Πανεπιστήμιο Κύπρου

Γραφείο Επικοινωνίας
Τομέας Προώθησης
και Προβολής

Τηλέφωνο: **22894304**
Ηλ. Διεύθυνση: **prinfo@ucy.ac.cy**
Ιστοσελίδα: **www.ucy.ac.cy/pr**

ΣΥΝΤΑΞΗ: ΦΩΤΕΙΝΗ ΠΑΝΑΓΗ

Πέμπτη, 24 Μαΐου 2018

ΜΕΓΑΛΗ ΑΠΕΙΛΗ ΓΙΑ ΤΙΣ ΔΗΜΟΣΙΕΣ ΕΤΑΙΡΕΙΕΣ ΟΙ ΔΙΑΔΙΚΤΥΑΚΕΣ ΕΠΙΘΕΣΕΙΣ

Έρευνα που διενεργήθηκε από τον Αν. Καθηγητή του Πανεπιστημίου Κύπρου Ανδρέα Μιλιδώνη μελέτησε τις επιπτώσεις των κυβερνοεπιθέσεων σε δημόσιες επιχειρήσεις.

Οι επιθέσεις μέσω διαδικτύου (Cyberattacks) κοστίζουν σε εταιρείες περίπου 445 δισεκατομμύρια δολάρια σε παγκόσμιο επίπεδο ετησίως. Πώς αυτές οι επιθέσεις επηρεάζουν την ανάπτυξη και την αξία των μετόχων με την πάροδο του χρόνου; Παρά την αυξανόμενη συνειδητοποίηση της απειλής επιθέσεων μέσω διαδικτύου, είναι άγνωστο ακόμα ποιες εταιρείες είναι πιο πιθανό να αποτελέσουν στόχο και πώς οι επιθέσεις επηρεάζουν την ανάπτυξη και την αξία των μετόχων με την πάροδο του χρόνου.

Ωστόσο, μια νέα μελέτη που διενεργήθηκε από τον Αναπληρωτή Καθηγητή του Τμήματος Λογιστικής και Χρηματοοικονομικών του Πανεπιστημίου Κύπρου, Ανδρέα Μιλιδώνη, σε συνεργασία με τους Shinichi Kamiya (Τεχνολογικό Πανεπιστήμιο Nanyang (NTU) της Σιγκαπούρης), Jun-koo Kang (Τεχνολογικό Πανεπιστήμιο Nanyang), Jungmin Kim (Πολυτεχνείο Χονγκ Κονγκ) και Rene Stulz (Κρατικό Πανεπιστήμιο του Οχάιο, Εθνικό Γραφείο Οικονομικών Ερευνών (NBER) και Ευρωπαϊκό Ινστιτούτο Εταιρικής Διακυβέρνησης (ECGI)) εξετάζει τα εν λόγω θέματα. Η μελέτη χρησιμοποιεί ένα περιεκτικό δείγμα γεγονότων παραβιάσεων δεδομένων που προκλήθηκαν από επιτυχείς επιθέσεις μέσω διαδικτύου που αναφέρθηκαν στην Υπηρεσία Ελέγχου Προστασίας Προσωπικών Δεδομένων (PRC) κατά την περίοδο 2005 έως 2014. Στη μελέτη περιλαμβάνονται μόνο κακόβουλες ενέργειες μέσω διαδικτύου, hacking και malware και εξετάζεται η βραχυπρόθεσμη αλλά και η μακροπρόθεσμη επίδραση (3 χρόνια μετά) που επιδέχονται τέτοιες επιθέσεις.

Η έρευνα με τίτλο, "*What is the Impact of Successful Cyberattacks on Target Firms?"* κυκλοφόρησε πρόσφατα υπό μορφή Επιστημονικής Εργασίας ως National Bureau of Economic Research **(**NBER**)** Working paper (*τα NBER Working Papers βρίσκονται στο νούμερο 1 των δημοφιλέστερων δημοσιεύσεων με βάση το Google Scholar στον τομέα "Business, Economics and Management" https://scholar.google.com/citations?view_op=top_venues&hl=el&vq=bus*).

Οι ερευνητές διαπίστωσαν ότι οι μεγάλες, πολύτιμες και ορατές επιχειρήσεις - *όπως οι εταιρείες που συγκαταλέγονται στη λίστα Fortune 500* – δέχονται συχνότερα επιθέσεις μέσω διαδικτύου, παρά το γεγονός ότι φαίνεται να διαθέτουν τους πόρους για να αντιμετωπίσουν το έγκλημα στον κυβερνοχώρο. Οι

εταιρείες που χρησιμοποιούν τα προσωπικά δεδομένα των πελατών για την καθημερινή τους δραστηριότητα, όπως αυτές στον χρηματοπιστωτικό και τον λιανικό τομέα, είναι επίσης συχνότεροι στόχοι, ανεξάρτητα από το μέγεθός τους.

Σύμφωνα με τα αποτελέσματα της έρευνας, οι τομείς που δέχονται συχνά επιτυχημένες επιθέσεις στον κυβερνοχώρο είναι οι υπηρεσίες, εταιρείες που ασχολούνται με χονδρικές και λιανικές πωλήσεις, με μεταφορές και την επικοινωνία. Για την αποτροπή της εγκληματικότητας μέσω διαδικτύου, η επαγρύπνηση του διοικητικού συμβουλίου μιας εταιρείας αποδίδει: Οι επιχειρήσεις που διαθέτουν επιτροπή διαχείρισης κινδύνου είναι λιγότερο πιθανό να δεχτούν επίθεση από εκείνες που δεν έχουν τέτοια επιτροπή.

Ο Αναπληρωτής Καθηγητής, Ανδρέας Μιλιδώνης σημείωσε ότι, η προστασία μιας επιχείρησης από τον κίνδυνο επίθεσης μέσω διαδικτύου ξεκινά από την αναγνώριση και αξιολόγηση των κινδύνων στους οποίους είναι εκτεθειμένη. *«Παρά την ευρεία αναγνώριση των αναδυόμενων απειλών που θέτει ο κίνδυνος επίθεσης μέσω διαδικτύου και η σημασία του ως νέου τύπου εταιρικού κινδύνου, ελάχιστα στοιχεία υπάρχουν για το πώς οι επιτυχημένες επιθέσεις επηρεάζουν τις επιχειρήσεις. Συγκεκριμένα, ελάχιστα γνωρίζουμε ποιοι τύποι επιχειρήσεων είναι πιθανό να βιώσουν επιθέσεις μέσω διαδικτύου και πώς τέτοιες επιθέσεις επηρεάζουν τον πλούτο, την ανάπτυξη και την οικονομική δύναμη των μετόχων. Επίσης, δεν γνωρίζουμε πολλά για το πώς οι επιχειρήσεις αλλάζουν τα κίνητρα διαχείρισης κινδύνων μετά από επιθέσεις στον κυβερνοχώρο»*, τόνισε ο Δρ Μιλιδώνης.

Όταν οι χάκερ αποκτούν πρόσβαση στα προσωπικά δεδομένα των πελατών, μια εταιρεία στις ΗΠΑ χάνει κατά μέσο όρο περισσότερα από 600 εκατομμύρια δολάρια, στην αξία των της χρηματιστηριακής της αξίας τις αμέσως επόμενες ημέρες. Οι μεγαλύτερες επιχειρήσεις, καθώς και οι επιχειρήσεις λιανικής πώλησης, σημειώνουν επίσης πτώση της αύξησης των πωλήσεων τρία χρόνια μετά από μια τέτοια επίθεση.

Από οικονομικής απόψεως, η έρευνα κατέδειξε ότι οι επιχειρήσεις συνήθως περιορίζονται μετά από επιθέσεις στον κυβερνοχώρο. Συγκεκριμένα, προσπαθούν να ξεπεράσουν τις απώλειες μειώνοντας τις επενδύσεις τους και αυξάνοντας το μακροπρόθεσμο χρέος. Μετά από μια επίθεση μέσω διαδικτύου, οι εταιρείες είναι επιφυλακτικές για ανάληψη ρίσκου και τείνουν να μειώνουν τα κίνητρα που δίνονται σε Διευθυντικά στελέχη για μελλοντική ανάληψη ρίσκου. Αυτό γίνεται με την μείωση των επιπλέον επιδομάτων (salary bonus) σε Διευθυντικά στελέχη όπως επίσης και την ανταλλαγή δικαιωμάτων αγοράς μετοχών της εταιρείας (option on company shares) με μετοχές περιορισμένης εξαργύρωσης (restricted shares).

Ο Αναπληρωτής Καθηγητής Ανδρέας Μιλιδώνης σημειώνει ότι αυτές οι αλλαγές μπορούν πράγματι να είναι επωφελείς, *«εάν μια ηλεκτρονική επίθεση οδηγεί σε επανεκτίμηση του κινδύνου μιας μελλοντικής ηλεκτρονικής επίθεσης και του συνεπακόλουθου κόστους μιας τέτοιας επίθεσης»*. Παρά το γεγονός ότι η ασφάλεια στον διαδίκτυο αποτελεί ένα από τα φλέγοντα ζητήματα της εποχής μας, σπάνια οι επιχειρήσεις εκτιμούν σωστά την πραγματική πιθανότητα μιας επίθεσης μέσω διαδικτύου και το κόστος που μπορεί να επιφέρει μια επιτυχημένη επίθεση.

Η έρευνα έχει ήδη προσελκύσει το ενδιαφέρον διεθνούς κύρους οργανισμών, όπως την Επιτροπή Κεφαλαιαγοράς των ΗΠΑ (US Securities and Exchange Commission), το Harvard Law School Forum on

Πανεπιστήμιο Κύπρου

Corporate Governance and Financial Regulation, τον ευρωπαϊκό VOX (CEPR's Policy Portal) αλλά και αρκετών δημοσιογράφων και αναλυτών σε διεθνή Μέσα Μαζικής Ενημέρωσης (π.χ. Bloomberg).

Διαβάστε στον ακόλουθο σύνδεσμο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135514 ολόκληρη την έρευνα.