2013/01/08

EPR01/2013

www.enisa.europa.eu

Νέα έκθεση του οργανισμού ENISA της ΕΕ για τον κυβερνοχώρο αναλύει για πρώτη φορά τις κορυφαίες τάσεις στο τοπίο των απειλών στον κυβερνοχώρο

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) της ΕΕ για την ασφάλεια στον κυβερνοχώρο δημοσίευσε την πρώτη και πιο ολοκληρωμένη Ανάλυση του τοπίου των απειλών στον κυβερνοχώρο για το 2012, που συνοψίζει περισσότερες από 120 εκθέσεις σχετικά με τις απειλές. Η έκθεση προσδιορίζει και παραθέτει τις κορυφαίες απειλές και τις τάσεις τους, και συμπεραίνει ότι τα τμήματα κώδικα υπολογιστή που εκμεταλλεύονται σφάλματα λογισμικού σε κάποιο πρόγραμμα περιήγησης (drive-by exploits) έχουν γίνει η κορυφαία διαδικτυακή απειλή.

Η Έκθεση για το τοπίο των απειλών που δημοσίευσε η ENISA συνοψίζει 120 πρόσφατες εκθέσεις του 2011 και 2012 από εταιρείες ασφαλείας, δίκτυα αριστείας, φορείς τυποποίησης και άλλα ανεξάρτητα μέρη, αποτελώντας έτσι την πιο ολοκληρωμένη σύνθεση που διατίθεται αυτή τη στιγμή σε παγκόσμιο επίπεδο. Η έκθεση παρέχει μια ανεξάρτητη γενική εικόνα των απειλών και των παραγόντων απειλής που έχουν παρατηρηθεί, καθώς και τις τρέχουσες κορυφαίες απειλές και τα τοπία των αναδυόμενων τάσεων των απειλών. Επιπλέον, η Έκθεση για το τοπίο των απειλών στον κυβερνοχώρο αναλύει τον «εχθρό στον κυβερνοχώρο», ενώ προσδιορίζει και παραθέτει τις δέκα (από τις συνολικά δεκαέξι) κορυφαίες απειλές σε αναδυόμενους τεχνολογικούς τομείς. Οι τομείς που εξετάζονται είναι η κινητή πληροφορική, τα κοινωνικά μέσα/η τεχνολογία κοινωνικών μέσων, οι υποδομές ζωτικής σημασίας, οι υποδομές εμπιστοσύνης, το σύννεφο, και τα μαζικά δεδομένα. Οι δέκα κορυφαίες απειλές που έχουν προσδιοριστεί είναι:

1. Κώδικας υπολογιστή που εκμεταλλεύεται σφάλματα λογισμικού σε κάποιο πρόγραμμα περιήγησης – Drive-by exploits (η προσθήκη κακόβουλου κώδικα που εκμεταλλεύεται τις ευπάθειες του προγράμματος περιήγησης)
2. Οι ιοί τύπου worm/δούρειοι ίπποι
3. Επιθέσεις με προσθήκη κακόβουλου κώδικα
4. Τα σετ προγραμμάτων εκμετάλλευσης της ευπάθειας (έτοιμο πακέτο λογισμικού για την αυτοματοποίηση του εγκλήματος στον κυβερνοχώρο)
5. Τα δίκτυα προγραμμάτων ρομπότ – Botnet (σφετερισμός υπολογιστών που ελέγχονται εξ αποστάσεως)
6. Οι(κατανεμημένες) επιθέσεις άρνησης υπηρεσιών ((Distributed) Denial of Service attacks – DDoS/DoS)
7. Το ηλεκτρονικό «ψάρεμα» – Phishing (δόλια ηλεκτρονικά μηνύματα και δόλιοι δικτυακοί τόποι)
8. Η διακινδύνευση εμπιστευτικών πληροφοριών (παραβιάσεις δεδομένων)
9. Το παραπλανητικό λογισμικό ασφαλείας (Rogueware/scareware)
10. Τα ανεπίκλητα ηλεκτρονικά μηνύματα

Τέλος, ο Οργανισμός καταλήγει σε μια σειρά συμπερασμάτων για τις εταιρείες και τους ενδιαφερόμενους φορείς αναφορικά με το πώς καταπολεμούνται καλύτερα οι απειλές στον κυβερνοχώρο κατά των επιχειρήσεων, των πολιτών και της ψηφιακής οικονομίας γενικά:

- Να χρησιμοποιείται κοινή ορολογία στις εκθέσεις για τις απειλές
- Να συμπεριλαμβάνεται η οπτική γωνία του τελικού χρήστη
- Να αναπτυχθούν σενάρια χρήσης για τα τοπία απειλών
- Να συλλέγονται πληροφορίες ασφαλείας για τα διάφορα περιστατικά, συμπεριλαμβανομένης της αρχής και του στόχου μιας επίθεσης
- Να μεταβάλλονται οι έλεγχοι ασφαλείας, ώστε να καλύπτονται οι αναδυόμενες τάσεις απειλής
- Να συλλέγονται και να αναπτύσσονται καλύτερα στοιχεία για τα εφαλτήρια (τις μεθόδους) των επιθέσεων, ώστε να γίνονται κατανοητές οι ροές εργασίας των επιθέσεων
- Να συλλέγονται και να αναπτύσσονται καλύτερα στοιχεία για τις επιπτώσεις που προκαλούν οι εισβολείς
- Να συλλέγονται και να διατηρούνται περισσότερες ποιοτικές πληροφορίες για τους παράγοντες απειλής

Ο Καθηγητής Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA, δήλωσε:

«Είμαι περήφανος που ο Οργανισμός αναλαμβάνει αυτό το σημαντικό έργο ώστε να γίνει καλύτερα κατανοητή η σύνθεση των τρεχουσών απειλών στον κυβερνοχώρο. Αυτή είναι η πρώτη και πιο ολοκληρωμένη Ανάλυση των απειλών στον κυβερνοχώρο που υπάρχει σήμερα, και σημείο αναφοράς για όλους τους υπευθύνους χάραξης πολιτικής και τους φορείς ασφαλείας στον κυβερνοχώρο».

Για την πλήρη **έκθεση**, όπου αναφέρονται σε βάθος όλες οι απειλές και τα συμπεράσματα

Για συνεντεύξεις: Graeme Cooper, Διευθυντής Δημοσίων Υποθέσεων, κινητό: +30 6951 782 268, ή Ulf Bergström, Εκπρόσωπος Τύπου, + 30 6948 460 143, press@enisa.europa.eu ή Δρ. Λούης Μαρίνος, louis.marinos@enisa.europa.eu

Μετάφραση. Η μόνη επίσημη έκδοση είναι η αγγλική.
http://www.enisa.europa.eu/media/enisa-in-greek/
www.enisa.europa.eu