ΜΥΡΙΩΠΟΣ (Τ2ΕΔΚ-04665)

Προηγμένη ανίχνευση εισβολών και παράνομου ηλεκτρονικού περιεχομένου για τη διασφάλιση επιχειρησιακής και λειτουργικής ασφάλειας σε κατανεμημένα συστήματα συστημάτων.

Το Έργο

Την άνοιξη του 2017 ξεκίνησε να διαδίδεται το πιο απλό αλλά πολύ γρήγορα επεκτεινόμενο τμήμα κακόβουλου λογισμικού με όνομα «NotPetya» που έχει δει ως σήμερα η ανθρωπότητα, το οποίο μετεξελίχθηκε στο «WannaCry» με αποκορύφωση το καλοκαίρι του 2017. Αυτό είχε ως αποτέλεσμα μεγάλες επιχειρήσεις να παύουν να λειτουργούν αποτελεσματικά με ανυπολόγιστο κόστος τόσο σε υποδομές όσο και σε χρήματα. Ανάμεσά τους προσβλήθηκε η Maersk όπου αναγκάστηκε να θέσει εκτός λειτουργίας χιλιάδες υπολογιστές και διακομιστές με κόστος που εκτιμάται στα 300 εκατομμύρια δολάρια. Το έργο ΜΥΡΙΩΠΟΣ έρχεται ως αντίδοτο στη διασφάλιση επιχειρησιακής και λειτουργικής ασφάλειας εισάγοντας και προτείνοντας νέες τεχνικές και συνδυαστικές υπηρεσίες τόσο σε επίπεδο υλικού όσο και σε επίπεδο λογισμικού για την έγκαιρη ανίχνευση εισβολών και παράνομου ηλεκτρονικού περιεχομένου με στόχο την επίτευξη αυξημένης προστασίας σε υποδομές, υπηρεσίες και εφαρμογές. Η αποκλιμάκωση των πιθανών εισβολών και κινδύνων περιλαμβάνει την ανάλυση και δεικτοδότηση της πληροφορίας στο διαδίκτυο και το σκοτεινό δίκτυο, δυνατότητες έγκαιρου εντοπισμού πιθανών εισβολών μέσω κατανεμημένης επεξεργασίας, γρήγορης εκφόρτωσης δεδομένων, επιτάχυνσης υλικού και επιβολής πολιτικών ασφάλειας. Το έργο ΜΥΡΙΩΠΟΣ θα υλοποιήσει μια ολιστική λύση ασφάλειας, ικανή να εξαλείψει τις κυβερνοεπιθέσεις, να προσδιορίσει και κατηγοριοποιήσει εγκαίρως παραβατικές συμπεριφορές στο διαδίκτυο και στο σκοτεινό δίκτυο μέσω της κατάλληλης μοντελοποίησης των διαφορετικών εννοιών του συστήματος συστημάτων, της προηγμένης επαλήθευσης και επιβολής πολιτικών ασφάλειας σε πραγματικό χρόνο.

Στόχοι

Οι στόχοι του έργου ΜΥΡΙΩΠΟΣ προσδιορίζονται με τη μέθοδο SMART (Specific, Measurable, Achievable, Realistic, Timely) και είναι οι ακόλουθοι:

- Ανάπτυξη μιας νέας υποδομής για κλιμακούμενες υπηρεσίες ασφάλειας δικτύων με στόχο την ασφαλή παραμετροποίηση, εγκατάσταση και λειτουργία κατανεμημένων υπηρεσιών ανίχνευσης και προστασίας σε ετερογενείς συλλογές υλικού και λογισμικού.
- Ανάπτυξη καινοτόμων μεθόδων ανίχνευσης ανωμαλιών σε πραγματικό χρόνο που επεκτείνουν την τρέχουσα τεχνολογική στάθμη, ευφυΐας ιστού και εξαγωγής σημασιολογικής γνώσης αξιοποιώντας τεχνικές βαθιάς μηχανικής μάθησης και έξυπνες κάρτες δικτύου που προσφέρουν κατανεμημένη επεξεργασία, γρήγορη εκφόρτωση «ύποπτης πληροφορίας» με προγραμματιζόμενα μονοπάτια δεδομένων

για την αποτελεσματική, ευέλικτη και έγκαιρη ανίχνευση παραβατικών δραστηριοτήτων στον κυβερνοχώρο.
- Ανάπτυξη ενός μοντέλου αξιολόγησης κινδύνου σε πραγματικό χρόνο που διευκολύνει τον χειρισμό απειλών εγκαίρως, σε συνδυασμό με ένα μοντέλο επιβολής πολιτικών ασφάλειας, ανθεκτικότητας και επιχειρησιακής προστασίας που λαμβάνει υπόψη το περιβάλλον και καταγραφές στον παγκόσμιο ιστό με σκοπό την εφαρμογή μέτρων μετριασμού, συστάσεων ή καταστολής. Στόχος 4: Επίδειξη πιλοτικής λειτουργίας, αξιολόγηση αποδοχής και υιοθέτησης του ενοποιημένου Πλαισίου ΜΥΡΙΩΠΟΣ σε μια περίπτωση χρήσης Έξυπνων Υποδομών Κτηρίου με συσκευές και υπηρεσίες από το άκρο ως το κέντρο των δεδομένων και τον καθορισμό διαφορετικών σεναρίων επίθεσης που επηρεάζονται από την ετερογένεια και την πολυπλοκότητα του συστήματος συστημάτων.

Αποτελέσματα

- Η ανάπτυξη και επίδειξη της αποτελεσματικότητας μιας σειράς καινοτόμων αλγορίθμων, μηχανισμών, βιβλιοθηκών προγραμματισμού, διεπαφών, υπηρεσιών και τεχνολογιών λογισμικού για την κατανεμημένη ευφυΐα ιστού και σκοτεινού δικτύου, κατανεμημένη βαθιά ανάλυση και νοημοσύνη κυβερνοαπειλών σε πραγματικό χρόνο.
- Η ανάπτυξη και επίδειξη της αποτελεσματικότητας μιας σειράς καινοτόμων τεχνολογιών λογισμικού και προϊόντων ποσοτικοποίησης κινδύνων από άκρη σε άκρη, εκφόρτωσης δεδομένων βάσει πολιτικών αποφυγής εισβολών, παρακολούθησης, ειδοποιήσεων και οπτικοποίησης περιουσιακών πόρων σε πραγματικό χρόνο σε ένα ενιαίο Πλαίσιο.
- Εφαρμογή και επικύρωση του Πλαισίου ΜΥΡΙΩΠΟΣ μέσω ενός συνόλου βιώσιμων προϊόντων ως αποτέλεσμα της Τεχνικής Σκοπιμότητας και ενός συνόλου προκαθορισμένων σεναρίων χρήσης σε Υποδομές Έξυπνων Κτηρίων, συμπεριλαμβανομένης της αξιολόγησης της απόδοσης ανίχνευσης ανωμαλιών σε πραγματικό χρόνο, κατανεμημένης βαθιάς ανάλυσης και εξόρυξης δεδομένων, γρήγορης εκφόρτωσης και προγραμματιζόμενων διαδρομών δεδομένων.
- Δημοσιεύσεις που θα παραχθούν από το έργο ως αποτέλεσμα της βιομηχανικής έρευνας με τη μορφή άρθρων σε τεχνικά επιστημονικά περιοδικά αλλά και σε διεθνή επιστημονικά συνέδρια. Σαν στόχο θέτουμε τη συγγραφή τουλάχιστον 6 άρθρων σε τεχνικά επιστημονικά περιοδικά υψηλού κύρους (IEEE, ACM, κλπ).
- Ενίσχυση ερευνητών που ασχολούνται με δραστηριότητες έρευνας κι ανάπτυξης των οποίων η συμμετοχή στο έργο κάνει πιο ουσιαστική και με μεγαλύτερο αντίκτυπο την παραγόμενη έρευνά τους, διευρύνοντας τη μελλοντική επαγγελματική τους πορεία. Τα αποτελέσματα του έργου θα συνεισφέρουν γενικότερα στην εξέλιξη και δια βίου μάθηση των ερευνητών μέσω δραστηριοτήτων διάδοσης της γνώσης όπως η συμμετοχή σε συνέδρια, ομάδες εργασίας και τεχνικών παρουσιάσεων.
- Ευρωπαϊκή διάσταση της έρευνας καθώς το έργο ΜΥΡΙΩΠΟΣ επεκτείνει το έργο ANASTACIA H2020-731558 και ASTRID H2020-786922 του προγράμματος Ορίζοντας 2020. Το έργο ΜΥΡΙΩΠΟΣ στοχεύει να καλύψει το κενό της ανίχνευσης και αντιμετώπισης κυβερνοκινδύνων σε πραγματικό χρόνο μέσα από ένα σύνολο μικρό-υπηρεσιών που χρησιμοποιούν πρωτοποριακούς αλγορίθμους βαθιάς μηχανικής μάθησης, κατανεμημένης ευφυΐας ιστού και σκοτεινού δικτύου, μηχανισμούς για τη

γρήγορη εκφόρτωση των δεδομένων και προγραμματιζόμενα μονοπάτια δεδομένων επιφέροντας άμεσο αντίκτυπο στο χώρο τεχνολογιών για τη ασφάλεια του κυβερνοχώρου.

Partners

Προϋπολογισμός Έργου: € 599.600
Δημόσια Δαπάνη: € 421.915