1. ΕΝΑΣ ΘΑΥΜΑΣΤΟΣ ΚΑΙΝΟΥΡΓΙΟΣ (;) ΚΟΣΜΟΣ

Μέσο: . . . . . .ΤΑ ΝΕΑ

Ημ. Έκδοσης: . . .27/09/2025 Ημ. Αποδελτίωσης: . . .27/09/2025

Σελίδα: 1

1. ΕΝΑΣ ΘΑΥΜΑΣΤΟΣ ΚΑΙΝΟΥΡΓΙΟΣ (;) ΚΟΣΜΟΣ

Μέσο: . . . . . .ΤΑ ΝΕΑ

Ημ. Έκδοσης: . . .27/09/2025 Ημ. Αποδελτίωσης: . . .27/09/2025

Σελίδα: 8

Κυβερνοεπιθέσεις

Ενας επικίνδυνος θαυμαστός καινούργιος (;) κόσμος

ΤΟΥ ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΚΑΡΑΤΡΑΝΤΟΥ

Η κυβερνοεπίθεση που είχε επίπτωση σε διάφορα ευρωπαϊκά αεροδρόμια και προκάλεσε καθυστερήσεις σε πτήσεις και ταλαιπωρία στους επιβάτες έφερε ξανά στο επίκεντρο το ζήτημα της κυβερνοασφάλειας στην Ευρώπη. Σύμφωνα με τα στοιχεία της έρευνας ως τώρα, στόχος της κυβερνοεπίθεσης ήταν το αυτοματοποιημένο λογισμικό check-in και επιβίβασης MUSE, που παρέχεται από την αμερικανική εταιρεία Collins Aerospace και χρησιμοποιείται από αεροπορικές εταιρείες παγκοσμίως. Η επίθεση είχε επίπτωση στα αεροδρόμια του Λονδίνου (Χίθροου), των Βρυξελλών, του Βερολίνου και του Δουβλίνου. Η Εθνική Υπηρεσία Καταπολέμησης του Εγκλήματος της Μεγάλης Βρετανίας (NCA) ανακοίνωσε πως συνέλαβε έναν ύποπτο για τη συγκεκριμένη επίθεση, με την έρευνα όμως να συνεχίζεται. Πρέπει να τονιστεί, πως παρά την αρχική μεγάλη ανησυχία, η Ευρωπαϊκή Επιτροπή εμφανίζεται καθησυχαστική και δεν χαρακτηρίζει την επίθεση σοβαρή ή επικίνδυνη. Το να ασχολείται όμως ένα κράτος ή ένας οργανισμός με το ζήτημα της κυβερνοασφάλειας ευκαιριακά και στο πλαίσιο διαχείρισης - ανταπόκρισης σε ένα περιστατικό δεν αποτελεί χαρακτηριστικό στοιχείο της κρισιμότητας του θέματος.

Η κυβερνοασφάλεια, τόσο για την ΕΕ, όσο και για την συντριπτική πλειονότητα των κρατών - μελών, αποτελεί κρίσιμη προτεραιότητα στην πολιτική ασφάλειας. Η ραγδαία λοιπόν ανάπτυξη της τεχνολογίας, στην εποχή της 4ης Βιομηχανικής Επανάστασης, της τεχνητής νοημοσύνης και του «Διαδικτύου των πραγμάτων» (Internet of Things) έχει μεταβάλει εκ βάθρων τη λειτουργία των κρατών, τις υποδομές και, κυρίως, την καθημερινότητα των πολιτών. Πράγματι, η ανάπτυξη μας τεχνολογίας μπορεί να βελτιώνει την ποιότητα της ζωής μας αλλά, παράλληλα, διευρύνει και την τρωτότητά μας. Αυτός είναι και ο βασικός λόγος που οι νέες τεχνολογίες είναι πλέον στενά συνδεδεμένες με τις πολιτικές ασφάλειας.

ΚΥΒΕΡΝΟΑΠΕΙΛΕΣ

Η αλματώδης εξέλιξη της τεχνολογίας είναι αυτή που έχει επηρεάσει τόσο την έννοια της ασφάλειας, όσο και τη φύση των απειλών. Από τις κυβερνοαπειλές μέχρι την τρομοκρατία και τις διάφορες μορφές βίας η κακόβουλη χρήση της τεχνολογίας έχει καταστεί εργαλείο των εγκληματιών, η τεχνολογία είναι, όμως, και το μεγαλύτερο όπλο για τους φορείς επιβολής του νόμου και τα κράτη. Αντίστοιχα τεχνολογικά εξελιγμένες, ωστόσο, είναι και οι απειλές τόσο από κρατικούς, όσο και μη κρατικούς δρώντες. Μετά-δεδομένα, αλγόριθμοι, τεχνητή νοημοσύνη, Διαδίκτυο των πάντων είναι συστατικά αυτής της φάσης.

Πρέπει σε αυτό το σημείο να κάνουμε μια διάκριση μεταξύ των απειλών ασφάλειας στον κυβερνοχώρο και στις κυβερνοεπιθέσεις αυτές καθαυτές. Στην πρώτη κατηγορία μιλάμε για ένα ευρύ φάσμα που εκτείνεται από τις οικονομικές απάτες, τη σεξουαλική εκμετάλλευση ανηλίκων, τα κυβερνοεγκλήματα, τη διακίνηση ψευδών ειδήσεων, της υβριδικής επίθεσης που θα εμπεριέχει και τη διάσταση του Διαδικτύου, τη δραστηριοποίηση του οργανωμένου εγκλήματος και της τρομοκρατίας στο «σκοτεινό διαδίκτυο» (dark web), όπως το εμπόριο όπλων και ναρκωτικών, η προπαγάνδα, η ριζοσπαστικοποίηση, η στρατολόγηση μαχητών μέχρι και τη χρηματοδότηση τρομοκρατικών επιθέσεων.

Στη δεύτερη κατηγορία ανήκουν οι κυβερνοεπιθέσεις με πλέον γνωστές μορφές την επίθεση κατά της διαθεσιμότητας συστήματος ή υπηρεσίας (DDOS- Distribution Denial of Services επιθέσεις) και το Λυτρισμικό (Ransomware).

Σύμφωνα με τον ENISA οι κυριότερες κυβερνοαπειλές που αντιμετωπίζει η ΕΕ και τα κράτη - μέλη είναι οι ακόλουθες:

1. Απειλές κατά της διαθεσιμότητας συστήματος ή υπηρεσίας (DDOS - Distribution Denial of Services επιθέσεις).
2. Λυτρισμικό (Ransomware)
3. Απειλές κατά των δεδομένων
4. Κοινωνική μηχανική (Social Engineering)
5. Κακόβουλο λογισμικό
6. Επιθέσεις στην αλυσίδα εφοδιασμού

Επί του συνολικού ποσοστού των επιθέσεων το 46% έχουν τη μορφή DDOS και το 27% Ransomware. Ειδικότερα, η DDOS έχει στόχο την πρόκληση τεχνητής υπερβολικής ζήτησης πρόσβασης σε ένα δίκτυο, με αποτέλεσμα αυτό να καθυστερήσει ή να διακόψει τη λειτουργία του. Ας φανταστούμε

1. ΕΝΑΣ ΘΑΥΜΑΣΤΟΣ ΚΑΙΝΟΥΡΓΙΟΣ (;) ΚΟΣΜΟΣ

Μέσο: . . . . . .ΤΑ ΝΕΑ
Ημ. Έκδοσης: . . .27/09/2025 Ημ. Αποδελτίωσης: . . .27/09/2025
Σελίδα: 9

εκατοντάδες ανθρώπους να εισβάλλουν την ίδια στιγμή σε ένα πολυκατάστημα και να ζητούν να εξυπηρετηθούν, μπλοκάροντας στην πράξη τη διαδικασία εξυπηρέτησης πελατών. Αυτό κάνει και η επίθεση DDOS σε ψηφιακό δίκτυο που παρέχει υπηρεσία και οι «πελάτες» είναι τα περίφημα bots ή botnets, μία σύντμηση από τη λέξη robot, δηλαδή ένα αυτοματοποιημένο πρόγραμμα που πραγματοποιεί προκαθορισμένες ενέργειες και προσποιείται τον χρήστη. Αυτός είναι και ο λόγος που πολύ συχνά συναντάμε καρτέλες που προσπαθούν να εντοπίσουν πως ο χρήστης δεν είναι robot-bot. Η Ransomware, από την άλλη, είναι μια επίθεση με κακόβουλο λογισμικό που «κλειδώνει» τον στόχο, με σκοπό τα λύτρα από τον κάτοχο της συσκευής/δικτύου/υπηρεσίας.

Τα πράγματα γίνονται δυσκολότερα όταν συζητάμε για το ποιος μπορεί και πραγματοποιεί τέτοιες επιθέσεις και γιατί. Πρόκειται για μια πραγματική Λερναία Ύδρα. Μεμονωμένοι χάκερ, ομάδες κυβερνοακτιβιστών, κυβερνοεγκληματίες που μισθώνουν τις υπηρεσίες τους, αλλά και παρακρατικές και κρατικές υπηρεσίες συγκεκριμένων κρατών. Ως παράδειγμα, πίσω από μια τέτοια επίθεση μπορούμε να βρούμε από τους Anonymous μέχρι τη Mustang Panda, κινεζική κυβερνοομάδα ή τους Killnet, που είναι οι πλέον ειδικοί σε επιθέσεις DDOS και λειτουργούν υποστηρικτικά προς τα συμφέροντα της Ρωσίας. Οι κυβερνοεπιθέσεις είναι άλλωστε συστατικό στοιχείο του υβριδικού δόγματος πολέμου και επιχειρήσεων, που αποτελεί τη βασική στρατηγική της Ρωσίας τα τελευταία χρόνια.

ΟΙ ΣΤΟΧΟΙ ΚΑΙ ΟΙ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ

Η επίθεση που επηρέασε τα αεροδρόμια επιβεβαιώνει με τον πλέον χαρακτηριστικό τρόπο πως αυτές οι ενέργειες δεν πραγματοποιούνται ωστόσο μόνο εναντίον δημόσιων υπηρεσιών, αλλά και κατά εταιρειών, ακόμη και ιδιωτών. Μια επίθεση DDOS μπορεί να στοχεύσει από το online τραπεζικό σύστημα μέχρι μια ηλεκτρονική πλατφόρμα παραγγελίας φαγητού, αλλά και ένα μέσο κοινωνικής δικτύωσης. Ενώ η πιο απλή μορφή επίθεσης Ransomware γίνεται κατά ιδιώτη, όπου με κλείδωμα του υπολογιστή του ζητούν ένα συγκεκριμένο χρηματικό ποσό ως αντάλλαγμα.

Αυτή είναι η εικόνα που προκύπτει και από τα στοιχεία του ENISA: 19% φορείς δημόσιας διοίκησης, 11% μεταφορές, 9% χρηματοπιστωτικές υπηρεσίες, 9% ψηφιακές υποδομές, 8% επιχειρήσεις, 8% ευρύ κοινό και 6% μεταποίηση. Εχει ενδιαφέρον η κατάσταση με τον τομέα των μεταφορών, που είναι ο δεύτερος σε στοχοποίηση. Από τον Ιούλιο του 2023 έως τον Ιούλιο του 2024 το 21% των επιθέσεων DDOS στην ΕΕ έγινε στον τομέα των μεταφορών. Οι δύο ομάδες που στοχεύουν περισσότερο τον τομέα των μεταφορών στην Ευρώπη είναι οι Noname057, ομάδα hackers που συνδέεται και υποστηρίζει τη Ρωσία και πραγματοποιεί κυρίως επιθέσεις DDOS και οι Black Basta, διεθνής ομάδα κυβερνοεγκληματιών που πραγματοποιεί κυρίως επιθέσεις Ransomware.

Ο τομέας των μεταφορών και κυρίως τα αεροδρόμια αποτελούν σημαντικό μέρος αυτών που χαρακτηρίζουμε ως κρίσιμες υποδομές ή οντότητες. Η ασφάλεια λοιπόν των κρίσιμων υποδομών είναι ένα από τα πλέον ραγδαία αναπτυσσόμενα πεδία της δημόσιας πολιτικής και της πολιτικής ασφάλειας και προστασίας, στο οποίο η ΕΕ έχει κάνει σημαντικά βήματα τα τελευταία χρόνια. Ωστόσο, δεν είναι μία εύκολη διαδικασία, καθώς προϋποθέτει την εμπλοκή και τη συνεργασία πολλών και διαφορετικών φορέων του Δημοσίου, αλλά και του ιδιωτικού τομέα. Είναι χαρακτηριστικό πως σε αρκετές περιπτώσεις πολλές χώρες δεν έχουν προσδιορίσει τις κρίσιμες υποδομές τους, ενώ και όπου αυτές έχουν προσδιοριστεί, υπάρχουν σημαντικές διαφοροποιήσεις μεταξύ των χωρών.

Σύμφωνα με την Οδηγία 2557 του 2022 για την ανθεκτικότητα των κρίσιμων οντοτήτων, την οποία η Ελλάδα θα ενσωματώσει το επόμενο διάστημα, ως κρίσιμη χαρακτηρίζεται μια δημόσια ή ιδιωτική οντότητα, η οποία ανήκει σε έναν από τους τομείς που προβλέπει η Οδηγία και παρέχει μια υπηρεσία, η οποία είναι κρίσιμης σημασίας για τη διατήρηση ζωτικών κοινωνικών λειτουργιών, οικονομικών δραστηριοτήτων, της δημόσιας υγείας και ασφάλειας ή του περιβάλλοντος.

Είναι χαρακτηριστικό πως η Οδηγία προβλέπει έντεκα τομείς, στους οποίες περιλαμβάνονται και οι μεταφορές και ειδικότερα: ενέργεια, μεταφορές, τραπεζικός τομέας, χρηματοπιστωτικά ιδρύματα, υγειονομικός τομέας, ύδρευση (πόσιμο νερό), διαχείριση λυμάτων, ψηφιακές υποδομές, δημόσια διοίκηση, Διάστημα και ο επισιτιστικός τομέας.

Πρέπει ωστόσο να τονιστεί πως στον τομέα της κυβερνοασφάλειας υπάρχει το πλαίσιο που βάζει η οδηγία NIS II, η οποία ενσωματώθηκε από την Ελλάδα με τον νόμο 5160 του 2024, με υπεύθυνο φορέα την Εθνική Αρχή Κυβερνοασφάλειας.

Η κυβερνοεπίθεση που είχε επίπτωση σε διάφορα ευρωπαϊκά αεροδρόμια (φωτογραφία από το Χίθρου) και προκάλεσε καθυστερήσεις σε πτήσεις και ταλαιπωρία στους επιβάτες, έφερε ξανά στο επίκεντρο το ζήτημα της κυβερνοασφάλειας στην Ευρώπη

Ο Τριαντάφυλλος Καρατράντος, είναι δρ. Ευρωπαϊκής Ασφάλειας και Νέων Απειλών, επιστημονικός συνεργάτης ΕΛΙΑΜΕΠ

REUTERS/ISABEL INFANTES

Οι υβριδικές απειλές

Λίγες ημέρες μετά την κυβερνοεπίθεση που επηρέασε τη λειτουργία των τεσσάρων αεροδρομίων, προέκυψε ένα ακόμη περιστατικό με την πτήση drones πάνω από την περιοχή του αεροδρομίου του Οσλο και της Κοπεγχάγης που συνέδεσε την κυβερνοασφάλεια με τις υβριδικές απειλές. Οι υβριδικές εκστρατείες είναι πολυδιάστατες, συνδυάζοντας καταναγκαστικά και ανατρεπτικά μέτρα, χρησιμοποιώντας συμβατικά και μη συμβατικά εργαλεία και τακτικές. Σχεδιάζονται έτσι ώστε να είναι δύσκολο να εντοπιστούν ή να αποτυπωθούν. Αυτές οι απειλές στοχεύουν σε κρίσιμες τρωτότητες και επιδιώκουν να δημιουργήσουν σύγχυση για να εμποδίσουν την ταχεία και αποτελεσματική λήψη αποφάσεων. Οι υβριδικές απειλές μπορεί να εκτείνονται από τις κυβερνοεπιθέσεις σε κρίσιμα συστήματα πληροφοριών, μέσω της διατάραξης κρίσιμων υπηρεσιών όπως η παροχή ενέργειας ή χρηματοπιστωτικών υπηρεσιών, ως και την υπονόμευση της εμπιστοσύνης του κοινού σε κρατικούς θεσμούς ή την εμβάθυνση των κοινωνικών διαιρέσεων.

Μια χαρακτηριστική περίπτωση κυβερνοεπιθέσεων στο πλαίσιο υβριδικής επιχείρησης είναι αυτή που αντιμετώπισε το Μαυροβούνιο από τον Μάιο του 2016 μέχρι τον Ιούνιο του 2017. Η χώρα δέχτηκε μία μεγάλη αύξηση τόσο στον αριθμό, όσο και στην ένταση των κυβερνοεπιθέσεων, οι οποίες από 22 το 2012, έφτασαν στις 400 το 2017. Κατά τη διάρκεια των κοινοβουλευτικών εκλογών του Οκτωβρίου του 2016 τα πολιτικά κόμματα και οι οργανώσεις της Κοινωνίας των Πολιτών που υποστήριζαν την ένταξη της χώρας στην ΕΕ και στο NATO έγιναν στόχος μεγάλης κλίμακας επιθέσεων DDoS. Οι επιθέσεις έγιναν από τη ρωσική ομάδα χάκερς APT28, γνωστή και ως Fancy Bear, η οποία είχε δεσμούς με την GRU, την στρατιωτική υπηρεσία πληροφοριών της Ρωσίας.

Η κυβερνοασφάλεια είναι ένα από τα πλέον δυναμικά πεδία της πολιτικής ασφάλειας. Πέραν των δεδομένων ιδιαιτεροτήτων, όπως είναι ο μεγάλος βαθμός εξάρτησης κρατών, επιχειρήσεων και πολιτών από τον κυβερνοχώρο και η ανάγκη στενής συνεργασίας δημόσιου και ιδιωτικού τομέα, οι αναδυόμενες τεχνολογίες, όπως το Διαδίκτυο των Πραγμάτων, έρχονται για να εξελίξουν δυναμικά τόσο τις κυβερνοαπειλές, όσο και την κυβερνοασφάλεια. Το μέλλον είναι ήδη εδώ και η πολιτική κυβερνοασφάλειας πρέπει να είναι πλήρως εμπροσθοβαρής, συνεργατική και συμπεριληπτική, στη βάση της συμμετοχής όλων μας στην ολιστική κοινωνική ανθεκτικότητα.