26 Ιανουαρίου 2018

Έγκλημα στον κυβερνοχώρο: καταπολεμούμε τα προβλήματα του 21ου αι. με εργαλεία του 19ου αι. (Δρ. Πέτρος Παναγιωτόπουλος, Συντονιστής Περιεχομένου Ενότητας Επιστημών – Πεμπτουσία)

/ Πεμπτουσία

Η πρόκληση για το έγκλημα στον κυβερνοχώρο: «Η καταπολέμηση των προβλημάτων του 21ου αιώνα γίνεται με εργαλεία του 19ου αιώνα»

Τι συμβαίνει στο διαδίκτυο; Πόσο ασφαλές είναι το σερφάρισμα; Πόσο επικίνδυνο είναι να είμαστε εκτεθειμένοι στους επιτήδειους; Υπάρχει επαρκής νομοθεσία για να αντιμετωπίσει τις κακόβουλες επιθέσεις εναντίον απλών και ανυποψίαστων πολιτών ή ακόμη και επιχειρήσεων από τους «χάκερς»; Υπάρχουν επαρκή τεχνικά μέσα για να αντιμετωπιστεί η διαδικτυακή παρανομία ή αυτή βρίσκεται πάντοτε πιο μπροστά από το νόμο;

Απαντήσεις σε αυτά αλλά και άλλα ερωτήματα δίνει ο εμπειρογνώμονας ασφαλείας Raj Samani, ένας άνθρωπος που στέκεται ανάμεσα στους πολίτες και τις επιθέσεις στον κυβερνοχώρο. Ο κ. Samani είναι αντιπρόεδρος, επικεφαλής τεχνικός διευθυντής της McAfee EMEA και ειδικός σύμβουλος του Ευρωπαϊκού Κέντρου Κυβερνοεγκλήματος.

Καθώς η απειλή των επιθέσεων στον κυβερνοχώρο γίνεται συνεχώς και πιο διαδεδομένη και οι επιθέσεις ολοένα και πιο καταστροφικές, οι επαγγελματίες της κυβερνοασφάλειας έχουν δει το πρόγραμμά τους να φορτώνεται. Στην πρώτη γραμμή αυτής της μάχης βρίσκεται και ο κ. Samani, ο οποίος αναλώνει εαυτόν καθημερινά στην ασφάλεια του διαδικτύου. Ο ίδιος θεωρεί ότι οι επιδόσεις του έχουν καλές και κακές στιγμές.

«Αγαπώ αυτό που κάνω», λέει. «Αλλά η μεγαλύτερη απογοήτευση για μένα είναι ότι οι άνθρωποι βλέπουν όλο αυτό το θέμα ως ένα θέμα πληροφορικής. Η πραγματικότητα είναι πως δεν είναι και ακριβώς έτσι. Πρέπει να καταλάβουν ότι αυτό επηρεάζει την καθημερινότητά τους. Πάρτε την επίθεση «WannaCry» το Μάιο, για παράδειγμα. Αυτό επηρέασε την ικανότητα των ανθρώπων να λαμβάνουν ιατρική περίθαλψη και να κάνουν τις εργασίες τους. Πρέπει να κάνουμε τους ανθρώπους να αναγνωρίσουν ότι αυτή είναι μια σοβαρή πρόκληση».

Σημειωτέον ότι κατά τη «WannaCry» δεσμεύτηκαν αρχεία από το σύστημα Windows και για να μπορούσαν οι χρήστες να αποκτήσουν ξανά πρόσβαση σ' αυτά θα έπρεπε να καταβάλουν ποσά μεταξύ 300-600 δολαρίων. «Θύμα» της επίθεσης είχε πέσει και το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

Στον αγώνα εναντίον αυτού που ο ίδιος περιγράφει ως «εξέλιξη του εγκλήματος», η κυβερνοασφάλεια και οι νομικοί αντιμετωπίζουν μερικές τεράστιες προκλήσεις. Οι κυριότερες από αυτές αφορούν την αναντιστοιχία της τεχνικής ισχύος των δύο πλευρών. «Στην πραγματικότητα προσπαθούμε να καταπολεμήσουμε ένα πρόβλημα του 21ου αιώνα με εργαλεία του 19ου αιώνα», σημειώνει. «Αν κάποιος θέλει να ξεκινήσει μια επίθεση στο Ηνωμένο Βασίλειο, μπορεί να το κάνει ώστε να φανεί ότι η επίθεση αυτή προέρχεται από οπουδήποτε στον κόσμο. Υπάρχουν βέβαια διεθνείς δικαιοδοσίες για την αντιμετώπιση του φαινομένου. Πώς μπορούν όμως οι δυνάμεις του νόμου να ασχοληθούν με το πρόβλημα μιας χώρας, ειδικά αν δεν έχουν εργασιακή σχέση με αυτή τη χώρα;».

Φυσικά, ο στόχος είναι πάντα ο περιορισμός των δυνατοτήτων της κυβερνοπαρανομίας, η τιμωρία των δραστών και τελικά να μπουν αυτοί πίσω από τα κάγκελα. Σε αυτό δεν έχουν επιτευχθεί και λίγα πράγματα: άτομα όπως ο Ρος Ούλμπριχτ, για παράδειγμα – που ήταν πίσω από τη διαδικτυακή μαύρη αγορά «Δρόμος του Μεταξιού» – και πολλοί άλλοι έχουν συλληφθεί. Ωστόσο, ο Samani επιμένει ότι υπάρχουν και άλλοι αποτελεσματικοί τρόποι αντιμετώπισης της πρόκλησης αυτής.

Εδώ είναι απαραίτητο να θυμίσουμε, ότι ο «Δρόμος του Μεταξιού» ήταν ένα «ηλεκτρονικό πολυκατάστημα», μια ιστοσελίδα του λεγόμενου «σκοτεινού» ή «βαθέος» διαδικτυακού ιστού, που εμπορευόταν ναρκωτικά (ενδεχομένως και άλλο παράνομο υλικό). Ξεκίνησε το 2010-2011, έκλεισε το 2013, ξανάνοιξε με άλλη μορφή την ίδια χρονιά και ξανάκλεισε οριστικά την επόμενη.

«Δείτε το έργο που κάναμε με άλλους οργανισμούς επιβολής του νόμου και ασφάλειας για να αναπτύξουμε το πρόγραμμα No More Ransom», λέει. «Όχι μόνο βοήθησε να εκπαιδεύσει το κοινό για τα ransomware, αλλά προσφέρει επίσης εργαλεία αποκρυπτογράφησης για να επιτρέψει στους ανθρώπους να ανακτούν αρχεία που έχουν κλειδωθεί από ransomware. Αυτό για μένα είναι απίστευτα θετικό».

Να διευκρινιστεί εδώ ότι το ransomware (ransom σημαίνει λύτρα) είναι επίθεση με κακόβουλο λογισμικό, στην οποία ζητείται από το «θύμα» να καταβάλει κάποια χρήματα σε ένα λογαριασμό, αν δεν θέλει να δημοσιοποιηθεί π.χ. ότι επισκέφθηκε

ανάρμοστο διαδικτυακό περιεχόμενο (λ.χ. σελίδες με πορνογραφικό υλικό).

Πιστεύει ότι η ψηφιακή ασφάλεια αποτελεί βασικό παράγοντα διαφοροποίησης και αξιολόγησης για τις επιχειρήσεις. Όσο μεγαλύτερη έμφαση δοθεί στο ζήτημα της ηλεκτρονικής ασφάλειας από μία επιχείρηση, τόσο καλύτερα αποτελέσματα θα έχει.

[Συνεχίζεται]