και επηρεάζουν μεγάλο μέρος του πληθυσμού. Οι τομείς που έχουν οριστεί είναι συνολικά 12.

Ειδική αναφορά έκανε στη νησιωτικότητα της Ελλάδας, επισημαίνοντας ότι ακόμη και ένα σούπερ μάρκετ σε ένα νησί μπορεί να χαρακτηριστεί κρίσιμη οντότητα, καθώς ενδέχεται να καλύπτει τις ανάγκες ολόκληρου του τοπικού πληθυσμού.

Η Γενική Γραμματεία καθορίζει τις κρίσιμες οντότητες και τις κατευθύνει ως προς τα μέτρα προστασίας από το σύνολο των κινδύνων, σύμφωνα με την προσέγγιση «all hazards approach», η οποία δεν περιορίζεται στις κυβερνοεπιθέσεις. Σε αυτές, ωστόσο, δίνεται προτεραιότητα, καθώς αποτελούν έναν ιδιαίτερα εύκολο κίνδυνο για τους επιτιθέμενους.

Όπως υπογράμμισε ο κ. Παπαγεωργίου, αποστολή της Γενικής Γραμματείας είναι «η προστασία της καθημερινότητας του πολίτη» απέναντι σε φυσικούς και τεχνολογικούς κινδύνους. Διευκρίνισε, τέλος, ότι το έργο της δεν περιορίζεται στην εποπτεία, αλλά περιλαμβάνει καθημερινή επικοινωνία και συνεργασία με τα υπουργεία και τις ίδιες τις κρίσιμες οντότητες, με στόχο την ενίσχυση της ανθεκτικότητας σε εθνικό επίπεδο.

«Είμαστε κομμάτια του ίδιου πάζλ. Τον συντονισμό τον κάνει η Γενική Γραμματεία», κατέληξε.

briefingnews.gr