Public

NEWSLETTER 2

NetPHISH

ΠΕΡΙΕΧΟΜΕΝΑ

Ανάπτυξη καινοτόμου εργαλείου τελικού χρήστη για την προστασία από επιθέσεις ηλεκτρονικού «ψαρέματος».

ΣΥΝΤΟΝΙΣΤΗΣ ΕΡΓΟΥ

Η Neurosoft είναι μια κορυφαία εταιρεία τεχνολογίας πληροφοριών και επικοινωνιών (ΤΠΕ) που παρέχει καινοτόμες λύσεις και υπηρεσίες με στόχο την αύξηση της αποδοτικότητας και της ασφάλειας. Η εταιρεία είναι εισηγμένη στο Ιταλικό Χρηματιστήριο από το 2009, με τον ΟΠΑΠ ως μέτοχο πλειοψηφίας και απασχολεί πάνω από 200 εξειδικευμένους επαγγελματίες. Δραστηριοποιείται στην Ελλάδα, την Κύπρο και τη Νοτιοανατολική Ευρώπη, προσφέροντας σύγχρονες λύσεις και υπηρεσίες σε Υποδομές (δίκτυο, cloud, ασφάλεια), Cyber και Field, ενώ υποστηρίζει ολιστικά τις επιχειρησιακές ανάγκες των πελατών της από το Σχεδιασμό και το Consulting έως την Υποστήριξη και τα Managed Services.

ΛΕΠΤΟΜΕΡΕΙΕΣ ΕΡΓΟΥ

Κωδικός Έργου: Τ1ΕΔΚ-05112

Ιστοσελίδα: https://netphish.net/

Ημερομηνία έναρξης: 6/9/2018

Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ NETPHISH

• Το σύστημα που αναπτύσσεται στο NetPHISH είναι ένα πολυδιάστατο σύστημα που προσφέρει υπηρεσίες εντοπισμού επιθέσεων ηλεκτρονικού «ψαρέματος», μέσω ηλεκτρονικής αλληλογραφίας και εκπαίδευσης των ατόμων ενός οργανισμού. Για την ευκολότερη ανάπτυξη και διαχείριση του συστήματος χωρίζεται σε τρία επιμέρους υποσυστήματα. Τα υποσυστήματα αυτά είναι το behavior analysis, το data analytics και το artificial intelligence.

• Το υποσύστημα behavior analysis εστιάζει στην εξαγωγή χαρακτηριστικών από τα μηνύματα ηλεκτρονικού ταχυδρομείο. Τα χαρακτηριστικά που εξάγονται χρησιμοποιούνται αργότερα από το υποσύστημα Artificial intelligence για να γίνει ανίχνευση για το αν ένα μήνυμα είναι κακόβουλο ή όχι. Εκτός από τα χαρακτηριστικά, σε αυτό το υποσύστημα δημιουργούνται κανόνες με βάση τους οποίους ανιχνεύονται κακόβουλα στοιχεία που περιέχονται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

• Το υποσύστημα data analytics αφορά τις λειτουργίες που πρέπει να γίνουν προτού προχωρήσει το σύστημα στην ανίχνευση. Πιο συγκεκριμένα, τα χαρακτηριστικά που εξάγονται από το υποσύστημα behavior analysis, επεξεργάζονται ώστε να είναι σε μια μορφή που να μπορούν να χρησιμοποιηθούν από το υποσύστημα artificial intelligence. Επιπλέον, πραγματοποιείται επιλογή των χαρακτηριστικών που έχουν μεγαλύτερη αξία ως προς την ανίχνευση. Σε αυτά το υποσύστημα πραγματοποιείται και η οπτικοποίηση των δεδομένων, η οποία παίζει πολύ σημαντικό ρόλο καθώς ο διαχειριστής μπορεί να πραγματοποιήσει ταχύτερα κάποιες λειτουργίες αναφορικά με την εξαγωγή συμπερασμάτων για τις επιθέσεις ηλεκτρονικού «ψαρέματος» που έχουν πραγματοποιηθεί, και για τη δημιουργία και διαχείριση των σεναρίων εκπαίδευσης που θα αποστέλλονται στους χρήστες.

• Το υποσύστημα artificial intelligence περιέχει τους αλγόριθμους μηχανικής μάθησης που χρησιμοποιούν τα χαρακτηριστικά που εξήχθησαν από το υποσύστημα Behavior analysis για να ανιχνεύσει τα μηνύματα ηλεκτρονικού ταχυδρομείου που σχετίζονται με τις επιθέσεις ηλεκτρονικού «ψαρέματος». Η διαδικασία της ανίχνευσης χωρίζεται σε δύο στάδια: το στάδιο της εκπαίδευσης και το στάδιο της ανίχνευσης καινούριων επιθέσεων. Το πρώτο στάδιο αφορά την εκπαίδευση των αλγορίθμων ώστε να δημιουργηθούν τα μοντέλα που θα μπορούν να διαχωρίσουν τα νόμιμα μηνύματα ηλεκτρονικής αλληλογραφίας από τα μηνύματα που σχετίζονται με τις επιθέσεις ηλεκτρονικού «ψαρέματος». Το δεύτερο στάδιο αφορά τη χρήση των μοντέλων σε κάθε καινούριο μήνυμα που φτάνει στο ηλεκτρονικό ταχυδρομείο ενός χρήστη.

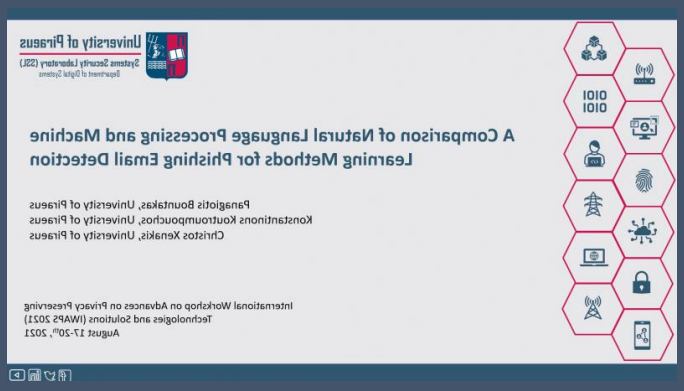
• Η υλοποίηση των παραπάνω υποσυστημάτων γίνεται με τη βοήθεια τριών δομικών στοιχείων (πράκτορας, NetPHISH server, NetPHISH cloud) που πραγματοποιούν τις λειτουργίες με στόχο την ανίχνευση επιθέσεων και την εκπαίδευση των χρηστών και δημιουργούν διαύλους επικοινωνίας για την ανταλλαγή των πληροφοριών ώστε να υλοποιηθούν οι λειτουργίες των υποσυστημάτων. Για την επικοινωνία των δομικών στοιχείων χρησιμοποιούνται πρωτόκολλα κρυπτογράφησης που καθιστούν τις δικτυακές επικοινωνίες ασφαλείς (π.χ. SSL).

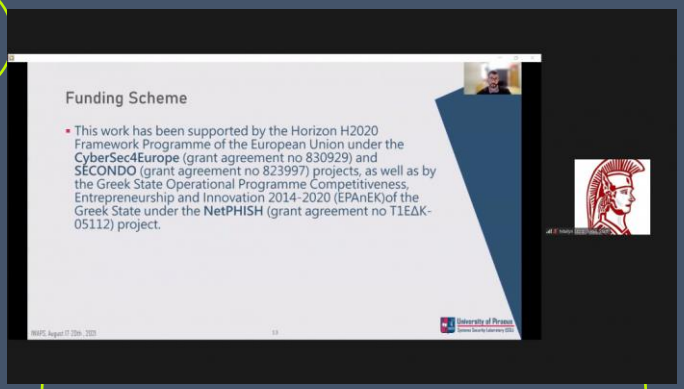
ΔΗΜΟΣΙΕΥΣΗ ΣΤΑ ΠΛΑΙΣΙΑ ΤΟΥ ΕΡΓΟΥ NETPHISH

Το Πανεπιστήμιο Πειραιά συμμετείχε στο συνέδριο 16th International Conference on Availability, Reliability, and Security (ARES 2021). Πιο συγκεκριμένα, ο υποψήφιος διδάκτορας Παναγιώτης Μπουντάκας, που συμμετέχει στην επιστημονική ομάδα του NetPHISH, μαζί με τους συνεργάτες του από το Πανεπιστήμο Πειραιά,

Καθηγητή Χρήστο Ξενάκη και Κώνσταντίνο Κουτρουμπούχο παρουσίασαν τη δημοσίευση “A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection” στο International Workshop on Advances on Privacy-Preserving Technologies and Solutions (IWAPS 2021). Στην δημοσίευση προτείνετε μια προσέγγιση που συνδυάζει τους κλάδους της επεξεργασίας φυσικής γλώσσας (Natural Language Processing) και της μηχανικής μάθησης (Machine Learning) για την ανίχνευση μηνυμάτων ηλεκτρονικού ταχυδρομείου που χρησιμοποιούνται για επιθέσεις ψαρέματος (phishing).

Ο σκοπός του συνεδρίου ήταν να παρουσιαστούν καινοτόμες ιδέες και τεχνολογίες καθώς και να συζητηθούν οι τελευταίες εξελίξεις στον κλάδο της ασφάλειας και ιδιωτικότητας συστημάτων και δικτύων.





ΣΥΜΜΕΤΟΧΗ ΤΟΥ ΕΠΙΣΤΗΜΟΝΙΚΟΥ ΥΠΕΥΘΥΝΟΥ ΤΟΥ NETPHISH ΚΑΘΗΓΗΤΗ ΧΡΗΣΤΟΥ ΞΕΝΑΚΗ ΣΤΟ CEO INITIATIVE 2021

Ο καθηγητής του Τμήματος Ψηφιακών Συστημάτων, του Πανεπιστημίου Πειραιώς και επιστημονικός υπεύθυνος του έργου NetPHISH ο κ. Χρήστος Ξενάκης, συμμετείχε στο CEO INITIATIVE 2021 στο πάνελ συζήτησης “THE NEXT CRISIS CEOs NEED TO THINK” μαζί με τους Γιώργος Δρυμιώτης, Διευθύνων Σύμβουλος, Cardlink και Γιώργος Πατσής, Ιδρυτής & Διευθύνων Σύμβουλος, Obrela Security Industries.

Στόχος της συζήτησης ήταν ο τρόπος πρόληψης και αντιμετώπισης των κυβερνοεπιθέσεων καθώς και η ανάδειξη νέων τεχνικών που έχει επιφέρει η εξέλιξη της τεχνολογίας. Στη συνέχεια τόνισε ότι πλέον οι νέες τεχνολογίες λειτουργούν ως εργαλεία από τους χάκερς ώστε να κάνουν πιο εκλεπτυσμένες μεθόδους επίθεσης.

Ο καθηγητής στη συζήτηση επισήμανε τους κινδύνους που κρύβει ο κυβερνοχώρος καθώς καθημερινά αρκετές εταιρίες, οργανισμοί αλλά και χρήστες γίνονται θύματα κυβερνοεπιθέσεων. Ένα από τα πιο συχνά είδη, είναι αυτό του phishing το οποίο μετρά καθημερινά χιλιάδες θύματα. Ως αποτέλεσμα αυτού είναι η διακύβευση της ασφάλεια όχι μόνο των ίδιων των χρηστών αλλά και των οργανισμών ή εταιρειών στις οποίες ανήκουν. Στη συνέχεια της ομιλίας, ο καθηγητής εκτός από τους κινδύνους στο διαδίκτυο αναφέρθηκε και στους τρόπους αντιμετώπισής τους, με τη χρήση τεχνικών μηχανικής μάθησης.

ΕΠΙΚΟΙΝΩΝΙΑ

Neurosoft S.A.

ΟΔΟΣ – ΑΡΙΘΜΟΣ: Λεωφ. Ηρακλείου 466 & Κύπρου
Τ.Κ. 141 22
ΠΟΛΗ: Αθήνα
ΤΗΛ: 210 6855061

Πανεπιστήμιο Πειραιώς

ΟΔΟΣ – ΑΡΙΘΜΟΣ: Γρηγορίου Λαμπράκη 122
Τ.Κ. 185 32
ΠΟΛΗ: Πειραιάς
ΤΗΛ: 210 4142613

LinkedIn

Website