ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας

17 Φεβρουαρίου 2026

ΔΕΛΤΙΟ ΤΥΠΟΥ

Το Γραφείο Επιτρόπου Επικοινωνιών - Αρχή Ψηφιακής Ασφάλειας στο πλαίσιο των αρμοδιοτήτων του έχει διεξάγει δύο παγκύπριες έρευνες με σκοπό τη συλλογή στοιχείων και πληροφοριών σχετικά με την κυβερνοασφάλεια στην Κυπριακή Δημοκρατία.

Οι έρευνες επικεντρώθηκαν, μεταξύ άλλων, στη διαχείριση θεμάτων κυβερνοασφάλειας ή/και ψηφιακής ασφάλειας, στη σημασία που αποδίδεται στα ζητήματα αυτά, στον τρόπο αντιμετώπισης περιστατικών κυβερνοεπιθέσεων, καθώς και στις επιπτώσεις που προκύπτουν από τέτοια περιστατικά.

Η πρώτη έρευνα απευθυνόταν σε επιχειρήσεις, διεξήχθη κατά την περίοδο Σεπτεμβρίου-Νοεμβρίου 2025, σε δείγμα 459 επιχειρήσεων από ένα ευρύ φάσμα στους τομείς της βιομηχανίας, του εμπορίου και των υπηρεσιών. Η δεύτερη έρευνα απευθυνόταν σε πολίτες και διεξήχθη τους μήνες Αύγουστο-Σεπτέμβριο 2025 σε δείγμα 1043 πολιτών.

Επιχειρήσεις

Τα κυριότερα αποτελέσματα της έρευνας που αφορά τις επιχειρήσεις, τα οποία παρουσιάστηκαν στη συνάντηση εμπλεκόμενων φορέων και αρχών που διεξήχθη στις 17 Δεκεμβρίου 2025, ήταν τα ακόλουθα:

1. Σχεδόν οι μισές επιχειρήσεις (53% το 2025, 47% το 2024 και 49% το 2023) δέχθηκαν κάποια επίθεση/παραβίαση κατά τους τελευταίους 12 μήνες με μέσο όρο 1 επίθεση κάθε 8 ημέρες καταγράφοντας μικρή αύξηση σε σχέση με το 2024 (1 επίθεση κάθε 10 ημέρες).
2. Από τις επιχειρήσεις που δέχθηκαν επίθεση/παραβίαση, για περισσότερες από τις μισές (51% το 2025) προέκυψε οικονομικό κόστος, το οποίο ανήλθε κατά μέσο όρο στις 12 χιλιάδες ευρώ. Παράλληλα, παρατηρείται ελαφρά μείωση στο ποσοστό των επιχειρήσεων που υπέστησαν οικονομική ζημιά σε σχέση με την προηγούμενη χρονιά (55% το 2024).
3. Η συχνότερη μορφή επίθεσης παραμένει το phishing, δηλαδή απατηλά μηνύματα μέσω ηλεκτρονικού ταχυδρομείου, με 44%, καταγράφοντας μείωση κατά 4 ποσοστιαίες μονάδες σε σχέση με το 2024 και κατά 1 μονάδα σε σχέση με το 2023. Το phishing αποτελεί επίσης την πιο πρόσφατη επίθεση που δέχτηκαν οι επιχειρήσεις φτάνοντας το 75%.
4. Σχεδόν μία στις τέσσερις επιχειρήσεις δεν έχει προβεί σε δημιουργία, επικαιροποίηση ή αναθεώρηση των πολιτικών κυβερνοασφάλειας για διάστημα άνω του ενός έτους, ώστε αυτές να συμβαδίζουν με τις τεχνολογικές εξελίξεις.
5. Καταγράφεται έλλειψη ενημέρωσης των επιχειρήσεων σχετικά με την ύπαρξη σεμιναρίων κυβερνοασφάλειας, καθώς το 43% δηλώνει άγνοια (50% το 2024 και 46% το 2023), ενώ μόλις το 22% συμμετείχε σε τέτοιες δράσεις (13% το 2024 και 17% το 2023). Αξίζει να σημειωθεί ότι οι επιχειρήσεις που συμμετείχαν σε σεμινάρια προχώρησαν σε ενέργειες ενίσχυσης των μέτρων ασφαλείας τους.
6. Από τις επιχειρήσεις που δεν δέχθηκαν κυβερνοεπίθεση, το 48% θεωρεί ότι αυτό οφείλεται στο γεγονός ότι η εταιρεία τους δεν αποτελεί «στόχο». Το ποσοστό αυτό παρουσιάζει αύξηση σε σχέση με τις δύο προηγούμενες έρευνες (37% το 2024 και 38% το 2023), γεγονός που προκαλεί ανησυχία, καθώς κάθε επιχείρηση μπορεί να αποτελέσει στόχο και θα πρέπει να λαμβάνει τα κατάλληλα μέτρα προστασίας.

Πολίτες

Τα κυριότερα αποτελέσματα της έρευνας που αφορά τους πολίτες, τα οποία παρουσιάστηκαν στην ίδια συνάντηση στις 17 Δεκεμβρίου 2025, είναι τα εξής:

1. Το ποσοστό των πολιτών που δέχθηκαν κυβερνοεπίθεση τους τελευταίους 12 μήνες ανήλθε στο 33%, παρουσιάζοντας μείωση σε σχέση με τα προηγούμενα δύο έτη (49% το 2024 και 47% το 2023). Ο μέσος αριθμός επιθέσεων ανά έτος ανήλθε σε 25,9, σημειώνοντας μικρή μείωση σε σχέση με το 2024 (28,5).
2. Από τους πολίτες που δέχθηκαν επίθεση για το 17% (13% για το 2024 και 19% για το 2023) υπήρξε κάποιο κόστος που ανέρχεται στα €141 κατά μέσο όρο. Ενδιαφέρον παρουσιάζει επίσης το γεγονός ότι το μεγαλύτερο κόστος παρουσιάζεται στην ηλικιακή ομάδα 35-44, σε αντίθεση με το 2024, όπου το μεγαλύτερο κόστος παρουσιαζόταν στην ηλικιακή ομάδα 18-34, ενώ το χαμηλότερο στην ηλικιακή ομάδα 45-54 (τόσο το 2025 όσο και το 2024).
3. Η συχνότερη μορφή επίθεσης στους πολίτες είναι επίσης το phishing, με ποσοστό 22%, καταγράφοντας βελτίωση κατά 17 ποσοστιαίες μονάδες σε σχέση με το 2024 και κατά 14 μονάδες σε σχέση με το 2023.
4. Από τους πολίτες που δεν δέχθηκαν επίθεση ή παραβίαση τον τελευταίο χρόνο, το 89% δεν αποκλείει το ενδεχόμενο να πέσει θύμα κακόβουλης ενέργειας στο μέλλον, ποσοστό αυξημένο κατά 2% σε σχέση με το 2024.
5. Διαπιστώνεται σημαντική άγνοια σχετικά με την ύπαρξη εκπαιδευτικών σεμιναρίων κυβερνοασφάλειας, καθώς το 74% των πολιτών δήλωσε ότι δεν γνωρίζει την ύπαρξή τους (αύξηση κατά 4% σε σχέση με το 2024), ενώ μόλις το 15% έχει συμμετάσχει σε τέτοιες δράσεις. Μετά την παρακολούθηση σεμιναρίων, οι σημαντικότερες αλλαγές που υιοθετήθηκαν ήταν η χρήση ισχυρών κωδικών, η συχνή αλλαγή τους και η αποφυγή ύποπτων ιστοσελίδων.

Βάσει των πιο πάνω αποτελεσμάτων, η Αρχή Ψηφιακής Ασφάλειας προτίθεται να διοργανώσει εκπαιδευτικά σεμινάρια, καθώς και εκστρατείες ενημέρωσης και ευαισθητοποίησης, με στόχο την ενίσχυση των γνώσεων και δεξιοτήτων σε θέματα κυβερνοασφάλειας τόσο των πολιτών όσο και των επιχειρήσεων. Συγκεκριμένα, και πάντα μεταξύ άλλων, για τις επιχειρήσεις προγραμματίζονται συνέδρια σε συνεργασία με τον ENISA, ενημερώσεις για νέες Ευρωπαϊκές χρηματοδοτήσεις σε συνεργασία με το ECCC, κοινές εκδηλώσεις με τις επιχειρηματικές οργανώσεις ΚΕΒΕ και ΟΕΒ, επιχειρηματικές αποστολές, νέες εξαγγελίες σχεδίων χορηγιών για στήριξη του τομέα, συμμετοχή σε εκθέσεις του εξωτερικού κ.α. Για τους πολίτες ευρύτερα θα πραγματοποιηθεί για τρίτη συνεχόμενη χρονιά το “Cybersecurity For All” Festival, το 2ο Cybersecurity Career Fair, εξειδικευμένες ενημερώσεις σε άτομα ηλικίας 65+ καθώς και πολυάριθμες εκπαιδεύσεις σε νηπιαγωγεία, δημοτικά, γυμνάσια και λύκεια. Οι έρευνες αυτές αποτελούν την τέταρτη στη σειρά χαρτογράφηση της κατάστασης της κυβερνοασφάλειας στην Κυπριακή Δημοκρατία και θα συνεχιστούν σε ετήσια βάση, εμπλουτιζόμενες ανάλογα με τις εξελίξεις και τις ανάγκες πληροφόρησης.

Τα αναλυτικά αποτελέσματα των ερευνών είναι διαθέσιμα σε μορφή pdf στον πιο κάτω σύνδεσμο:

https://dsa.cy/category/press-releases/survey-2025