

## **Ο ENISA σκιαγραφεί το τοπίο των απειλών στον κυβερνοχώρο κατά το 2014: οι 15 κυριότερες απειλές στον κυβερνοχώρο, οι παράγοντες απειλής στον κυβερνοχώρο, οι μέθοδοι επίθεσης στον κυβερνοχώρο και οι τάσεις απειλής για αναδυόμενους τεχνολογικούς τομείς.**

Η έκθεση [Τοπίο απειλών 2014 του ENISA](#) (ETL 2014), που δημοσιεύτηκε σήμερα είναι η τρίτη κατά σειρά ετήσια έκθεση, η οποία ενοποιεί και αναλύει τις κυριότερες απειλές στον κυβερνοχώρο και τη σχετική εξέλιξη κατά τη διάρκεια του 2014. Το Τοπίο απειλών 2014 του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), δραστηριότητα που συμβάλλει στην προσπάθεια επίτευξης των στόχων που διατυπώνονται στη στρατηγική ασφάλειας στον κυβερνοχώρο για την ΕΕ, τονίζει τη σημασία της ανάλυσης των απειλών και τον προσδιορισμό των αναδυόμενων τάσεων στην ασφάλεια στον κυβερνοχώρο.

Μεταξύ των καινοτομιών της έκθεσης ETL 2014 είναι:

- οι πληροφορίες για τα διανύσματα επιθέσεων (attack vectors), που δίνουν κάποια πρώτα στοιχεία για τον τρόπο μιας επίθεσης στον κυβερνοχώρο
- η εμβάθυνση σε περιπτώσεις χρήσης των πληροφοριών για απειλές, δείχνοντας τον τρόπο που η ανάλυση των απειλών μπορεί να χρησιμοποιηθεί στις φάσεις διαχείρισης της ασφάλειας, και
- η συμμετοχή των ενδιαφερόμενων φορέων, αποτελούμενων από 13 εμπειρογνώμονες από Ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), παρόχους, κράτη μέλη και χρήστες.

Το 2014 παρατηρήθηκαν σημαντικές αλλαγές στις κυριότερες απειλές: αυξημένη περιπλοκότητα των επιθέσεων, επιτυχείς επιθέσεις σε ζωτικής σημασίας λειτουργίες ασφαλείας του διαδικτύου, αλλά και επιτυχείς επιχειρήσεις διεθνούς συντονισμού για επιβολή του νόμου, καθώς επίσης πάροχοι ασφαλείας. Πολλές από τις αλλαγές που σημειώθηκαν στις απειλές στον κυβερνοχώρο μπορούν να αποδοθούν ακριβώς σ' αυτόν το συντονισμό και στην κινητοποίηση της κοινότητας του κυβερνοχώρου. Ωστόσο, τα διαθέσιμα στοιχεία υποδεικνύουν ότι τα μελλοντικά τοπία των απειλών στον κυβερνοχώρο θα συνεχίσουν να έχουν μεγάλη δυναμική.

Το 2014 μπορεί να χαρακτηριστεί ως έτος της παραβίασης δεδομένων. Οι σοβαρότατες παραβιάσεις δεδομένων κατέδειξαν σοβαρότατες επιθέσεις σε κύριες λειτουργίες ασφαλείας του διαδικτύου, δείχνοντας πόσο αποτελεσματικά καταχρώνται οι παράγοντες απειλής τις αδυναμίες ασφαλείας επιχειρήσεων και κυβερνήσεων. Τα κύρια διδάγματα που αντλούνται από την ETL υπογραμμίζουν ότι η προχειρότητα ως προς την ασφάλεια στον κυβερνοχώρο είναι ο νούμερο ένα λόγος των παραβιάσεων, αντιπροσωπεύοντας το 50% των περιπτώσεων. Επιπλέον, μια θετική εξέλιξη αντανακλάται στην αύξηση τόσο της ποιότητας όσο και της ποσότητας των πληροφοριών που συλλέγονται, οδηγώντας σε καλύτερη αξιολόγηση των απειλών και αναλυτικότερο υλικό για τους τελικούς χρήστες.

Στην ETL 2014, τα στοιχεία για τις εξελίξεις αυτές ενοποιούνται μέσω των κυριότερων απειλών στον κυβερνοχώρο και των αναδυόμενων τάσεων απειλών σε διάφορους τομείς τεχνολογίας και εφαρμογών, με αναφορές σε περισσότερες από 400 σχετικές πηγές για τις απειλές, για να διευκολυνθούν οι υπεύθυνοι χάραξης πολιτικής, οι ειδικοί στην ασφάλεια και τα ενδιαφερόμενα άτομα να περιηγηθούν μέσα στο τοπίο των απειλών στον κυβερνοχώρο.

28/01/2015

EPR04/2015

www.enisa.europa.eu

Οι αναδυόμενες τεχνολογίες που θα επηρεάσουν το τοπίο των απειλών είναι: φυσικά συστήματα στον κυβερνοχώρο (CPS), κινητή πληροφορική και υπολογιστικό νέφος, υποδομές εμπιστοσύνης, μαζικά δεδομένα και το Διαδίκτυο των πραγμάτων. Τα CPS – που επηρεάζουν σε σημαντικό βαθμό την προστασία των υποδομών πληροφοριών ζωτικής σημασίας – αντιπροσωπεύουν μια ξεχωριστή ευκαιρία για τη δημιουργία ανταγωνιστικών πλεονεκτημάτων για την ευρωπαϊκή βιομηχανία και έρευνα.

Ο [Udo Helmbrecht](#), εκτελεστικός διευθυντής του ENISA, έκανε τα εξής σχόλια για το έργο: «Ο προσδιορισμός και η κατανόηση της δυναμικής των απειλών στον κυβερνοχώρο εξελίσσεται σε ένα πολύ σημαντικό εργαλείο ασφαλείας στον κυβερνοχώρο. Η δυναμική του τοπίου των απειλών στον κυβερνοχώρο θέτει τις παραμέτρους για ευέλικτα αλλά αποτελεσματικά καθεστώτα προστασίας ασφαλείας που θα είναι προσαρμοσμένα στην πραγματική έκθεση. Η κατανόηση των δεσμών εξάρτησης ανάμεσα σε όλες τις συνιστώσες του τοπίου των απειλών αποτελεί σημαντική γνώση και καταλυτικό μοχλό για τις ενεργές και ευέλικτες πρακτικές διαχείρισης ασφαλείας. Με την ETL 2014, ο ENISA συνεχίζει να συμβάλλει στο να τίθεται στη διάθεση του κοινού η γνώση για τις απειλές στον κυβερνοχώρο».

Φέτος, ο ENISA ανέπτυξε δύο θεματικά τοπία για τις απειλές: ένα για τον τομέα της [Υποδομής του Διαδικτύου](#) και ένα για τα περιβάλλοντα «έξυπνου σπιτιού», που θα δημοσιευτούν τον επόμενο μήνα. Τα μεμονωμένα θεματικά τοπία για τις απειλές παρέχουν καθοδήγηση για την ανάπτυξη προστατευτικών μέτρων ώστε να ελαχιστοποιηθεί η έκθεση των πολύτιμων περιουσιακών στοιχείων στις απειλές σε διάφορους τομείς.

Για την πλήρη έκθεση: [Τοπίο απειλών 2014 του ENISA](#)

#### Σημειώσεις προς τους συντάκτες:

- Ο **πίνακας 1** δίνει «Επισκόπηση των 15 κυριότερων αξιολογημένων τρεχουσών απειλών στον κυβερνοχώρο και των αναδυόμενων τάσεων» του «Τοπίου απειλών 2014 του ENISA». **σελ. iv**
- Ο **πίνακας 2** «Επισκόπηση και σύγκριση των τρεχόντων τοπίων απειλών κατά το 2014 και το 2013» δείχνει αλλαγές σε σχέση και με τις τάσεις και με την κατάταξη των αξιολογημένων απειλών στον κυβερνοχώρο, **σελ. 39**
- **Πίνακας 3:** «Συμμετοχή των παραγόντων απειλής στις κυριότερες απειλές», **σελ. 49**
- Έκθεση ETL ανά κεφάλαιο: Σκοπός, πεδίο εφαρμογής και μέθοδος **σελ. 5**, ETL 2014 **σελ. 13**, Παράγοντες απειλής **σελ. 41**, Διανύσματα επιθέσεων **σελ. 51**, Το τοπίο των αναδυόμενων απειλών **σελ. 59**, Προβληματισμοί και συμπεράσματα, **σελ. 79**

Για **συνεντεύξεις**: Δρ. Λούης Μαρίνος, Εμπειρογνώμων στην Ασφάλεια δικτύων και πληροφοριών, ENISA

**Email:** [louis.marinos@enisa.europa.eu](mailto:louis.marinos@enisa.europa.eu), **Τηλ.:** (+30) 2814 409 682