Η ασφάλεια στον κυβερνοχώρο σύμφωνα με τον Γουίνι το Αρκουδάκι: Νέα έκθεση του Ευρωπαϊκού Οργανισμού ENISA σχετικά με τη χρήση «ψηφιακών παγίδων» ή honeypots ("βάζα με το μέλι") για τον εντοπισμό δικτυακών επιθέσεων

Ο οργανισμός της ΕΕ «για την ασφάλεια στον κυβερνοχώρο» ENISA παρουσιάζει μια λεπτομερή μελέτη σχετικά με 30 διαφορετικές «ψηφιακές παγίδες» ή honeypots που μπορούν να χρησιμοποιηθούν από τις Ομάδες Αντιμετώπισης Έκτακτων Αναγκών στην Πληροφορική (CERTs) και τις Εθνικές/Κυβερνητικές CERTs για τον προληπτικό εντοπισμό των επιθέσεων στον κυβερνοχώρο. Η μελέτη αποκαλύπτει εμπόδια στην κατανόηση των βασικών εννοιών περί honeypots και υποβάλλει συστάσεις σχετικά με το που θα πρέπει να χρησιμοποιούνται.

Ο αυξανόμενος αριθμός σύνθετων επιθέσεων στον κυβερνοχώρο απαιτεί καλύτερους μηχανισμούς έγκαιρου εντοπισμού για τις CERTs. Τα honeypots είναι απλά, παγίδες με μοναδικό στόχο να δελεάσουν τους επιτιθέμενους παριστάνοντας μια πραγματική υπολογιστική πηγή (π.χ. υπηρεσία, εφαρμογή, σύστημα ή δεδομένα). Οποιαδήποτε οντότητα συνδεθεί σε κάποιο honeypot θεωρείται ύποπτη και όλη η δραστηριότητα παρακολουθείται με στόχο να εντοπιστεί η δόλια δραστηριότητα.

Αυτή η μελέτη αποτελεί συνέχεια μιας πρόσφατης έκθεσης του ENISA για τον προληπτικό εντοπισμό περιστατικών ασφαλείας δικτύου. Η προηγούμενη έκθεση κατέληγε στο συμπέρασμα ότι ενώ οι CERT αναγνωρίζουν πως τα honeypots παρέχουν σημαντική γνώση κατά της ηλεκτρονικής πειρατείας, η χρησιμότητά τους για τον εντοπισμό και τη διερεύνηση επιθέσεων εξακολουθεί να μην είναι τόσο διαδεδομένη όσο θα περίμενε κανείς. Το γεγονός αυτό θέτει φραγμούς στην ανάπτυξή τους.

Η νέα μελέτη παρουσιάζει πρακτικές στρατηγικές ανάπτυξης και σημαντικά ζητήματα για τις CERT. Συνολικά, ελέγχθηκαν και αξιολογήθηκαν 30 honeypots σε διαφορετικές κατηγορίες. Στόχος: η πληροφόρηση σχετικά με ποιες τεχνολογίες ανοιχτού κώδικα και ποια honeypots είναι καλύτερα για εγκατάσταση και χρήση. Εφόσον δεν υπάρχει κάποια μαγική λύση, αυτή η νέα μελέτη εντόπισε ορισμένες ελλείψεις και ορισμένους φραγμούς στην εγκατάσταση των honeypots: η δυσκολία στη χρήση, η ανεπαρκής τεκμηρίωση, η έλλειψη σταθερότητας λογισμικού και υποστήριξης των προγραμματιστών, η ελάχιστη τυποποίηση και η ανάγκη ατόμων με εξειδικευμένες γνώσεις καθώς και προβλήματα κατανόησης των βασικών εννοιών περί honeypots . Η μελέτη παραθέτει επίσης μια ταξινόμηση και διερευνά το μέλλον των honeypots.

Ο εκτελεστικός διευθυντής του ENISA, καθηγητής Udo Helmbrecht σχολιάζει:

«Τα honeypots αποτελούν ένα ισχυρό εργαλείο για τις CERT προκειμένου να συλλέξουν πληροφορίες για εν δυνάμει απειλές χωρίς επιπτώσεις στις υποδομές παραγωγής. Με ορθή εγκατάσταση, τα honeypots *προσφέρουν σημαντικά οφέλη στις CERT. Η δόλια δραστηριότητα στους κόλπους των ομάδων CERT μπορεί*

να εντοπιστεί ώστε να παρέχει έγκαιρη προειδοποίηση σχετικά με κακόβουλο λογισμικό, νέα είδη εκμεταλλεύσεων (exploits), τρωτά σημεία και κακόβουλη συμπεριφορά καθώς και τη δυνατότητα άντλησης γνώσεων για τις τακτικές των επιτιθέμενων. Κατά συνέπεια, εάν οι ομάδες CERT στην Ευρώπη αναγνωρίσουν τα honeypots ως ελκυστική επιλογή, θα μπορούσαν να προασπίσουν καλύτερα τα συμφέροντα τους.»

Για την πλήρη έκθεση
Για το ιστορικό: COM(2009)149 και NATO Legal Implications of Countering Botnets

Για συνεντεύξεις παρακαλούμε επικοινωνήστε: Ulf Bergstrom, εκπρόσωπος, press@enisa.europa.eu ή κινητό: +30 6948 460 143 ή Cosmin Cioabanu, εμπειρογνώμονας ENISA στο opsec@enisa.europa.eu

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