Η ΚΑΘΗΜΕΡΙΝΗ

Είδος: Εφημερίδα / Κύρια / Πολιτική / Κυριακάτικη
Ημερομηνία: Κυριακή, 19-03-2023
Σελίδα: 10
Μέγεθος: 1190 cm ²
Μέση κυκλοφορία: 4000
Επικοινωνία εντύπου: +357 22472500

Λέξη κλειδί: ΠΟΛΕΟΔΟΜΙΑ - ΧΩΡΟΤΑΞΙΑ

Πάγωσαν πράξεις 150 εκατ. ευρώ στο κτηματολόγιο

Μιλούν στην «Κ» ο διευθυντής του Κτηματολογίου, ο νυν και ο τέως υφυπουργός Καινοτομίας και ο ειδικός του Cybersecurity

Σε κυβερνοεπιθέσεις που σχετίζονται με «ransomware» τα κίνητρα συνήθως είναι οικονομικά και μπορεί να γίνουν είτε από άτομα που ενεργούν από μόνα τους, είτε από οργανωμένες ομάδες.

Του **ΠΑΝΑΓΙΩΤΗ ΡΟΥΓΚΑΛΑ**

Η Κύπρος έγινε στόχος κυβερνοεπιθέσεων τις τελευταίες ημέρες, με μεγάλο της θύμα την Πύλη Κτηματολογίου. Οι τεχνικοί ακόμα και σήμερα προσπαθούν να αποκαταστήσουν την πλήρη λειτουργία της έπειτα από την κυβερνοεπίθεση που δέχθηκε το βράδυ της 8ης Μαρτίου και που μέχρι σήμερα έχει βάλει στο «περίμενε» πράξεις που εκτιμώνται στα 150 εκατομμύρια ευρώ. Πέραν της πύλης Κτηματολογίου, που είναι «αιμοδότης» για την κυπριακή οικονομία και τον τομέα των ακινήτων γενικότερα, στόχος έγινε επίσης και το Πανεπιστήμιο Κύπρου από «χάκερς». Την «τριπλέτα» των παράλληλων επιθέσεων θα συμπλήρωνε και το υπουργείο Άμυνας, όμως, τα συστήματα ασφαλείας του δεν άφησαν περιθώρια εισχώρησης και μέσα σε 3 - 4 ώρες οι «χάκερς» εγκατέλειψαν την προσπάθεια. Το γενικότερο πρόβλημα φαίνεται να έχει και άλλες προεκτάσεις, που εκτείνονται σε αρκετούς τομείς της οικονομίας. Η «Κ» είναι δέκτης πληροφοριών πως μεγάλοι ιδιωτικοί οργανισμοί στην Κύπρο έχουν μπει το τελευταίο διάστημα στον κατάλογο των θυμάτων από κυβερνοεπιθέσεις. Στις περιπτώσεις κυβερνοεπιθέσεων σε ιδιωτικές εταιρείες, οι «χάκερς» έλαβαν και λύτρα για να αποδεσμεύσουν τις πληροφορίες που είχαν υποκλέψει. Γίνεται λόγος για ποσά τα οποία κυμαίνονταν από 50 – 100 χιλιάδες ευρώ.

Γυρνώντας στα του κτηματολογίου και της κυβερνοεπίθεσης που υπέστη, οι πράξεις με τις οποίες ασχολείται είναι δύο κατηγοριών. Από τη μια οι πωλήσεις και από την άλλη οι υποθήκες που γίνονται για σύναψη δανείων. Σύμφωνα με στοιχεία που παραχώρησε στην «Κ» ο διευθυντής του Κτηματολογίου, Ελίκος Ηλία, το τμήμα διεκπεραιώνει 20.799 πωλήσεις το χρόνο –βάσει των στατιστικών του 2022– και το τίμημα (αξία) ανέρχεται στα 4,18 δισεκατομμύρια ευρώ. Όσον αφορά στις υποθήκες, το 2022 οι αιτήσεις έφτασαν στις 14.489 και αφορούσαν δάνεια ύψους 3,29 δισεκατομμυρίων ευρώ. Σύνολο δηλαδή, στα 7,47 δισεκατομμύρια ευρώ οι πράξεις το 2022. Από εκεί και πέρα, αν υπολογίσουμε πως οι εργάσιμες ημέρες για το κτηματολόγιο είναι 220 ετησίως, τότε προκύπτει πως την κάθε ημέρα γίνονται πράξεις ύψους 34 εκατ. ευρώ σε όλα τα επαρχιακά κτηματολόγια. Όπως δήλωσε ο κ. Ηλία, το κτηματολόγιο Λευκωσίας ήταν κλειστό για 4 ημέρες, της Λεμεσού ήταν για 5 ημέρες, ενώ της Λάρνακας, Αμμόχωστου και Πάφου ήταν για 6 ημέρες. Μόνο δηλαδή για 4 ημέρες, κατά μέσο όρο μπήκε «φρένο» σε πράξεις 136 εκατ. ευρώ, ενώ για τις υπόλοιπες 2 ημέρες για τα κτηματολόγια εκτός της Λευκωσίας, μία εκτίμηση για συν 14 εκατ. ευρώ πράξεων που καθυστέρησαν φαντάζει ρεαλιστική. Έτσι προκύπτουν και τα 150 εκατ. ευρώ καθυστερήσεων στις πράξεις. Σύμφωνα με τον κ. Ηλία, θα υπάρξει πλήρης ανάκαμψη του Τμήματος σε περίπου 10 ημέρες.

Μια κυβερνοεπίθεση έχει κάποια χαρακτηριστικά, όπως οι μέθοδοι και τεχνικές που χρησιμοποιήθηκαν, τα οποία υποδηλώνουν τις προθέσεις του ατόμου ή της ομάδας στην οποία μπορεί να ανήκουν. Υπάρχουν ομάδες που δρουν στο χρηματοπιστωτικό τομέα, ενώ άλλες σε κρίσιμες υποδομές στον ενεργειακό τομέα, και ούτω καθ' εξής. Οι προθέσεις και τα κίνητρα ποικίλουν σύμφωνα με ειδικούς του κλάδου. Σε κυβερνοεπιθέσεις που σχετίζονται με «ransomware», τα κίνητρα συνήθως είναι οικονομικά και μπορεί να γίνουν είτε από άτομα που ενεργούν από μόνα τους, είτε από οργανωμένες ομάδες. Υπάρχουν περιπτώσεις κατά τις οποίες, ενώ φαινομενικά τα κίνητρα είναι οικονομικά, η επίθεση αποσκοπεί στην υποκλοπή ευαίσθητων δεδομένων και πνευματικής ιδιοκτησίας ή στην πρόκληση ανεπανόρθωτης ζημιάς σε συστήματα. Τα τελευταία χρόνια παρουσιάζονται αυξητικές τάσεις σε επιθέσεις από ομάδες που είναι προσκείμενες στο οργανωμένο κυβερνοέγκλημα, οι οποίες μέσω του κέρδους από «ransomware» καθώς και την πώληση ευαίσθητων πληροφοριών στο «dark web», πέραν του οικονομικού οφέλους, χρηματοδοτούν κι άλλες παράνομες δραστηριότητες. Παράλληλα, από το 2021 παρουσιάζεται πιο έντονα το φαινόμενο του «hacker-as-a-service» στο οποίο οι επιτήδειοι ενεργούν επί πληρωμή μέσω κάποιου συμβολαίου. Τέλος, η αβεβαιότητα που προκαλείται από γεωπολιτικά γεγονότα, όπως ο πόλεμος στην Ουκρανία, δημιουργεί ένα περιβάλλον που ευνοεί το κυβερνοέγκλημα το οποίο εκμεταλλευόμενο τις ελλείψεις σε τρόφιμα και στην ενέργεια, επιχειρεί σε πραγματικό χρόνο να προκαλέσει εκτεταμένη αστάθεια στην αλυσίδα εφοδιασμού.

Ο νέος υφυπουργός Καινοτομίας, Έρευνας και Ψηφιακής Πολιτικής, Φίλιππος Χατζηζαχαρίας.

Από το 2021 παρουσιάζεται πιο έντονα το φαινόμενο του «hacker-as-a-service» όπου οι επιτήδειοι ενεργούν επί πληρωμή μέσω κάποιου συμβολαίου.

Ο ειδικός της κυβερνοασφάλειας, Associate Director, CEE&EM Security & Resilience services Partner, Kyndryl Κύπρου, Χρίστος Γιακουμής.

Στις περιπτώσεις κυβερνοεπιθέσεων σε ιδιωτικές εταιρείες, οι «χάκερς» έλαβαν και λύτρα για να αποδεσμεύσουν τις πληροφορίες που είχαν υποκλέψει. Γίνεται λόγος για ποσά από 50 - 100 χιλιάδες ευρώ.

Δεν δώσαμε λύτρα

Ο νέος υφυπουργός Καινοτομίας, Έρευνας και Ψηφιακής Πολιτικής, Φίλιππος Χατζηζαχαρίας, κληθείς να σχολιάσει το φαινόμενο των κυβερνοεπιθέσεων και συγκεκριμένα αν έχει γίνει η Κύπρος στόχος των χάκερς, σημείωσε πως «δεν είναι φαινόμενο που απασχολεί μόνο την Κύπρο και υπάρχουν αρκετά, πρόσφατα παραδείγματα σε παγκόσμιο επίπεδο, ακόμη και σε χώρες που χρησιμοποιούν συστήματα υψίστης ασφαλείας. Το πρόβλημα των κυβερνοεπιθέσεων και ευρύτερα των επιθέσεων από χάκερς σε διάφορους οργανισμούς είναι ζήτημα διαχρονικό, αρά δεν μιλάμε για κάτι πρωτοφανές. Στόχος των λεγόμενων χάκερς είμαστε δυνητικά όλες και όλοι».

Σε ερώτηση αν είναι ανοχύρωτες οι κυβερνητικές υπηρεσίες, πώς μπορούν να οχυρωθούν και αν έχει πλάνο οχύρωσης, απάντησε: «Οι κυβερνητικές υπηρεσίες χρειάζονται περαιτέρω ενίσχυση και αυτό είναι δεδομένο. Ωστόσο, η κατάσταση παραμένει υπό διαχείριση και δεν υπάρχει λόγος τρομοκρατίας. Παρόλα αυτά δεν εφησυχάζουμε. Οι κυβερνοεπιθέσεις είναι μέρος της καθημερινότητάς μας και ως κράτος οφείλουμε να προετοιμαστούμε ακόμη για το χειρότερο σενάριο. Αντιλαμβάνεστε ότι τα συστήματα ασφαλείας δεν είναι διακοσμητικά, πρέπει και επιβάλλεται να χρησιμοποιούνται ορθά. Χρειάζονται συντήρηση, συνεχόμενη αναβάθμιση και αντικατάσταση όπου πρέπει. Παράλληλα και μέχρι την αντικατάσταση των συστημάτων ασφαλείας στις κρατικές υπηρεσίες πρέπει να γίνει ενδελεχής ενημέρωση και εκπαίδευση του προσωπικού. Πρέπει δηλαδή ο ανθρώπινος παράγοντας να μπορεί στον μεγαλύτερο βαθμό να αναγνωρίσει 'πειρατικές' επιθέσεις και να τις αποφεύγει. Ακόμη και εάν κατορθώσουμε να έχουμε τα υψηλότερα συστήματα ασφαλείας υπάρχει πάντοτε η πιθανότητα να χτυπηθεί το κράτος. Το ζήτημα είναι να είμαστε έτοιμοι τόσο να τις αποφύγουμε όσο και να τις αντιμετωπίσουμε, χωρίς απώλειες, εάν τελικά συμβούν. Υπάρχει πάντοτε πιθανότητα επίθεσης, δεν γνωρίζουμε όμως το πότε και πώς, συνεπώς η ετοιμότητα είναι το παν. Πρέπει να υπάρχει επαρκής πρόληψη στη βάση ακόμη και του χειρότερου σεναρίου επίθεσης. Με την σημαντική συμβολή των επιστημόνων μας και των εμπλεκόμενων φορέων θα εργαστούμε προς την σωστή κατεύθυνση για να διασφαλίσουμε το καλύτερο δυνατό αποτέλεσμα. Παράλαβα χαρτοφυλάκιο πριν από 20 ημέρες. Πρέπει να πάρουμε τα πράγματα από την αρχή, να εξακριβώσουμε τις ελλείψεις και να δράσουμε ουσιαστικά. Τέλος, σαν κράτος πρέπει να πράξουμε με ευθύνη και να επενδύσουμε σε άρτια συστήματα ασφαλείας με ό,τι αυτό περιλαμβάνει, αφού το οικονομικό πλήγμα μετά από τέτοιες επιθέσεις δημιουργεί αλυσιδωτές επιπτώσεις».

Συγκεκριμένα για το κτύπημα στο κτηματολόγιο και για τη ζημιά που υπέστη, εξήγησε ότι, «βρίσκεται υπό εξέλιξη έρευνα, από την οποία θα διαπιστωθεί ποια είναι επακριβώς η ζημιά. Μέχρι σήμερα έχουν ήδη παραδοθεί κάποιες υπηρεσίες του Κτηματολογίου, ακολουθείται συγκεκριμένη διαδικασία για την επάνοδο τμημάτων των μηχανογραφικών χωρίς απώλειες. Το ζήτημα όντως ήταν σοβαρό, ωστόσο είναι υπό διαχείριση».

Συνάμα, έδωσε ένα τέλος στα σενάρια ότι οι συγκεκριμένοι χάκερς που κτύπησαν το κτηματολόγιο έλαβαν λύτρα. Όπως είπε ο υφυπουργός, «οι επιθέσεις είναι σαφώς εκβιαστικές και ο στόχος τους τις περισσότερες φορές είναι η απόσπαση χρηματικού ποσού, δηλαδή λύτρα. Σύμφωνα με την ενημέρωση που είχα, δεν έχει δοθεί οποιοδήποτε ποσό για να επανακτήσουμε τα δεδομένα μας. Τα δεδομένα ανακτήθηκαν πίσω χωρίς να χρειαστεί οποιαδήποτε επικοινωνία με τους χάκερς».

Πώς δρουν οι χάκερς

Ο ειδικός της κυβερνοασφάλειας, Associate Director, CEE&EM Security & Resilience services Partner, Kyndryl Κύπρου, Χρίστος Γιακουμής, εξηγεί με τη σειρά του στην «Κ» πως δρουν οι χάκερς, τι ζητούν και πως πληρώνονται. «Σε περιπτώσεις 'ransomware', οι κυβερνοεγκληματίες εκμεταλλευόμενοι είτε κάποια ευπάθεια σε συστήματα και εφαρμογές, είτε τον ανθρώπινο παράγοντα μέσω phishing, αποκτούν πρόσβαση σε συστήματα και προχωρούν στην κρυπτογράφηση των αρχείων καθώς και των αντίγραφων ασφαλείας (backups). Ακολούθως, τα θύματα ενημερώνονται στην οθόνη τους ή μέσω κάποιου αρχείου για τον τρόπο και χρόνο πληρωμής των λύτρων για να τους δοθούν τα κλειδιά αποκρυπτογράφησης των αρχείων. Η επιλογή των κρυπτονομισμάτων ως μέσο πληρωμής δεν είναι τυχαία καθώς καθιστά εξαιρετικά δύσκολο τον εντοπισμό των εγκληματικών στοιχείων. Είναι επίσης άγνωστο εάν μετά την πληρωμή οι κυβερνοεγκληματίες θα τους δώσουν τα σχετικά κλειδιά. Υπάρχουν όμως και παραδείγματα από οργανισμούς που προχώρησαν σε πληρωμές μη μπορώντας να ανακτήσουν τα δεδομένα και τα συστήματα από τα αντίγραφα ασφαλείας. Η συμβουλή που δίδεται είναι οι οργανισμοί να μην προχωρούν σε πληρωμή των λύτρων, να ενημερώνουν τις αρμόδιες αρχές, ενεργοποιώντας παράλληλα το πλάνο απόκρισης περιστατικών και αξιολογώντας όλα τα δεδομένα μέχρι την πλήρη αποκατάσταση.

Ο κ. Γιακουμή εξήγησε στη συνέχεια πώς οχυρώνονται τα κράτη εντοπισμό και απόκριση, καθώς και ανάκτηση από περιστατικά. Σε εθνικό επίπεδο υπάρχει το σχετικό νομοθετικό πλαίσιο στο οποίο καθορίζονται όλα τα μέτρα τα οποία πρέπει να λαμβάνονται από τις κρίσιμες υποδομές και φορείς εκμετάλλευσης βασικών υπηρεσιών. Επίσης, τα κράτη μέλη της Ευρωπαϊκής Ένωσης συνεργάζονται μέσω κοινών προγραμμάτων καθώς και για ανταλλαγή πληροφοριών για αντιμετώπιση κυβερνοαπειλών. Ένα ολοκληρωμένο πρόγραμμα θέτει τα θεμέλια για τη δημιουργία κουλτούρας κυβερνοασφάλειας στον οργανισμό όπου ο κάθε υπάλληλος και το κάθε τμήμα λειτουργεί με γνώμονα την προστασία των δεδομένων και των πληροφοριακών συστημάτων. Η εκπαίδευση του προσωπικού σε τέτοια θέματα επιβάλλεται και είναι απαραίτητη για την έγκαιρη ανίχνευση περιστατικών όπως phishing. Επιπλέον, οι οργανισμοί θα πρέπει να αναθεωρήσουν τις υπάρχουσες υποδομές και να προχωρήσουν σε εκσυγχρονισμό τους, με την εισαγωγή και σχεδιασμό υποδομών με βάση τις αρχές μηδενικής εμπιστοσύνης (zero trust) όπως microsegementation, identity and privileged access management, immutable storage, κτλ. Παράλληλα η αξιολόγηση των συστημάτων και διαδικασιών μέσω ασκήσεων τύπου cyber attack simulation, penetration testing και red teaming βοηθούν στον εντοπισμό ευπαθειών που πιθανόν να μην εντοπίζονται από αυτοματοποιημένα συστήματα ασφαλείας και λογισμικά σάρωσης.

Ως ειδικός του Cybersecurity ο κ. Γιακουμής εξήγησε στην «Κ» πως πρέπει να προστατευτεί η Κύπρος από εδώ και πέρα. «Τα τελευταία χρόνια έχουν γίνει αρκετά και σημαντικά βήματα από τις Αρχές σε συνεργασία με το δημόσιο, ιδιωτικό και ακαδημαϊκό τομέα. Παράλληλα όμως, αναγνωρίζεται ότι οι κυβερνοεπιθέσεις θα εντείνονται και θα γίνονται όλο και πιο εξειδικευμένες. Γι' αυτό τον λόγο, η συζήτηση πλέον έχει μεταφερθεί από το 'εάν' γίνει κάποιο περιστατικό στο 'όταν θα γίνει' και στο πώς να γίνουμε πιο ανθεκτικοί. Απαραίτητο συστατικό για να επιτύχει το όποιο εγχείρημα όμως είναι η καλλιέργεια κουλτούρας και η ευαισθητοποίηση σε θέματα κυβερνοασφάλειας. Υπάρχουν παραδείγματα οργανισμών που αντιμετωπίζουν ακόμη την κυβερνοασφάλεια ως ένα πρόβλημα του τμήματος Πληροφορικής. Αυτό πρέπει να εκλείψει. Οι Διοικήσεις καλούνται πλέον να είναι ενημερωμένες, εξασφαλίζοντας την επιχειρησιακή ανθεκτικότητα, λαμβάνοντας τα απαραίτητα μέτρα τα οποία θα ενισχύσουν το επίπεδο ασφάλειας των πληροφοριακών συστημάτων, την επαρκή στελέχωση με εξειδικευμένο προσωπικό καθώς και τη σταδιακή δημιουργία κουλτούρας κυβερνοασφάλειας. Επιπρόσθετο ζητούμενο είναι επίσης η ταχύτητα και η ευελιξία με την οποία θα κινηθούμε συλλογικά για να εφαρμόσουμε τα απαραίτητα μέτρα. Στην εποχή του ψηφιακού μετασχηματισμού και της καινοτομίας, η ασφάλεια στον κυβερνοχώρο αποτελεί απαραίτητο στοιχείο για τη δημιουργία ενός περιβάλλοντος εμπιστοσύνης και σταθερότητας».

Κυριάκος Κόκκινος: Μεγάλη σημασία να επενδύσουμε στην κυβερνοάμυνα

Ο πρώτος υφυπουργός Καινοτομίας της Κύπρου, Κυριάκος Κόκκινος, σημείωσε από πλευράς του πως, μετά τον πόλεμο στην Ουκρανία, έχουν εντατικοποιηθεί οι επιθέσεις των χάκερς παγκοσμίως και δεν γίνονται μόνο στην Κύπρο. «Το φαινόμενο έχει εντατικοποιηθεί σε όλες τις εκφάνσεις, είτε για να ζητήσουν λύτρα οι χάκερς, είτε για να δοκιμάσουν τις δυνάμεις τους, είτε είναι για να κλέψουν δεδομένα για να τα πωλήσουν αλλού, είτε απλώς για να κάνουν ζημιά σε υποδομές», εξήγησε. Ο κ. Κόκκινος έδωσε το δικό του στίγμα, λέγοντας πως, στην κυβερνοεπίθεση εξ ορισμού τα πρόσωπα είναι πάντα ένα βήμα μπροστά. Το ζήτημα κατά τον πρώην υφυπουργό δεν είναι η κυβερνοεπίθεση, αλλά η κυβερνοάμυνα, δηλαδή να υπάρχουν οι μηχανισμοί για να ελεγχθεί κατά πόσο είναι θύμα κυβερνοεπίθεσης η όποια οντότητα, αλλά και να γίνεται αντιληπτό το επίπεδο διείσδυσής τους στα δεδομένα. Ερωτηθείς σχετικά, ο κ. Κόκκινος επισήμανε πως η Κύπρος διαθέτει συστήματα κυβερνοάμυνας και πρέπει να εξελίσσονται συνεχώς με καινούργιες τεχνολογίες και με ανθρώπινο δυναμικό που μπορεί να τη χειριστεί. «Το ανθρώπινο δυναμικό είναι πιο σημαντικό από το να υπάρχουν απλώς τα εργαλεία. Συνάμα, μεγάλο ζήτημα είναι η αντίληψη της κυβερνοασφάλειας. Εσφαλμένα ανάγεται ως τεχνολογική πρόκληση, καθώς είναι πρόκληση επιχειρησιακή. Εξαρτάται από τις δομές, τις γνώσεις και την εγρήγορση που υπάρχει, αλλά και τις διαδικασίες για να ενεργοποιηθούν μηχανισμοί, τέτοιοι που να μην επιτρέψουν να γίνει μεγάλο κακό κατά την επίθεση», σημείωσε.