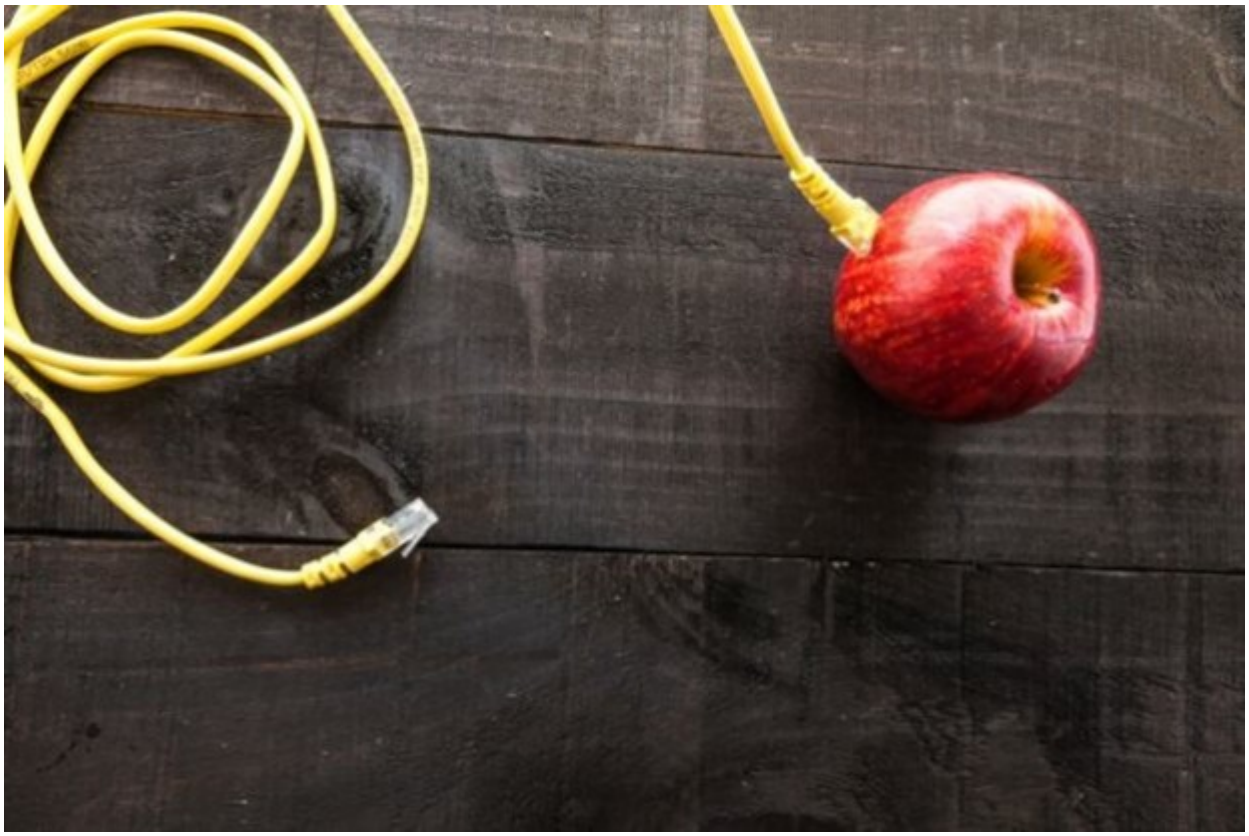
11 Απριλίου 2016

Δικτύωση: Από τι να φυλαγόμαστε;

/ Επιστήμες, Τέχνες & Πολιτισμός

Image not found or type unknown



Κάμερες, οικιακές συσκευές, κινητά και ταμπλέτες, όλα είναι πια δικτυωμένα. Χαρούμενοι με όλα τα καλούδια, ξεχνάμε συνήθως τους κινδύνους. Πώς θα προστατευθούμε;

Πριν από λίγες ημέρες διάβασα ένα πολύ ενδιαφέρον άρθρο. Εφερε την υπογραφή του βρετανού συναδέλφου **Μαρκ Γουόρντ** από το BBC, ο οποίος διερωτώμενος για το πόσο εύκολο είναι να χακάρει κανείς την κάμερα του σπιτιού του αποφάσισε να κάνει ένα πείραμα. Κάλεσε δύο χάκερ να σπάσουν το σύστημα της κάμερας για να δει πώς μπορεί κάποιος επιτιθέμενος να αποκτήσει πρόσβαση στο νοικοκυριό του. Ενας εκ των δύο ήταν ο Ελληνας **Κυπριανός Βασιλόπουλος**, σύμβουλος ασφαλείας πληροφοριακών συστημάτων.
Εμείς εντοπίσαμε τον Ελληνα ειδικό, ο οποίος μας εξήγησε τι ακριβώς συνέβη στο Λονδίνο. «*Ο δημοσιογράφος του BBC μας κάλεσε στο σπίτι του και μας ζήτησε να δείξουμε αν είναι ασφαλές ένα οικιακό δίκτυο με κάποιες συνδεδεμένες συσκευές, όπως π.χ. η κάμερα. Αυτό που δείξαμε είναι ότι και μέσω ενός απλού email, της κάμερας και του οικιακού ρούτερ καταφέραμε να αποκτήσουμε πρόσβαση στο δίκτυό του*

» εξηγεί στο «Βήμα» ο κ. Βασιλόπουλος.

Ψηφιακοί εισβολείς στο σπίτι μας

Με μια πληθώρα έξυπνων και δικτυωμένων συσκευών να μας περιβάλλει και νέες προτάσεις να κάνουν διαρκώς την εμφάνισή τους για ένα ενοποιημένο δίκτυο που θα μπορούμε να ελέγχουμε από παντού, οι απειλές είναι ξεκάθαρες και οι επιτήδειοι αμέτρητοι. «*Πλέον δεν είναι και τόσο δύσκολο να «μπει» κανείς στο δίκτυο κάποιου. Οσο περισσότερες είναι οι συσκευές που συνδέονται στο Διαδίκτυο (κάμερες, ρούτερ, γκάτζετ κ.ά.) τόσο μεγαλύτερο είναι και το ρίσκο μιας υποτιθέμενης επίθεσης. Στο σπίτι είναι λίγο ανώνυμη η κατάσταση, συγκριτικά με μια στοχευμένη επίθεση σε μια εταιρεία. Δεν ξέρεις δηλαδή σε ποιον ανήκει η διεύθυνση IP (Internet Protocol Address) – εκεί στοχεύει κανείς στα τυφλά, όμως αν αποκτήσει πρόσβαση σε κάποιες συσκευές, τότε μπορεί να τις αξιοποιήσει για δικούς του λόγους*».
Οπως μας ενημερώνει ο κ. Βασιλόπουλος, δεν χρειάζεται κανείς να διαθέτει σπουδές στην Πληροφορική για να καταφέρει να χακάρει ένα σύστημα. « *Υπάρχουν «τρύπες» που είναι πολύ εύκολο να τις βρει κάποιος, και άλλες που απαιτούν πιο εξειδικευμένες γνώσεις. Η ευπάθεια που βρήκαμε π.χ. στην κάμερα του BBC δεν απαιτούσε ιδιαίτερες γνώσεις πληροφορικής. Αρκούσε κανείς να γνωρίζει κάποια βασικά πράγματα, να ασχολείται στον ελεύθερο χρόνο του, να διαβάζει, να ενημερώνεται, για να μπορέσει να αξιοποιήσει τη συγκεκριμένη αδυναμία του συστήματος. Στη συνέχεια μαζί με τον δημοσιογράφο βρήκαμε την αντίστοιχη ιστοσελίδα όπου εμφανίζονταν 1,5 εκατομμύριο κάμερες σε όλο τον κόσμο με το ίδιο λειτουργικό σύστημα. Το μέγεθος, όπως καταλαβαίνετε, είναι τεράστιο».*

Προσοχή στις κάμερες

Το πρόβλημα, σύμφωνα με τον ειδικό ασφαλείας, ξεκινάει από τους ίδιους τους χρήστες οι οποίοι τις περισσότερες φορές εμφανίζονται μάλλον αφελείς απέναντι στους πιθανούς κινδύνους. «*Οι περισσότεροι γονείς, ειδικά στην Ελλάδα, και το λέω εμπειρικά, δεν είναι και πολύ της τεχνολογίας. Οπότε βάζουν μια κάμερα, τη συνδέουν στο δίκτυο του σπιτιού τους έτσι ώστε και όταν πάνε στη δουλειά να μπορούν να παρακολουθούν κάποια πράγματα. Είτε αφήνουν τον προεπιλεγμένο κωδικό της εταιρείας στην κάμερα, είτε τον αλλάζουν. Ομως συμβαίνει το εξής: οι περισσότεροι κατασκευαστές που φτιάχνουν τις κάμερες, λίγο-πολύ έχουν το ίδιο λειτουργικό σύστημα. Αυτό το σύστημα δεν είναι τόσο καλά προστατευμένο ώστε να παρέχει στους χρήστες υψηλή ασφάλεια. Οι επιτήδειοι λοιπόν παίρνουν μια τέτοια κάμερα στο σπίτι τους, μελετούν το λειτουργικό σύστημα που τρέχει από κάτω, βρίσκουν ευπάθειες, στη συνέχεια εντοπίζουν τις ιστοσελίδες στις οποίες αναφέρονται οι συσκευές που είναι συνδεδεμένες στο Διαδίκτυο σε παγκόσμιο επίπεδο και ξεκινούν να χτυπούν τις κάμερες ανά χώρα ή μία-μία, παρακάμπτοντας*

τη διαδικασία ασφαλείας τους, με αποτέλεσμα να αποκτούν πρόσβαση σε αυτές».
Σε περίπτωση που θέλουμε να αγοράσουμε μια κάμερα, σύμφωνα με τον κ. Βασιλόπουλο, καλό είναι να καταφεύγουμε σε γνωστές εταιρείες και όχι σε φθηνές λύσεις από άγνωστους κατασκευαστές. «*Κατά την ενεργοποίηση της κάμερας το λεγόμενο firmware που τη συνοδεύει θα πρέπει να αναβαθμιστεί αμέσως στην τελευταία έκδοση (αν υπάρχει). Επίσης όταν βγάζουμε μια συσκευή στο Διαδίκτυο, αν θέλουμε να τη βλέπουμε από smartphone ή από τον υπολογιστή του γραφείου μας, τότε καλό είναι να την περιορίσουμε. Δηλαδή, θα πρέπει να ενεργοποιήσουμε το λεγόμενο VPN (Virtual Private Network) που έχει ο ρούτερ του σπιτιού και από τη συσκευή να συνδεόμαστε μέσω VPN στον ρούτερ και η κάμερα που βρίσκεται πίσω από τη σύνδεση αυτή να επιλέγεται τοπικά στο δίκτυο ούτως ώστε να μην είναι ορατή διαδικτυακά. Η σύνδεση VPN είναι κρυπτογραφημένη οπότε ό,τι σύνδεση γίνεται εκεί δεν μπορεί να σπάσει από κάποιον άλλον που θα ήθελε να αποκτήσει πρόσβαση στα δεδομένα αυτά. Ως χρήστες καλό είναι να μη βγάζουμε οικιακές συσκευές στο Διαδίκτυο τις οποίες είτε δεν πολυγνωρίζουμε, είτε δεν εμπιστευόμαστε. Προσωπικά, τις κάμερες τις προσέχω πάρα πολύ*».

Ο ταχυδρόμος «χτυπά» συσκευές

Σε ένα νοικοκυριό μπορεί κανείς να συναντήσει μια smart TV, ένα λάπτοπ, ένα tablet και ένα smartphone. Οι απειλές άραγε για την καθεμιά από τις παραπάνω συσκευές είναι ίδιες; «*Η περίπτωση της smart TV είναι πιο περίπλοκη και απαιτεί συγκεκριμένη τεχνική, είναι πιο δύσκολο να γίνει κάτι τέτοιο. Στις υπόλοιπες συσκευές (λάπτοπ, κινητό, tablet), αν θέλω να αποκτήσω πρόσβαση μπορώ, για παράδειγμα, να σας στείλω ένα email το οποίο δεν θα ενεργοποιήσει κανένα απολύτως μέτρο ασφαλείας, όπως π.χ. το antivirus. Θα μοιάζει με αληθοφανές επισυναπτόμενο αρχείο (ένας λογαριασμός τηλεφώνου, ενημέρωση από την εφορία κ.ά.), ο παραλήπτης θα το ανοίξει και από όποια συσκευή γίνει αυτό θα γυρίσει σε εμένα μια σύνδεση. Ετσι, θα έχω πλήρη πρόσβαση στη συσκευή σας*».
Σύμφωνα με τον ειδικό, η προστασία που προσφέρουν τα υπάρχοντα συστήματα antivirus δεν αγγίζει ούτε το 70% και αυτό γιατί ο επιτιθέμενος γνωρίζει τα μέτρα που μπορεί να λάβει κάποιος. Κατεβάζει λοιπόν στον υπολογιστή του το οποιοδήποτε antivirus, ελέγχει το σύστημα για ευπάθειες και αλλάζει διαρκώς το αρχείο-«παγίδα» μέχρις ότου καταφέρει να κοροϊδέψει το antivirus. «*Σε παγκόσμια κλίμακα, όλες οι εταιρείες που ασχολούνται με την ασφάλεια κάνουν ακριβώς αυτό: προσπαθούν να στείλουν ένα τέτοιο αρχείο για να κοροϊδέψουν το antivirus*».
«*Η αλήθεια είναι ότι ο πόλεμος μεταξύ των εταιρειών ασφαλείας, που βγάζουν τα antivirus και των επιτιθεμένων δεν γίνεται επί ίσοις όροις γιατί πάντα ο επιτιθέμενος βρίσκεται ένα βήμα πιο μπροστά. Σαν επιτιθέμενος, έχω το πλεονέκτημα μέσω του κακόβουλου αρχείου που φτιάχνω να κάνω ό,τι χρειάζεται για να παρακάμψω την ασφάλεια*» μας λέει ο ειδικός. «*Αν είμαστε υποψιασμένοι όμως, π.χ. αν λάβουμε ένα τέτοιο αρχείο ενώ δεν το περιμένουμε, αν δούμε κάτι που δεν έχουμε ξαναδεί, απλά δεν το ανοίγουμε*»

.

Οταν οι εφαρμογές τρυπώνουν στην κάμερα

Δεν είναι λίγες όμως και οι εφαρμογές που κατά την εγκατάσταση ή την αναβάθμισή τους μας ζητούν να αποδεχτούμε πρόσβαση στην κάμερα και στο μικρόφωνο της συσκευής μας. «*Αυτό έχει να κάνει καθαρά με τον τύπο της εφαρμογής. Από τη στιγμή όμως που ο χρήστης αποδέχεται την πρόσβαση στο μικρόφωνο ή στην κάμερα του κινητού του, αυτός που έχει φτιάξει την εφαρμογή ενδεχομένως να τη χρησιμοποιήσει π.χ. για να βγάλει κάποια φωτογραφία, να ακούσει κάποια συνομιλία, οτιδήποτε. Επίσης όταν σας καλούν από εταιρείες ενώ δεν έχετε δώσει τα προσωπικά σας στοιχεία, το κινητό σας, το email σας, αυτό συμβαίνει – μεταξύ άλλων – και από εφαρμογές ή εταιρείες delivery οι οποίες παραχωρούν τα προσωπικά δεδομένα των χρηστών ή των πελατών τους έναντι κάποιου χρηματικού ποσού*» μας λέει ο κ. Βασιλόπουλος.

Ενας «έξυπνος» κόσμος στην παλάμη μας

Σε ένα οικοσύστημα δικτυωμένων συσκευών που θα επικοινωνούν μεταξύ τους βασίζεται τ

Image not found or type unknown

Σε ένα οικοσύστημα δικτυωμένων συσκευών που θα επικοινωνούν μεταξύ τους βασίζεται το Internet των Πραγμάτων (IoT), με την ασφάλεια, κατά τους ειδικούς, να αποτελεί πυρήνα της επιτυχίας του

Με το Internet των Πραγμάτων (Internet of Things – IoT), οι συσκευές αποκτούν νοημοσύνη, συνδέονται μεταξύ τους, δημιουργούν ένα πολύ μεγάλο δίκτυο το οποίο ξεφεύγει από τα όρια του σπιτιού, προσφέροντας στους χρήστες πρόσβαση και έλεγχο από οπουδήποτε. Τι θα μπορούσε να κρύβει όμως μια ασφυκτικά δικτυωμένη καθημερινότητα και τι θα μπορούσαμε να συναντήσουμε τα επόμενα χρόνια; «*Δεν αποκλείεται να έρθουμε αντιμέτωποι με μια απειλή που δεν έχουμε γνωρίσει ως τώρα. Το θεωρώ σίγουρο γιατί η τεχνολογία εξελίσσεται πάρα πολύ γρήγορα, με αποτέλεσμα ακόμη και μεγάλοι παίκτες του χώρου να μην μπορούν να τις ακολουθήσουν. Αρα ένας απλός χρήστης είναι απλά αδύνατο να ακολουθήσει τους ιλιγγιώδεις αυτούς ρυθμούς. Το σημαντικότερο όλων είναι η ενημέρωση και η ασφάλεια. Οταν π.χ. έχουμε τη δημιουργία των έξυπνων νοικοκυριών και δεν έχουμε ασφάλεια, δεν έχουμε τίποτε – ο χρήστης αργά ή γρήγορα θα έρθει*

αντιμέτωπος με κάποια απειλή. Είμαι της άποψης ότι όλα πρέπει να γίνονται στην ώρα τους. Το ότι βγήκε τώρα μια έξυπνη ηλεκτρονική κλειδαριά για το σπίτι ή ένα σύστημα για να ξεκλειδώνουμε το αυτοκίνητό μας μέσω του smartphone δεν σημαίνει ότι πρέπει όλοι να το βάλουμε. Ας δώσουμε λίγο χρόνο, να δούμε τι ακριβώς είναι. Δεν χρειάζεται να υιοθετούμε ό,τι νέο κυκλοφορεί, πόσω μάλλον όταν δεν είμαστε και ιδιαίτερα εξοικειωμένοι με αυτό» καταλήγει ο κ. Βασιλόπουλος.

Ονειρα γλυκά, σε βλέπω

Τον περασμένο Ιούλιο, μια οικογένεια από το Οντάριο στον Καναδά ήρθε αντιμέτωπη με το

Image not found or type unknown

Τον περασμένο Ιούλιο, μια οικογένεια από το Οντάριο στον Καναδά ήρθε αντιμέτωπη με τον ψηφιακό εισβολέα στην κάμερα του μωρού τους όταν αυτή άρχισε να παίζει παράξενη μουσική

Τον τελευταίο χρόνο οι καταγγελίες γονιών σχετικά με την κατάληψη από

αγνώστους των συστημάτων βρεφικής παρακολούθησης (κάμερα, μόνιτορ) που είχαν εγκαταστήσει στο σπίτι τους για να βλέπουν εξ αποστάσεως τα παιδιά τους, έχουν εκτοξευθεί στα ύψη. Χαρακτηριστικά, τον περασμένο Ιούλιο, μια οικογένεια από το Οντάριο στον Καναδά ήρθε αντιμέτωπη με τον ψηφιακό εισβολέα όταν η κάμερα του μωρού τους άρχισε να παίζει παράξενη μουσική. Σε άλλη περίπτωση, όπως είχε αποκαλύψει στο αμερικανικό ειδησεογραφικό δίκτυο CBS ένα ζευγάρι από τη Νέα Υόρκη, το τρίχρονο παιδάκι τους τούς έλεγε διαρκώς ότι φοβάται τον κύριο της κάμερας. Αρχικά οι γονείς θεώρησαν ότι όλα ήταν στη φαντασία του μικρού ώσπου τον περασμένο Απρίλιο οι γονείς έντρομοι άκουσαν μια ανδρική φωνή να λέει: *«Ξύπνα, αγοράκι, σε ψάχνει ο μπαμπάς».* Και μια γυναίκα από το Κάνσας όμως κατάλαβε ότι παρακολουθούνταν μέσα στο ίδιο της το σπίτι όταν, ενώ έβαζε το παιδί της για ύπνο, η κάμερα άρχισε να κινείται ακολουθώντας την στον χώρο.

«Οπως και με κάθε άλλη ψηφιακή συσκευή οικιακής χρήσης, υπάρχει πιθανός κίνδυνος εισβολής αν η συσκευή αυτή δεν είναι ασφαλής» μας εξηγεί ο κ. **Ντέιβιντ Εμ**, κύριος ερευνητής ασφαλείας της ρωσικής εταιρείας συστημάτων ασφαλείας Kaspersky Lab*. «Η πιο ανησυχητική πτυχή αυτού είναι ο κίνδυνος που ελλοχεύει για τα πιο ευάλωτα μέλη της κάθε οικογένειας. Δηλαδή, το γεγονός ότι οι άνθρωποι αυτοί μπορούν να αλληλεπιδράσουν με ένα μικρό παιδί. Εναλλακτικά θα μπορούσαν να χρησιμοποιήσουν την κάμερα για να κατασκοπεύσουν τους κατόχους της – να ακούσουν συνομιλίες, να παρακολουθούν ποιος μπαίνει και ποιος βγαίνει από το δωμάτιο όπου χρησιμοποιείται η συσκευή κ.ά. Αν, για παράδειγμα, η κάμερα βρίσκεται συνδεδεμένη στο οικιακό δίκτυο μέσω Wi-Fi και οι πληροφορίες του λογαριασμού δεν είναι ασφαλείς, θα μπορούσε να επιτρέψει σε έναν εισβολέα να αποκτήσει πρόσβαση σε άλλες συσκευές στο σπίτι ή σε δεδομένα που μεταδίδονται μέσω του δικτύου».*

Ο ειδικός προτείνει στους γονείς που αναζητούν μια συσκευή βρεφικής παρακολούθησης να επιλέξουν ένα μοντέλο που δεν συνδέεται στο Διαδίκτυο, σαν αυτά που παραπέμπουν σε Walkie-Talkie. *«Διαφορετικά στην περίπτωση μιας σύγχρονης κάμερας οι γονείς θα πρέπει να απενεργοποιήσουν τη λειτουργία που επιτρέπει την προφορική επικοινωνία με το παιδί προκειμένου να μην μπορεί κάποιος να του μιλήσει μέσα από αυτήν».* Στην ερώτηση τι μπορούμε να κάνουμε ως καταναλωτές για να προστατευθούμε ο ειδικός της Kaspersky Lab αναφέρει ότι υπάρχουν κάποια βασικά βήματα που θα μπορούσαν να ενισχύσουν την προστασία μας. *«Αρχικά βεβαιωθείτε ότι έχετε αλλάξει τον προεπιλεγμένο κωδικό πρόσβασης για να εμποδίσετε κάποιον να αποκτήσει πρόσβαση στη συσκευή. Στη συνέχεια βεβαιωθείτε ότι έχετε εγκαταστήσει τις διαθέσιμες τελευταίες ενημερώσεις του λογισμικού που είναι εγκατεστημένο στη συσκευή. Τέλος, αλλάξτε τον προεπιλεγμένο κωδικό πρόσβασης στον ρούτερ και εγκαταστήστε και εκεί τις τελευταίες ενημερώσεις».*

«Βρισκόμαστε στα πρόθυρα ενός κόσμου όπου τα πάντα είναι συνδεδεμένα – όχι μόνο οι παραδοσιακοί υπολογιστές αλλά και αντικείμενα καθημερινής χρήσης, ακόμη και οι ίδιοι οι άνθρωποι. Η τάση αυτή είναι πολλά υποσχόμενη καθώς προσφέρει την ευκαιρία για ένα λαμπρό μέλλον που φέρνει μαζί του μια καλύτερη ποιότητα ζωής. Ωστόσο, αν τα αντικείμενα καθημερινής χρήσης (CCTV κάμερες, οικιακές συσκευές, wearables και εμφυτεύματα) δεν είναι ασφαλή, τότε υπάρχει διττός κίνδυνος. Κατ' αρχάς, τα προσωπικά μας δεδομένα μπορεί να υποκλαπούν από έναν εισβολέα. Δεύτερον, η συσκευή θα μπορούσε να χρησιμοποιηθεί ως όχημα για την πρόσβαση στο οικιακό μας δίκτυο. Είναι ζωτικής σημασίας ως εκ τούτου οι κατασκευαστές τέτοιων συσκευών να σκέφτονται την ασφάλεια ήδη από το στάδιο του σχεδιασμού τους. Είναι επίσης ζωτικής σημασίας οι καταναλωτές να κατανοήσουν τους δυνητικούς κινδύνους που εγκυμονούν οι επισφαλείς συσκευές IoT και να λαμβάνουν τα μέτρα που μπορούν ώστε να μειώσουν την έκθεσή τους σε πιθανές επιθέσεις» επισημαίνει ο κ. Εμ.

Επιθέσεις και σε αυτοκίνητα;

Την περασμένη εβδομάδα το FBI και η Εθνική Υπηρεσία Ασφάλειας Αυτοκινητοδρόμων των ΗΠΑ προειδοποίησε ότι τα αυτοκίνητα «γίνονται όλο και πιο ευάλωτα» σε επιθέσεις από χάκερ. «Δεν οδηγούν απαραίτητα όλα τα περιστατικά χάκινγκ σε κίνδυνο ασφάλειας – δίνοντας δηλαδή τον έλεγχο του οχήματος στον επιτιθέμενο -, είναι σημαντικό όμως για τους καταναλωτές να λάβουν μέτρα ώστε να ελαχιστοποιήσουν τον κίνδυνο» ανέφεραν μεταξύ άλλων οι δύο υπηρεσίες στην επίσημη ανακοίνωσή τους. Σύμφωνα με το Reuters, τον περασμένο Ιούλιο η Fiat Chrysler προχώρησε στην ανάκληση 1,4 εκατ. Jeep

Cherokee στις ΗΠΑ για ενημέρωση λογισμικού. Η ανάκληση της αυτοκινητοβιομηχανίας ανακοινώθηκε κατόπιν αποκάλυψης του περιοδικού «Wired» ότι χάκερ μπορούσαν να παρέμβουν σε ορισμένα συστήματα του οχήματος, όπως το τιμόνι και τα φρένα. Στις αρχές του 2015 η BMW ανακοίνωσε ότι είχε «μπαλώσει» κενό ασφάλειας μέσα από το οποίο χάκερ μπορούσαν να ανοίξουν τις πόρτες 2,2 εκατομμυρίων αυτοκινήτων. Την ίδια χρονιά, η General Motors είχε διαθέσει ενημέρωση ασφαλείας για ένα app της μέσω του οποίου χάκερ μπορούσαν να καταλάβουν τον έλεγχο ορισμένων λειτουργιών του plugin υβριδικού Chevrolet Volt, όπως το άνοιγμα των θυρών και την εκκίνηση του κινητήρα. Το FBI προειδοποιεί, τέλος, τους οδηγούς να προσέχουν τυχόν παραπλανητικά email για ενημερώσεις λογισμικού τα οποία οδηγούν στην εγκατάσταση κακόβουλου κώδικα και δεν προέρχονται από τις εταιρείες. Ως σήμερα ωστόσο, σύμφωνα με επίσημα στοιχεία της Αμερικανικής Υπηρεσίας Ασφάλειας Αυτοκινητοδρόμων, δεν έχει καταγραφεί περιστατικό κυβερνοεπίθεσης σε οχήματα.

Βενιού Ειρήνη
Πηγή: tovima.gr