«Ο διαδικτυακός κίνδυνος στα Ανώτατα Εκπαιδευτικά Ιδρύματα και η ανάγκη προστασίας τους από απειλές στο ψηφιακό κόσμο. Έρευνα στα Εκπαιδευτικά Ιδρύματα του Νομού Θεσσαλονίκης»

Καϊμακάμη Νικολέττα[1], Τέγος Γεώργιος[2]

[1]Οικονομολόγος, Μεταπτυχιακό Δίπλωμα, Χρηματοοικονομική Διοίκηση, Λογιστική και Πληροφοριακά Συστήματα, Τμήμα Λογιστικής και Χρηματοοικονομικής, Σ.Δ.Ο., Α.Τ.Ε.Ι.Θ.
kaimakami_nikoletta@gmail.com
[2] Καθηγητής Πληροφορικής, Τμήμα Λογιστικής και Χρηματοοικονομικής, Σ.Δ.Ο., Α.Τ.Ε.Ι.Θ.
gtegos@gen.teithe.gr

ΠΕΡΙΛΗΨΗ

Ο σύγχρονος ψηφιακός κόσμος, παράλληλα με τις αμέτρητες δυνατότητες που προσφέρει στους χρήστες του διαδικτύου, δημιουργεί ένα πρωτόγνωρο αίσθημα ανασφάλειας. Η παραβίαση των ηλεκτρονικών δεδομένων αποτελεί ένα νέο είδος απειλής, άρρηκτα συνυφασμένης με τον διαδικτυακό κίνδυνο, ο οποίος αφορά όλους τους οργανισμούς, επιχειρήσεις και Ιδρύματα, ανεξαρτήτως μεγέθους και αντικειμένου εργασιών. Από τα κύματα των κυβερνοεπιθέσεων, δεν θα μπορούσε να εξαιρεθεί ο κλάδος της Εκπαίδευσης, με τα Πανεπιστήμια να αποτελούν δελεαστικό στόχο για κάθε επίδοξο hacker. Με την ενσωμάτωση της τεχνολογίας της πληροφορίας στη μαθησιακή διαδικασία και με συνεχώς αυξανόμενο τον αριθμό των συνδεδεμένων χρηστών στα Πανεπιστημιακά δίκτυα, γίνεται ακόμα επιτακτικότερη η ανάγκη προστασίας των πληροφοριακών συστημάτων τους από τις διαδικτυακές απειλές. Σκοπός του παρόντος άρθρου, είναι να διερευνήσει τους λόγους στοχοποίησης των Ανώτατων Εκπαιδευτικών Ιδρυμάτων, καθώς και να διαπιστώσει μέσω ερευνητικής προσέγγισης το βαθμό συνειδητοποίησης της σπουδαιότητας του διαδικτυακού κινδύνου από το προσωπικό τους. Ειδικότερα δε, θα αποκαλυφθεί το πως αντιλαμβάνονται και ποια στάση ακολουθούν απέναντι στις απειλές του διαδικτύου τα Ανώτατα Εκπαιδευτικά Ιδρύματα στον Νομό Θεσσαλονίκης.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: *Διαδίκτυο, Κίνδυνος, Ασφάλεια, Ανώτατα Εκπαιδευτικά Ιδρύματα*

ΕΙΣΑΓΩΓΗ

Στους παραδοσιακούς κινδύνους που αντιμετώπιζαν ως τώρα οι διάφοροι κλάδοι της οικονομίας, έρχεται να προστεθεί τις τελευταίες δεκαετίες και η απειλή της παραβίασης των ηλεκτρονικών δεδομένων τους ή αλλιώς ο κίνδυνος μιας κυβερνοεπίθεσης. Ο διαδικτυακός κίνδυνος συμπεριλαμβάνει

οποιονδήποτε κίνδυνο συνδέεται με χρήση και διαχείριση ηλεκτρονικών δεδομένων και έχει χαρακτηριστεί ως ο πλέον μεγαλύτερος, λειτουργικός συστημικός κίνδυνος που έχει αντιμετωπίσει η ασφαλιστική αγορά στον τελευταίο μισό αιώνα. Επηρεάζει κάθε είδους οργάνωση ανά το κόσμο, γεγονός που οδήγησε τα περιστατικά ασφαλείας στον κυβερνοχώρο να φτάσουν το 2014 κατά μέσο όρο ημερησίως τα 117.339, ενώ αξιοσημείωτη επίσης ήταν η εκτίμηση σε επίπεδο κόστους για τους κινδύνους στον κυβερνοχώρο, η οποία άγγιζε τα 400 δις δολάρια ετησίως (Fullbright, 2016).

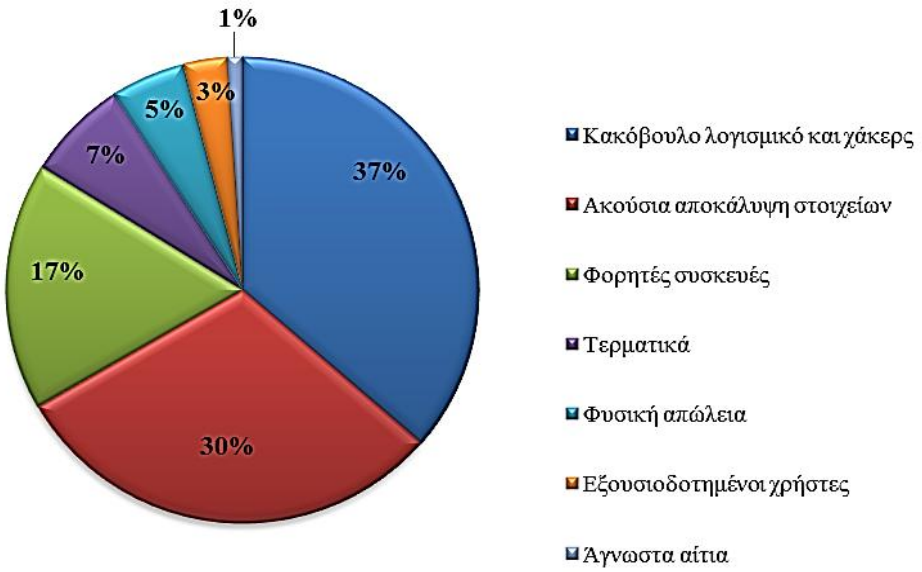
Σε ένα περιβάλλον συνεχώς μεταβαλλόμενο και εξελισσόμενο τεχνολογικά, η ανάγκη ασφαλούς μεταφοράς και διατήρησης δεδομένων για τους χρήστες του διαδικτύου γίνεται ακόμα μεγαλύτερη. Καθώς συνήθως κρίνονται αναποτελεσματικά όλα τα μέτρα πρόληψης και προστασίας των Εκπαιδευτικών Ιδρυμάτων απέναντι στις διαδικτυακές απειλές, στην ανασφάλεια λύση έρχεται να δώσει η σωστή ενημέρωση και η καλλιέργεια της κουλτούρας ασφαλείας. Αυτές, παράλληλα με την υιοθέτηση ενός οργανωμένου σχέδιου απόκρισης περιστατικών, αποτελούν συστατικά απαραίτητα για την θωράκιση των δικτύων τους απέναντι στις απειλές του ψηφιακού κόσμου. Το άρθρο αυτό έρχεται να καλύψει σε θεωρητικό επίπεδο θέματα ασφάλειας δικτύου των Πανεπιστημιακών Ιδρυμάτων, παραθέτοντας παράλληλα στατιστικά στοιχεία της έρευνας που διεξήχθη σε αυτά του Νομού Θεσσαλονίκης, προκειμένου να διερευνηθεί η στάση τους απέναντι στον διαδικτυακό κίνδυνο.

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

Η ηλεκτρονική επικοινωνία είναι ουσιώδης και βασική στη λειτουργία των Πανεπιστημιακών Ιδρυμάτων οπότε θα ήταν αδύνατο να μην τα αφορά η απειλή ενός συμβάντος ασφαλείας. Η παραβίαση των συστημάτων αποτελεί συνεπακόλουθο μιας αστοχίας των συστημάτων πληροφοριών και του λογισμικού, κακής διαχείρισης των ίδιων των χρηστών, αποτυχημένων εσωτερικών διαδικασιών ή εξωτερικών αστάθμητων παραγόντων. Προκαλείται δε, από κακόβουλες δράσεις χρηστών που έχουν απώτερο σκοπό να προκαλέσουν βλάβες και διαταραχές στην ομαλή λειτουργία του εκάστοτε Οργανισμού, προκαλώντας τόσο ηθικές όσο και οικονομικές απώλειες, μέσω της προσβολής της ασφάλειας των πληροφοριών. Η διατάραξη της ασφάλειας των πληροφοριών επηρεάζει άμεσα τις θεμελιώδεις αρχές τους, δηλαδή την εμπιστευτικότητα την ακεραιότητα και τη διαθεσιμότητά τους (Cebula et all, 2010, OECD, 2016, Biener et al, 2015).

Βασισμένοι σε έρευνα που διεξήχθη το δίμηνο Οκτωβρίου-Νοεμβρίου 2017 και στην οποία συμμετείχαν εκπαιδευτικοί όλων των βαθμίδων, διοικητικό προσωπικό και συνεργάτες των Πανεπιστημιακών Ιδρυμάτων του Νομού Θεσσαλονίκης (Παράρτημα), ο διαδικτυακός κίνδυνος αναγνωρίστηκε με ποσοστό 95% ως ο πλέον σημαντικός ανάμεσα σε αυτούς που καλούνται να αντιμετωπίσουν οι διάφοροι οργανισμοί, ενώ ποσοστό 39,8% από τους συμμετέχοντες στην έρευνα, τον θεωρεί κύρια απειλή ειδικά για αυτά. Επιπλέον υποστηρίχθηκε, πως η συνεχής αύξηση, εξέλιξη και διαφοροποίηση των

ιντερνετικών εισβολών είναι σημαντικός παράγοντας που συντελεί στην ανασφάλεια στο διαδίκτυο με ποσοστό 26,9% (Καϊμακάμη, 2017).



Σχήμα 1: Τύποι συμβάντων που επηρεάζουν την Ανώτατη Εκπαίδευση.

Σύμφωνα με την εταιρία εξειδικευμένης ασφάλισης Beasley, από το σύνολο των επιθέσεων που χειρίστηκε το 2016, οι παραβιάσεις σε συστήματα Εκπαιδευτικών Ιδρυμάτων μέσω κακόβουλου λογισμικού, παρουσίασαν αύξηση σε σχέση με το 2015 αγγίζοντας το 45% έναντι του 35% της προηγούμενης χρονιά. Όπως εξάλλου διαπιστώνουν οι ειδικοί στην παροχή υπηρεσιών cyber risk της Ernest and Young στο Σχήμα 1., οι παραβάσεις δεδομένων βάσει της επιρροής τους στην τριτοβάθμια εκπαίδευση κατατάσσονται ως εξής: στην πρώτη θέση των απειλών για την ανώτατη εκπαίδευση και με ποσοστό 37% βρίσκεται η ηλεκτρονική παραβίαση από εξωτερικό χρήστη μέσω κακόβουλου λογισμικού, malware ή hacking. Αυτό μπορεί ενδεικτικά να γίνει με πρακτικές ηλεκτρονικού ψαρέματος, άρνηση παροχή υπηρεσίας και μολυσματικά μηνύματα. Αμέσως μετά με 30% βρίσκουμε τις ακούσιες αποκαλύψεις ενώ στη συνέχεια βρίσκουμε την απώλεια τόσο φορητών όσο και σταθερών συσκευών και λοιπών μέσων πρόσβασης στο διαδίκτυο Έπειτα ακολουθούν με ποσοστό 5% η φυσική απώλεια-απόρριψη αρχείου μη ψηφιακής μορφής, ενώ την προτελευταία θέση με ποσοστό 3% καταλαμβάνει η εκούσια παραβίαση του συστήματος από εξουσιοδοτημένο χρήστη. Τέλος με ποσοστό μόλις 1% έχουμε άγνωστες αιτίες. (Abhey et al 2016; Beasley, 2017,;Roman, 2015).

Η λίστα των Πανεπιστημιακών Ιδρυμάτων που βίωσαν με οποιοδήποτε τρόπο παραβιάσεις των δεδομένων τους είναι μακρά. Στα καταγεγραμμένα περιστατικά ασφαλείας Πανεπιστημιακών συστημάτων από το 2005 ως σήμερα, συγκαταλέγονται μεγάλα ονόματα γνωστών Εκπαιδευτικών Ιδρυμάτων του εξωτερικού. Συμπεριλαμβάνουν βέβαια μονάχα αυτά τα οποία δημοσιοποιήθηκαν, διότι δεδομένων των επιπτώσεων μιας κυβερνοεπίθεσης,

υπάρχουν περιπτώσεις που αυτή είτε δεν γνωστοποιείται εγκαίρως, είτε και καθόλου από τον φορέα που έχει πληγεί, οπότε τα κρούσματα είναι πολύ περισσότερα από όσα έχουν καταμετρηθεί. Ενδεικτικά αναφέρουμε την περίπτωση του UC Berkeley, όπου το 2016 εκτέθηκαν λόγω παραβίασης των συστημάτων του 80.000 οικονομικά αρχεία ή αυτή του UCLA όπου περισσότεροι από 30.000 μαθητές, τρέχοντες και πρώην του ιδρύματος ενημερώθηκαν τον Αύγουστο του 2017 για παραβίαση της ασφάλειάς του και πιθανή έκθεση προσωπικών δεδομένων τους. Ομοίως στο Πανεπιστήμιο του Ουισκόνσιν αναφέρθηκαν περίπου 90.000 έως 100.000 προσπάθειες ημερησίως, από την Kiva μόνο, για διείσδυση στο σύστημά του, ενώ το 2014 στο Πανεπιστήμιο του Maryland, εκτέθηκαν προσωπικά δεδομένα περίπου 310.000 φοιτητών και συνεργατών που χρονολογούνταν από το 1998. (Privacy Rights Clearinghouse; Abhey et al, 2016)

Κατανοούμε πως χρήση τεχνολογίας ως μέσο προστασίας και ασφάλειας δικτύων είναι καταλυτική και αξίζει να αναφέρουμε ως σημαντική τη χρήση κρυπτογραφίας στο χώρο των Εκπαιδευτικών Ιδρυμάτων αλλά και την εφαρμογή αμυντικών μηχανισμών, όπως τα τείχη προστασίας, τα ηλεκτρονικά πιστοποιητικά, όπως και την ενσωμάτωση ακόμα πιο σύγχρονων μεθόδων πρόληψης και εντοπισμού διαδικτυακών εισβολών, όπως η τεχνητή νοημοσύνη και μηχανική μάθησης σε αυτούς. Η τεχνολογία όμως από μόνη της δεν επαρκεί ώστε να προστατευτούν τα συστήματά των Πανεπιστημίων, σε αυτό συνηγορούν αυτά της Θεσσαλονίκης με ποσοστό 82,10%, υποστηρίζοντας πως απαραίτητη προϋπόθεση για την αποτελεσματική προστασία των συστημάτων, είναι να γίνονται πάντα οι απαραίτητες αναβαθμίσεις και επικαιροποιήσεις τόσο στο υλικό όσο και στο διαθέσιμο λογισμικό, καθώς επίσης θα πρέπει συνδυαστικά να λαμβάνονται επιπλέον μέτρα προστασίας, όπως η ενημέρωση και εκπαίδευση των χρηστών.

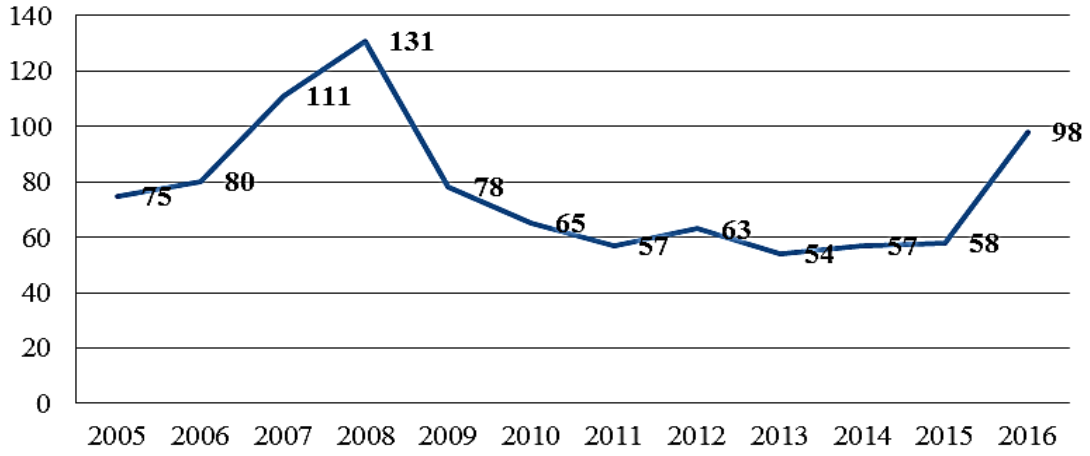
Η ΕΛΚΥΣΤΙΚΟΤΗΤΑ ΚΑΙ ΕΥΑΙΣΘΗΣΙΑ ΤΩΝ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΙΔΡΥΜΑΤΩΝ ΣΤΙΣ ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ

Είναι γεγονός πως τα Εκπαιδευτικά Ιδρύματα και ιδιαίτερα τα Πανεπιστήμια, λόγω των πλούσιων δεδομένων που φιλοξενούν στις βάσεις τους, βρίσκονται μεταξύ των βασικών προς παραβίαση στόχων. Εξάλλου η ελευθερία της πρόσβασης μέσω πολλών και διαφορετικών σημείων κάνει δύσκολη την προστασία τους και τα κάνουν ακόμα πιο δελεαστικά, προκαλώντας τα να συνδυάσουν την κουλτούρα της ελεύθερης ανταλλαγής ιδεών με την προστασία από τις κυβερνοεπιθέσεις (Roman, 2015). Η ελκυστικότητα των Πανεπιστημίων ως στόχων κυβερνοεπιθέσεων μπορεί να δικαιολογηθεί, καθώς προκειμένου αυτά να οργανωθούν και να λειτουργήσουν σωστά, καλούνται να συλλέξουν από τους φοιτητές, προσωπικό και συνεργάτες τους, ερευνητές και συμμετέχοντες σε κάποιο έργο, πληθώρα απαραίτητων πληροφοριών, τις οποίες επεξεργάζονται και διατηρούν στις βάσεις δεδομένων τους για αρκετό καιρό. Ειδικά όταν πρόκειται για Πανεπιστημιακά Ιδρύματα του Εξωτερικού, το φάσμα των δεδομένων αυτών διευρύνεται ακόμα, συμπεριλαμβάνοντας και επιπλέον στοιχεία, όπως αριθμούς κοινωνικής ασφάλισης, αποτελέσματα

ιατρικών εξετάσεων, ακόμα και λεπτομέρειες δόσεων δανείων, τραπεζικούς λογαριασμούς και λοιπά φορολογικά στοιχεία (Amigorena, 2017).

Η πειρατεία σε ένα Πανεπιστημιακό Ίδρυμα είναι επίσης εξαιρετικά προσοδοφόρα, καθώς ο μεγάλος όγκος πληροφοριών προσωπικής ταυτοποίησης, πολλές φορές βρίσκεται να διαπραγματεύεται στην λεγόμενη υπόγεια διαδικτυακή αγορά. Περίπου 300 από τα μεγαλύτερα Πανεπιστήμια των ΗΠΑ ανακάλυψαν 13.930.176 κλεμμένα διαπιστευτήρια ηλεκτρονικού ταχυδρομείου τους να πωλούνται από 3,50 έως 10 $ ανά τεμάχιο (Jackson, 2017). Ο κλεμμένος όμως για τους hackers θησαυρός μπορεί κάλλιστα να περιλαμβάνει πνευματική ιδιοκτησία και αξιόλογο ερευνητικό έργο, γεγονός που κάνει την προσπάθεια παραβίασης των συστημάτων τους ακόμα πιο ελκυστική. Στο συμπέρασμα αυτό συνηγορούν και τα Εκπαιδευτικά Ιδρύματα του νομού Θεσσαλονίκης με ποσοστό 70,60% ενισχύοντας έτσι την πεποίθηση ότι ο διαδικτυακός κίνδυνος είναι υπαρκτός και αποτελεί όντως βασική απειλή για αυτά (Καϊμακάμη, 2017).

Όπως παρατηρούμε στο Σχήμα 2, διαχρονικά υπήρξε μία σχετική ύφεση στις παραβιάσεις δεδομένων στην Εκπαίδευση ως ποσοστό προς το σύνολο των παραβιάσεων κατά το διάστημα 2008-2015. Τα τελευταία όμως έτη αυτό το τοπίο αλλάζει με αύξηση του ποσοστού τους από 58% σε 98% για το διάστημα 2015 αρχές του 2016 (Identity Theft Resource Center), ενισχύοντας το γεγονός πως τα Εκπαιδευτικά Ιδρύματα εξακολουθούν να διατηρούν την ελκυστικότητά τους ως στόχοι για τους κακόβουλους χρήστες του διαδικτύου. Επιπρόσθετα, δεδομένου ότι συνήθως υπάρχουν περιορισμένοι μηχανισμοί ελέγχου των ποικίλων τρόπων πρόσβασης στους εσωτερικούς πόρους του πληροφοριακού συστήματος ενός Πανεπιστημίου. Γίνεται κατανοητό πως το δίκτυο τους, αποτελεί ένα πολυσύνθετο πληροφοριακό περιβάλλον όπου μεγάλης αξίας δεδομένα συνδυάζονται με μεγάλη επιφάνεια επίθεσης και προκειμένου να είναι ασφαλές, θα πρέπει ακολουθώντας την εξέλιξη της τεχνολογίας να προσαρμόζεται σε αυτή χρησιμοποιώντας αντίστοιχα μέσα και μέτρα προστασίας (Polyakov, 2017).



Σχήμα 2: Στατιστικά παραβιάσεων στην εκπαίδευση 2005-16.

Δεν θα πρέπει να αμελήσουμε επίσης το γεγονός, ότι στα δίκτυα πολλών πανεπιστημίων υπάρχει η δυνατότητα ασύρματης σύνδεσης από πληθώρα προσωπικού και φοιτητών σε ηλεκτρονικά περιβάλλοντα μάθησης και συνεργασίας, στα οποία τις περισσότερες φορές η σύνδεση γίνεται από ιδιωτική συσκευή. Γίνεται κατανοητό ότι το έργο της προστασίας των Πανεπιστημιακών δικτύων είναι δύσκολο και η εξασφάλισή τους είναι πραγματικά μια πρόκληση (Hammargren et al, 2016). Κατανοώντας τους λόγους που κάνουν τα Πανεπιστημιακά Ιδρύματα ελκυστικά σε κακόβουλους εισβολείς, θα πρέπει να αναφέρουμε παράλληλα και τους λόγους για τους οποίους θεωρούνται πως είναι πιο ευάλωτα, συγκεντρώνοντάς τους στους παρακάτω (Andrus, 2016):

- Μεγάλος μεταβατικός πληθυσμός. Το προσωπικό διδακτικό και διοικητικό, οι φοιτητές και εξωτερικοί συνεργάτες των Ιδρυμάτων μεταβάλλονται διαχρονικά, οπότε στα πληροφοριακά συστήματα φιλοξενείται πληθώρα νέων προσωπικών και οικονομικών δεδομένων η οποία ανανεώνεται συνέχεια.
- Ελευθερία στην πρόσβαση δικτύων και δεδομένων. Βάσει της ελεύθερης ανταλλαγής ιδεών και της άμεση πρόσβασης στην πληροφόρηση, τόσο το προσωπικό όσο και οι υπόλοιποι ενδιαφερόμενοι θα πρέπει να μπορούν να έχουν σε άμεσο χρόνο διαθέσιμες τις πληροφορίες που τους ενδιαφέρουν.
- Αποκεντρωμένα συστήματα δεδομένων. Η χρήση εξωτερικών συσκευών σύνδεσης παράλληλα με τη χρήση ασύρματου δικτύου ακόμα και από διαφορετικές γεωγραφικές τοποθεσίες πρόσβασης, δίνουν τη δυνατότητα σε κάποιον κακόβουλο χρήστη να χρησιμοποιήσει ευάλωτα σημεία συνδέσεων, προκειμένου να διεισδύσει και αυτός στο δίκτυο. Εξάλλου υπάρχει ροή πολλών δεδομένων διαμέσου υπηρεσιών διαδικτύου και σε έναν μεγάλο αριθμό διεπαφών (Alderson, 2015).
- Ανεπαρκής εποπτεία Δικτύου. Τις περισσότερες φορές ούτε το προσωπικό αλλά και ούτε το λογισμικό ενός Πανεπιστημίου αρκεί για να προληφθούν, να εντοπιστούν και αντιμετωπιστούν εγκαίρως τα συμβάντα ασφαλείας..

Δυστυχώς τα Εκπαιδευτικά Ιδρύματα, λόγω της ελευθερίας στην προσβασιμότητα, η οποία επιβάλλεται για την εξυπηρέτηση σκοπών τους, αφήνουν έναν μεγάλο δίαυλο επικοινωνίας ανοιχτό προς όλους και προσπελάσιμο μέσω πολλών μερών και με διαφορετικούς τρόπους. Το γεγονός αυτό όντως ενθαρύνει επίδοξους κακόβουλους χρήστες, οι οποίοι εκμεταλλευόμενοι παράλληλα και ευπάθειες του δικτύου λόγω ανεπαρκών υποδομών, βάζουν ως στόχο τα Εκπαιδευτικά Ιδρύματα προκειμένου να παραβιάσουν τα συστήματά τους και να αποκτήσουν πρόσβαση σε πολύτιμα δεδομένα. Σε έρευνα που διεξήχθη στα Ανώτατα Εκπαιδευτικά Ιδρύματα του Νομού Θεσσαλονίκης, οι συμμετέχοντες υποστήριξαν πως αυτά είναι πιθανώς πιο ευάλωτα σε κυβερνοεπιθέσεις συνδιαστικά: εξαιτίας της εύκολης ηλεκτρονικής πρόσβασης σε αυτά, εξαιτίας της ανεπαρκούς υποδομής προστασίας στον κυβερνοχώρο καθώς και λόγω των νέων συσκευών που

συνδέονται διαχρονικά στο δίκτυό τους. Ο συνδιασμός αυτός των απαντήσεων έλαβε ποσοστό 46,30%, ενώ ακολούθησε με μεγάλη διαφορά 18,4% μόνο, η ανεπάρκεια υποδομών και με 16,9% οι νεές συνδεόμενες συσκευές (Καϊμακάμη, 2017).

Γίνεται κατανοητό, πως ο ρόλος που καλούνται να διαδραματίσουν οι ηγέτες της τεχνολογίας της πληροφορίας είναι πολύ σημαντικός, διότι με την τεχνογνωσία τους και σε στενή συνεργασία με τον υπόλοιπο Πανεπιστημιακό κόσμο, θα μπορέσουν να δημιουργήσουν ένα ουσιαστικό πλέγμα προστασίας των Εκπαιδευτικών Ιδρυμάτων απέναντι στις παραβιάσεις του διαδικτύου και την κλοπή δεδομένων. Εξάλλου με την εφαρμογή του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων G.D.P.R., θα υπάρχει η υποχρεωτική ύπαρξη του υπεύθυνου προστασίας δεδομένων, ο οποίος κάλλιστα μπορεί να βρίσκεται ανάμεσα σε αυτούς. Ο Κανονισμός με την υποχρεωτική εφαρμογή του δημιουργεί ένα νέο πλαίσιο ψηφιακής πραγματικότητας, δίνοντας έμφαση στην ασφάλεια των δεδομένων. Μέσω της δέσμης των μέτρων του προβλέπει και την ενιαία εφαρμογή τους, οριοθετεί την ορθή συμπεριφορά των κρατών αναφορικά με την ασφάλεια στο διαδίκτυο. Συμπεραίνουμε πως με την κατάλληλη τεχνολογική υποδομή των πληροφοριακών συστημάτων, την εκπαίδευση του προσωπικού και με παράλληλη την ανάπτυξη της αποκαλούμενης κουλτούρας ασφαλείας θα μπορέσει ο χώρος των Πανεπιστημίων να εξασφαλιστεί από τις συνεχώς εξελισσόμενες απειλές του κυβερνοχώρου (Vmwareemeablog, 2016).

ΚΟΥΛΤΟΥΡΑ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια στον κυβερνοχώρο αποτελεί υποσύνολο της ασφάλειας των πληροφοριών και αναφέρεται στις πρακτικές που ακολουθούνται προκειμένου να διασφαλιστεί η προστασία δεδομένων, δικτύων και τερματικών του κάθε οργανισμού από πάσης φύσεως παραβιάσεις, ώστε να περιοριστεί η πιθανότητα απώλειας και ζημιών. Οι απειλές στον κυβερνοχώρο όμως δεν αναφέρονται μονάχα στον Οργανισμό ως σύνολο αλλά αφορούν και ξεχωριστά τον κάθε χρήστη του δικτύου του, ο οποίος αν δεν έχει λάβει τη σωστή κατάρτιση και πλήρη ενημέρωση, πιθανό να αποτελέσει τρωτό σημείο στην άμυνα του. Με ποσοστό περίπου 49%, τα ανθρώπινα λάθη θεωρούνται κύρια αιτία των περιστατικών ασφαλείας στον εκπαιδευτικό χώρο, ενώ η εικόνα σχετικά με την αιτία διακοπής λειτουργίας των συστημάτων παραμένει η ίδια και οφείλεται με ποσοστό 54% σε λανθασμένη ή τυχαία δραστηριότητα των ψηφιακών χρηστών. Επισημαίνοντας λοιπόν πως ενδογενείς παράγοντες των ιδρυμάτων αποτελούν την πιο σημαντική απειλή, κατανοούμε το πόσο σημαντική είναι η καλλιέργεια στο εσωτερικό τους της αποκαλούμενης κουλτούρας ασφαλείας (Brooks, 2017).

Η ανάπτυξη κουλτούρας ασφαλείας οδηγεί στην κατανόηση και συνδρομή των χρηστών του διαδικτύου σε θέματα ασφαλείας. Αυτό φυσικά μπορεί να επιτευχθεί, μονάχα μέσω συνεχούς εκπαίδευσης, επαγρύπνησης και ετοιμότητάς τους, δεδομένου πως συνήθως δικές τους πρακτικές, δράσεις ή παραλείψεις οδηγούν σε παραβιάσεις του δικτύου πληροφοριών. Για να

καταλάβουμε τη σημασία του ανθρώπινου παράγοντα στον διαδικτυακό κίνδυνο, αξίζει να αναφέρουμε πως το 52% των παραβιάσεων ασφαλείας οφείλεται συνήθως σε ανθρώπινο λάθος (Thibodeaux, 2016), ενώ απειλή για τα Εκπαιδευτικά Ιδρύματα θεωρούνται με μεγαλύτερο ποσοστό οι ίδιοι οι υπάλληλοι με ποσοστό 77% παρά εξωτερικοί εισβολείς, λόγω την αδυναμίας ελέγχου ή παρακολούθησης της δραστηριότητάς τους καθώς και εξαιτίας της ανεπαρκούς εκπαίδευσής τους. Παράλληλα, μεγάλο πρόβλημα αποτελεί η έλλειψη κονδυλιών σχετικά με την ασφάλεια δικτύων, η οποία δεν θα πρέπει να αναφέρεται μόνο στην περιμετρική ασφάλεια των δικτύων αλλά να επικεντρώνεται και στην ασφάλεια καθ' αυτών των δεδομένων (Bolkan, 2017).

Γίνεται κατανοητό, πως οι χρήστες θα πρέπει αρχικά να γνωρίζουν και να εφαρμόζουν τους βασικούς απλούς κανόνες ασφαλούς πλοήγησης στο διαδίκτυο και παράλληλα να είναι σε θέση να αναγνωρίσουν και να αντιμετωπίσουν τις πιθανές διαδικτυακές απειλές. Σημαντικό είναι το γεγονός πως μόνο το 25,4% των εκπαιδευτικών, δικοικητικού προσωπικού και συνεργατών των Πανεπιστημίων της Θεσσαλονίκης έχει παρακολουθήσει κάποιο σεμινάριο ή είχε οποιαδήποτε ενημέρωση πάνω σε θέματα ασφαλούς πλοήγησης στο διαδίκτυο. Αυτό είναι ιδιαίτερα αποθαρυντικό, δεδομένου πως οι περισότερες παραβιάσεις δεδομένων οφείλονται συνήθως σε ανθρώπινα λάθη των ίδιων των εξουσιοδοτημένων και πιστοποιημένων χρηστών (Καϊμακάμη, 2017). Κατανοούμε λοιπόν, πως θα πρέπει να υπάρξει μία μέριμνα από μέρους των οργάνων διοίκησης των Ανώτατων Εκπαιδευτικών Ιδρυμάτων, ώστε να καλυφτεί αυτό το κενό στη γνώση και να δημιουργηθεί όπως πολλές φορές έχουμε τονίσει, η κουλτούρα ασφάλειας. Από τις απλές τακτικές, όπως η συχνή αλλαγή και χρήση ενός ισχυρού κωδικού πρόσβασης μέχρι την εφαρμογή του συνόλου των κανόνων της στρατηγικής του Οργανισμού σε θέματα κυβερνοασφαλείας, όπως αυτή εκφράζεται μέσω της υιοθέτησης μιας υγιούς διαδικτυακής συμπεριφοράς, ενισχύει σε κάθε περίπτωση το επίπεδο άμυνάς του, ενώ ουσιώδους σημασίας είναι σε περίπτωση ενός αναπόφευκτου συμβάντος ασφαλείας της ύπαρξης του σχεδίου απόκρισης περιστατικών.

ΣΧΕΔΙΟ ΑΠΟΚΡΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ

Σημαντικό ρόλο στην αντιμετώπιση μιας πιθανής κυβερνοεπίθεσης διαδραματίζει το σχέδιο απόκρισης περιστατικών το οποίο εφαρμόζεται στην περίπτωση που τα προληπτικά μέτρα ασφαλείας κριθούν αναποτελεσματικά και υπάρξει επιτυχής παραβίαση των ηλεκτρονικών συστημάτων. Με τον όρο απάντηση ή απόκριση σε περιπτώσεις συμβάντων ασφαλείας, αναφερόμαστε σε μία οργανωμένη προσέγγιση προκειμένου να γίνει δυνατό να διαχειριστούν καλύτερα οι επιβλαβείς συνέπειες μιας κυβερνοεπίθεσης. Βασικός και κύριος στόχος κάθε σχεδίου αντιμετώπισης τέτοιων έκτακτων περιστατικών, είναι αρχικά να περιοριστούν όσο το δυνατόν οι συνέπειες του «συμβάντος» και να είναι άμεση η ανάκτηση των δυνάμεων του Οργανισμού, επιχείρησης αλλά και Ιδρύματος, οι οποίοι θα πρέπει να είναι σε θέση να συνεχίσουν απρόσκοπτα τη δραστηριότητά τους. Στο σχέδιο αυτό περιλαμβάνονται αναλυτικά διευκρινίσεις

σχετικά με το πως ορίζεται το κάθε περιστατικό, οι διαδικασίες που ακολουθούνται και η πολιτική που εφαρμόζεται προκειμένου να ελαχιστοποιηθεί το κόστος απόκρισης (Μαυρίδης, 2015).

Είναι πολύ σημαντικός τόσο ο έγκαιρος εντοπισμός όσο και η άμεση και αποτελεσματική απόκριση στο συμβάν ασφαλείας. Το μεσοδιάστημα αυτό είναι κρίσιμο διοτί δεδομένα που παραμείνουν εκτεθημένα για μακρύ χρονικό διάστημα μπορούν να οδηγήσουν σε κάθετη αύξηση του κόστους και των συνεπειών σε όλα τα επίπεδα. Αξίζει να αναφέρουμε την περίπτωση παραβίασης των συστημάτων της Ιατρικής Σχολής του Πανεπιστημίου της Ουάσιγκτον, όπου υπάλληλος λαμβάνοντας μήνυμα ηλεκτρονικού ψαρέματος και απαντώντας σε αυτό, επέτρεψε να διεισδύσει στο δίκτυο κακόβουλος χρήστης, ο οποίος απέκτησε πρόσβαση στα δεδομένα 80.000 ασθενών και τα προσωπικά δεδομένα των υπαλλήλων του Ιδρύματος. Αν και το ηλεκτρονικό μήνυμα παραδόθηκε στις 2 Δεκεμβρίου του 2016, η εισβολή δεν εντοπίστηκε άμεσα και η Ιατρική Σχολή ενημερώθηκε για την επίθεση μόλις στις 24 Ιανουαρίου του επόμενου έτους (Freedman, 2017). Αντιλαμβανόμαστε πως ένα τέτοιο συμβάν επηρεάζει κόστη σε διάφορα επίπεδα,όπως οικονομικά, κόστη ειδοποιήσεων,αλλά και έμμεσα κόστη όπως το αντίκτυπο στη φήμη του Πανεπιστημίου.

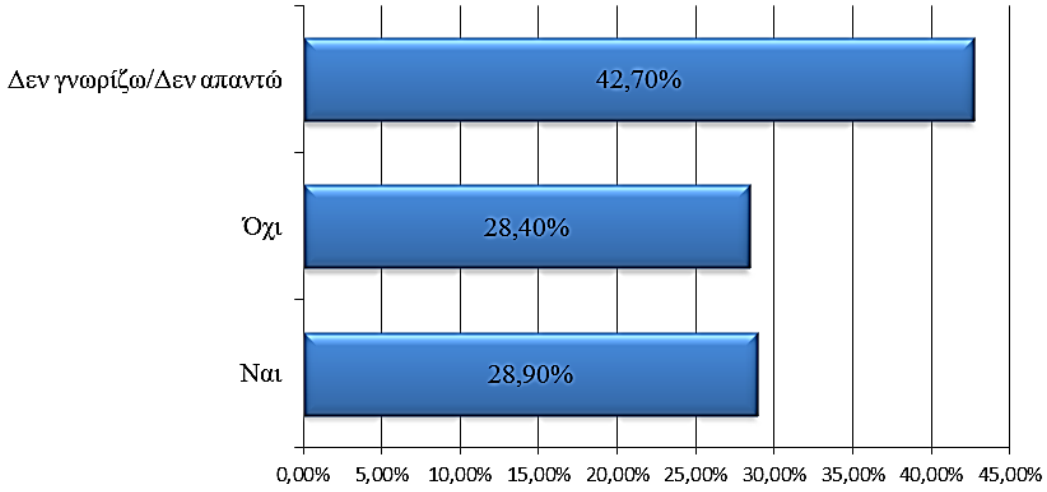
Πρέπει να υπογραμμιστεί πως το σχέδιο απόκρισης περιστατικών θα πρέπει πάντα πρέπει να συμβαδίζει με όλη την στρατηγική ασφάλειας στον κυβερνοχώρο, περιλαμβάνοντας ένα σύνολο εργαλείων και τακτικών που εξασφαλίζουν την αποτελεσματικότερη απόκριση σε οποιαδήποτε απειλή των πληροφοριακών συστημάτων. Σε αυτήν την απόκριση είναι ουσιώδους σημασίας η ετοιμότητα τόσο των συστημάτων, όσο και ανθρώπινη εγρήγορση, η οποία είναι απαραίτητη ώστε να περιοριστεί άμεσα το συμβάν και να ελαχιστοποιηθούν τα διάφορα κόστη που αυτό προκαλεί (O' Boyle, 2017). Συγκεκριμένα, κάθε σχέδιο αντιμετώπισης περιστατικών ασφαλείας σε ένα Εκπαιδευτικό Ίδρυμα θα πρέπει να είναι οργανωμένο σωστά και οφείλει να περιλαμβάνει τα παρακάτω ενδεικτικά ουσιώδη στοιχεία:

- Βεβαιωνόμαστε ότι υπάρχει σχέδιο επιχειρησιακής συνέχειας, στο οποίο να περιγράφονται οι διαδικασίες αποκατάστασης της λειτουργίας των συστημάτων μετά από πιθανή παραβίαση..
- Αναπτύσσουμε σχέδιο επικοινωνίας προκειμένου να υπάρχει δίαυλος ενημέρωσης για όλα τα συνεργαζόμενα μέρη.
- Παρέχουμε συνεχή κατάρτιση του προσωπικού σε θέματα σχετικά με τους κινδύνους στο κυβερνοχώρο.
- Τηρούμε πάντα αντίγραφα ασφαλείας και γνωστοποιούμε σε όλους τον τρόπο ανάκτησης των αρχείων από αυτά.
- Καθιστούμε γνωστό τον τρόπο εντοπισμού και τις μεθόδους αντιμετώπισης ενός συμβάντος ασφαλείας. Στην προσπάθεια να καταπολεμηθεί το κακόβουλο λογισμικό, οι δείκτες συμβιβασμού, παρέχουν πολύ σημαντική βοήθεια, αυξάνοντας κατά πολύ τα ποσοστά έγκαιρης ανίχνευσης κακόβουλων παραβιάσεων και

βελτιώνοντας εξαιρετικά τους χρόνους απόκρισης στα διάφορα συμβάντα ασφαλείας (Lord, 2017).

- Κάνουμε πρακτική εφαρμογή του σχεδίου αντιμετώπισης περιστατικών ασφαλείας. Εφόσον έχει καταρτιστεί ένα ολοκληρωμένο σχέδιο αντιμετώπισης περιστατικών, αυτό θα πρέπει να δοκιμαστεί ως προς την λειτουργικότητά του.

Οφείλουμε να αναφερθούμε επίσης στην ασφάλιση του διαδικτυακού κινδύνου, που αποτελεί έναν συνεχώς αναπτυσσόμενο κλάδο στον τομέα των ασφαλίσεων. Η παροχή υπηρεσιών από κάποιον επαγγελματία του χώρου, μπορεί να είναι στην περίπτωση του κινδύνου διαδικτύου μία έξυπνη λύση προκειμένου να εξασφαλιστεί σε διάφορα επίπεδα ο Οργανισμός σε περίπτωση μιας κακόβουλης εισβολής. Αποτελεί ένα χρήσιμο εργαλείο διαχείρισης αλλά και μεταφοράς του κινδύνου, δεδομένου ότι τα ασφαλιστικά προϊόντα καλύπτουν την επιχείρηση σε οικονομικό επίπεδο και αναλαμβάνουν την υλοποίηση του πλάνου αντιμετώπισης των περιστατικών.



Σχήμα 3: Γνώση ύπαρξης σχεδίου απόκρισης περιστατικών στο Ίδρυμα όπου εργάζονται.

Δυστυχώς αναφορικά με το σχέδιο απόκρισης περιστατικών όπως φαίνεται και στο Σχήμα 3, τα Ανώτατα Εκπαιδευτικά Ιδρύματα του νομού Θεσσαλονίκης δηλώνουν σε μεγάλο ποσοστό άγνοια, αφού τα τρία τέταρτα των ερωτηθέντων απάντησαν πως είτε δεν γνωρίζουν είτε δεν απαντούν σχετικά με την ύπαρξη σχεδίου απόκρισης στο Εκπαιδευτικό Ίδρυμά τους. Έχουμε τονίσει πως κατά την κατάρτιση του σχεδίου θα πρέπει να προβλεφθεί η ενημέρωση των εμπλεκομένων, ώστε να υπάρχει μία ομοιόμορφη σχεδιασμένη αντίδραση προκειμένου να περιοριστεί ο αντίκτυπος μιας κυβερνοεπίθεσης και κάτι τέτοιο δεν εκφράζεται μέσω των συγκεκριμένων απαντήσεων. Ακολουθούν με σχεδόν ίδια ποσοστά οι υπόλοιπες απαντήσεις, αφού μέσω του 28,90% των συμμετεχόντων εκφράστηκε πως υπάρχει η πρόβλεψη ενός σχεδίου απόκρισης, ενώ αντίθετα αρνητικά απάντησε το υπόλοιπο 28,40%.

Στο σημείο αυτό θα αναφερθούμε στα γεγονότα της επικίνδυνης παγκόσμιας κυβερνοεπίθεσης που έπληξε στις 12 Μαΐου του 2017, κολοσσούς όπως η Fedex, Renault, Nissan, περισσότερα των 4.000 Εκπαιδευτικών Ερευνητικών Ιδρυμάτων στην Κίνα και Πανεπιστήμια της Ιταλίας, ενώ ανάμεσα σε αυτούς στόχο αποτέλεσε και το Αριστοτέλειο Πανεπιστήμιο της Θεσσαλονίκης. Ο ιός ονομαζόταν WannaCry και εκμεταλλευόμενος κενά ασφαλείας των Windows παρέλυσε υπολογιστές κρυπτογραφώντας τα αρχεία τους και απαιτώντας λύτρα για την επαναφορά τους. Στο Αριστοτέλειο Πανεπιστήμιο η παραβίαση εντοπίστηκε στο Κέντρο Ηλεκτρονικής Διακυβέρνησης καθώς πολλοί χρήστες ανακάλυψαν κρυπτογραφημένα αρχεία τους ενώ κάποια άλλα είχαν αφαιρεθεί. Υπήρξε επίσημη ανακοίνωση για το συμβάν στους εμπλεκόμενους το ίδιο απόγευμα, ενώ το Α.Π.Θ με την έγκαιρη με επέμβαση των υπευθύνων για την ασφάλεια των δικτύων εξάλειψε τον κίνδυνο μέσα σε 4 ώρες και 31 λεπτά από την στιγμή της κυβερνοεπίθεσης. Ακολούθως το επόμενο πρωί ενημερώθηκε και το τμήμα δίωξης Ηλεκτρονικού Εγκλήματος. Όπως η ιστορία απέδειξε, το Α. Π. Θ. χάρη στο άρτια οργανωμένο τμήμα ηλεκτρονικής διακυβέρνησης και ακολουθώντας τα βήματα απόκρισης περιστατικών, αποτελεί χαρακτηριστικό παράδειγμα άμεσης και αποτελεσματικής αντιμετώπισης ενός συμβάντος ασφαλείας, επιτυγχάνοντας στο μέγιστο τον περιορισμό του κινδύνου (PC.MAG, 2017; Documento.news, 2017).

Η ανταπόκριση των ερωτηθέντων σχετικά με την στάση που ακολούθησε το Ίδρυμά τους μετά το συγκεκριμένο περιστατικό ασφαλείας ήταν η εξής: ποσοστό 42,8% των ερωτηθέντων υποστήριξε πως το Εκπαιδευτικό Ίδρυμα όπου ανήκαν έλαβε επιπλέον μέτρα ασφαλείας, ενώ αντίθετα, ποσοστό της τάξης του 48,3% των ερωτηθέντων απάντησε πως κανένα επιπλέον μέτρο δεν λήφθηκε από την διοίκηση του Ιδρύματός τους. Τέλος με ποσοστό 8,9% οι συμμετέχοντες απάντησαν πως είτε δεν γνώριζαν αν υφίσταται όντως τέτοιο περιστατικό, είτε πως δεν ήξεραν αν υπήρξαν επιπλέον μέτρα ασφαλείας κ.α.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Ανεξάρτητα από το πόσο καλά είναι σχεδιασμένο ένα δίκτυο πάντοτε θα προκύπτουν θέματα ανθεκτικότητάς του απέναντι στον κυβερνοκίνδυνο. Ο κάθε Οργανισμός θα πρέπει να είναι σε θέση να σχεδιάζει σωστά την ασφάλεια των συστημάτων του, εφαρμόζοντας πρακτικές που θα του επιτρέπουν να εντοπίζει, να αξιολογεί και να διαχειρίζεται τις απειλές, εξασφαλίζοντας με τον τρόπο αυτό την απρόσκοπτη συνέχεια των εργασιών του. Τα Ανώτατα Εκπαιδευτικά Ιδρύματα της Θεσσαλονίκης, όπως εξάλλου και όλοι οι υπόλοιποι Οργανισμοί, Ιδύματα και επιχειρήσεις, καλούνται να βρίσκονται σε εγρήγορση σχετικά με θέματα που αφορούν τον διαδικτυακό κινδύνο και η οποιαδήποτε προσπάθεια ευαισθητοποίησης θα πρέπει να ξεκινήσει από τα όργανα διοίκησής τους. Μέσω των αποτελεσμάτων της έρευνας διαπιστώθηκε η σημασία η οποία δίνεται στον διαδικτυακό κίνδυνο, όμως παράλληλα και η ελλιπής ενημέρωση αλλά και ετοιμότητα των Πανεπιστημιακών Ιδρυμάτων να αντιμετωπίσουν θέματα ασφαλείας.

Επιβάλλεται να γίνει προσπάθεια ενημέρωσης του προσωπικού των Ιδρυμάτων και σε όσα δεν υπάρχει ήδη, να καταρτιστεί ένα οργανωμένο σχέδιο στρατηγικής απέναντι στον κυβερνοκίνδυνο.

Η υιοθέτηση διαδικασιών ψηφιοποίησης και διαχείρισης των πληροφοριών θα ενέχει πάντα τον κίνδυνο της πιθανής παραβίασής τους. Οι μέθοδοι και οι πρακτικές διείσδυσης στα πληροφοριακά δίκτυα από μέρους κακόβουλων χρηστών, πολλαπλασιάζονται και εξελίσσονται. Τα Εκπαιδευτικά Ιδρύματα, θα πρέπει να είναι πάντα σε ετοιμότητα, ώστε στην περίπτωση που η παραβίαση δεδομένων είναι αναπόφευκτη, να εξασφαλίσουν τις προϋποθέσεις ανάκαμψής τους και να εφαρμόσουν τις ορθές πρακτικές αντιμετώπισης του συμβάντος. Συνειδητοποιώντας επίσης τη σημασία του κινδύνου, θα πρέπει να διαθέσουν περισσότερο χρόνο, πόρους και προσπάθεια για την προστασία των πληροφοριακών τους συστημάτων, υιοθετώντας μια αποτελεσματική στρατηγική διαχείρισής τους, δεδομένου πως εκτός των οικονομικών επιπτώσεων στα Εκπαιδευτικά Ιδρύματα, διακυβεύεται και η ίδια η φήμη τους.

Ο καθένας μας μπορεί να πέσει θύμα κυβερνοεπίθεσης και τα ποσοστά συμφωνούν πλειοψηφικά πως η πιθανότητα αυτή είναι εξαιρετικά μεγάλη, αφού το 93,5% των Ανώτατων Εκπαιδευτικών Ιδρυμάτων της Θεσσαλονίκης απάντησε καταφατικά. Τα υπάρχοντα συστήματα και προγράμματα ασφαλείας μπορεί πιθανώς να μην επαρκούν, καθώς η εποπτεία σε έναν τόσο μεγάλο χώρο με πολυπληθείς τρόπους και μέσα πρόσβασης είναι δύσκολο έργο, έτσι θα πρέπει ο καθένας από τους χρήστες των συστημάτων, χωριστά και με τον τρόπο του να συμβάλει στην οικοδόμηση ενός ασφαλούς Ακαδημαϊκού πληροφοριακού δικτύου (Amigorena, 2017).

ΒΙΒΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Καϊμακάμη Ν., (2017), Ο διαδικτυακός κίνδυνος στα Ανώτατα Εκπαιδευτικά Ιδρύματα, η ανάγκη προστασίας τους από απειλές στον ψηφιακό κόσμο και η πρόκληση συμμόρφωσης στον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων. Έρευνα στα Ανώτατα Εκπαιδευτικά Ιδρύματα του Νομού Θεσσαλονίκης, Μεταπτυχιακή Εργασία, Σχολή Οικονομίας και Διοίκησης, Α.Τ.Ε.Ι. Θεσσαλονίκης

Μαυρίδης Ι., (2015), Πληροφορική Θεωρία της πληροφορίας και της επικοινωνίας Κρυπτογραφία, Αρχές ανάπτυξης λογισμικού Γλώσσες προγραμματισμού Τεχνολογίες παγκόσμιου ιστού, Κεφ. 12, Απόκριση σε συμβάντα & Digital Forensics, Μεταπτυχιακή Εργασία, Πανεπιστήμιο Μακεδονίας

Documento news, (13/05/2017), Ασήμαντες οι ζημιές στο ΑΠΘ από την κυβερνοεπίθεση. Ανακτήθηκε στις 10/08/2017 από την ιστοσελίδα http://www.documentonews.gr/article/ashmantes-oi-zhmies-sto-apo-apo-thn-kybernoepithesh

PC. MAG, (16/05/2017), WannaCry: Το χρονικό της μεγαλύτερης κυβερνοεπίθεσης στην ιστορία. Ανακτήθηκε στις 05/11/2017 από την ιστοσελίδα http://gr.pcmag.com/wannacry/26656/feature/wannacry-to-khroniko-tes-megaluteres-kubernoepitheses-sten-i

Abhay R., Fahad K., Seyed H., Krishna A. (25/08/2016), Cybersecurity in higher education: the changing threat landscape.Ανακτήθηκε στις 12/06/2017 από την ιστοσελίδα https://consulting.ey.com/cybersecurity-in-higher-education-the-changing-threat-landscape/

Alderson J., (03/03/2015), How Safe is Your Student Data? Data Privacy Implications for Higher Education. Ανακτήθηκε στις 06/06/2017 από την ιστοσελίδα http://www.adventures.com/2015/03/how-safe-is-your-student-data-data-privacy-implications-for-higher-education/

Amigorena F., (24/04/2017), An education in avoiding data breaches in schools, colleges, and universities. Ανακτήθηκε στις 20/09/2017 από την ιστοσελίδα https://www. itgovernanceusa. com/blog/an-education-in-avoiding-data-breaches-in-schools-colleges-and-universities/

Andrus F., (02/08/2016), Why Hackers Go After Universities.Ανακτήθηκε στις 15/06/2017 από την ιστοσελίδα https://www. bradfordnetworks. com/hackers-go-universities/

Beasley breach insights, (23/01/2017), Ransomware attacks soar in 2016, projected to double again in 2017. Ανακτήθηκε στις 09/09/2017 από τη διεύθυνση https://www. beazley. com/Documents/Insights/201701-beazley-breach-insights-us. pdf

Biener Ch., Eling M., Wirfs H., (2015), Insurability of Cyber Risk: An Empirical Analysis, Working Papers on Risk Management and Insurance. Geneva Papers on Risk and Insurance, Vol. 40 No. 151, January 2015,University of St. Gallen, School of Finance Research Paper No. 2015/03.Ανακτήθηκε στις 21/07/2017 από τη διεύθυνση https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf

Bolkan J., (08/09/2017), Most Ed Institutions Unprepared for Data Risks. Ανακτήθηκε στις 03/11/2017 από την ιστοσελίδα https://campustechnology.com/articles/2017/09/08/most-ed-institutions-unprepared-for-data-risks.aspx

Brooks R., (05/09/2017), Top security risks in education.Ανακτήθηκε στις 10/11/2017 από την ιστοσελίδα https://blog. netwrix. com/2017/09/05/infographics-top-cybersecurity-risks-in-education/

Cebula J., Young L.R., Taxonomy of Operational Cyber Security Risks, TECHNICAL NOTE. CMU/SEI-2010-TN-028. CERT® Program, Carnegie Mellon University, December 2010.Ανακτήθηκε στις 12/11/2017 από τη διεύθυνση http://www.sei.cmu.edu/reports/10tn028.pdf

Jackson K., (29/03/2017), Millions of Stolen US University Email Credentials for Sale on the Dark Web. Ανακτήθηκε στις 01/04/2017 από την ιστοσελίδα https://www. darkreading. com/threat-intelligence/millions-of-stolen-us-university-email-credentials-for-sale-on-the-dark-web--/d/d-id/1328511

Lord N., (27/07/2017), What are indicators of compromise? Ανακτήθηκε στις 14/09/2017, από την ιστοσελίδα https://digitalguardian. com/blog/what-are-indicators-compromise

Freedman L., (13/04/2017), Washington University School of Medicine Victim of Phishing Attack, Posted in health information privacy,hipaa and health information. Ανακτήθηκε στις 05/08/2018 από την ιστοσελίδα https://www. dataprivacyandsecurityinsider. com/2017/04/washington-university-school-of-medicine-victim-of-phishing-attack/

Fulbright Norton Rose Report, (2016), Cyber Risks and Insurance.An Introduction to Cross Class Cyber Liabilities, International Underwriting Association of London Limited. First Published: January 2016.Ανάκτηση στις 20/10/2017 από τη διεύθυνση http://www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf

Identity Theft Resource Center. Ανακτήθηκε στις 05/08/2017 από τη διεύθυνση
http://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf

O' Boyle T., (19/06/2017), Stay Ahead of Security Threats with a 7-Step Incident Response Plan. Ανακτήθηκε στις 04/09/2017 από τη διεύθυνση https://er.educause.edu/blogs/2017/6/stay-ahead-of-security-threats-with-a-7-step-incident-response-plan

Polyakov A., (11/08/2017), What Cyberthreats Do Higher Education Institutions Face. Ανακτήθηκε στις 22/09/2017 από τη διεύθυνση https://www.forbes. com/sites/forbestechcouncil/2017/08/21/what-cyberthreats-do-higher-education-institutions-face/#60d08ae1640d

Privacy Rights Clearinghouse Breach Subtotal, Organization type Education rates Ανακτήθηκε στις 07/04/2018 από τη διεύθυνση https://www. privacyrights. org/data-breaches?title=&org_type%5B%5D=259

Roman J., (03/02/2015), Universities: Prime Breach Targets, Maintaining a Culture of Openness While Mitigating Cyberthreats. Ανακτήθηκε στις 10/08/2017 από τη διεύθυνση https://www.databreachtoday. asia/universities-prime-breach-targets-a-7865

Thibodeaux T., (09/03/2016), Cybersecurity training for a multigenerational workforce. Ανακτήθηκε στις 10/08/2017 από τη διεύθυνση https://www.cio.com/article/3041070/security/cybersecurity-training-for-a-multigenerational-workforce. html

Hammargren L.R., Harris E.Ch. (06/09/2016), Higher education's vulnerability to cyber-attacks, Establishing a Written Information Security Program to address exposure, Ανακτήθηκε στις 10/10/2017 από την ιστοσελίδα https://www. universitybusiness. com/article/0816-wisp

Vmwareemeablog, (21/03/2016), The University Challenge – How to Protect Higher Education Institutions from Cyber Crime. Ανακτήθηκε στις 06/07/2017 από τη διεύθυνση http://vmwareemeablog. com, http://vmwareemeablog. com/uk/the-university-challenge-how-to-protect-higher-education-institutions-from-cyber-crime/

ΠΑΡΑΡΤΗΜΑ

ΜΕΘΟΔΟΛΟΓΙΑ ΈΡΕΥΝΑΣ ΣΤΑ ΑΝΩΤΑΤΑ ΕΚΠΑΙΔΕΥΤΙΚΑ ΙΔΡΥΜΑΤΑ ΤΟΥ ΝΟΜΟΥ ΘΕΣΣΑΛΟΝΙΚΗΣ

Η έρευνα στην οποία βασίζονται τα στοιχεία της παρούσας εργασίας έλαβε χώρα το δίμηνο Οκτωβρίου-Νοεμβρίου 2017 και σε αυτήν συμμετείχαν τα Δημόσια Ανώτατα Εκπαιδευτικά Ιδρύματα του Νομού Θεσσαλονίκης. Συγκεκριμένα η φόρμα του ερωτηματολογίου της έρευνας απεστάλη μέσω ηλεκτρονικού ταχυδρομείου σε προσωπικό των σχολών του Αριστοτελείου Πανεπιστημίου της Θεσσαλονίκης, του Πανεπιστημίου Μακεδονίας, του Αλεξάνδρειου Τεχνολογικού Ιδρύματος Θεσσαλονίκης και του Διεθνούς Πανεπιστημίου. Στην έρευνα δεν συμμετείχε το προσωπικό της Α.Σ.ΠΑΙ.ΤΕ Θεσσαλονίκης και του Ανοιχτού Πανεπιστημίου καθώς το μόνιμο προσωπικό τους στον Νομό, δεν επαρκούσε ώστε το δείγμα να είναι αντιπροσωπευτικό. Οι ηλεκτρονικές διευθύνσεις που συλλέχτηκαν υπήρχαν διαθέσιμες στις ιστοσελίδες των κατά τόπους αντίστοιχων σχολών των Ιδρυμάτων, οι απαντήσεις ήταν ανώνυμες και τονίστηκε με σαφή τρόπο στους συμμετέχοντες πως η έρευνα ήταν απολύτως εμπιστευτική.

Το ερωτηματολόγιο της έρευνας απευθύνθηκε σε Ακαδημαϊκό προσωπικό όλων των Εκπαιδευτικών βαθμίδων, εργαστηριακό προσωπικό, ειδικό επιστημονικό προσωπικό, βοηθητικό προσωπικό, συνεργάτες καθώς και διοικητικό προσωπικό και είχε ως θέμα: «Ο διαδικτυακός κίνδυνος στα Ανώτατα Εκπαιδευτικά Ιδρύματα, η ανάγκη προστασίας τους από απειλές στον ψηφιακό κόσμο και η πρόκληση συμμόρφωσης στον Γενικό Κανονισμό Προστασίας Δεδομένων». Συνολικά εκ των περίπου 600 ηλεκτρονικών μηνυμάτων που εστάλησαν, ελήφθησαν 200 συμπληρωμένα ερωτηματολόγια, αριθμός ο οποίος κρίθηκε ικανοποιητικός προκειμένου τα συμπεράσματα να είναι αντιπροσωπευτικά για να εκφράσουν τις τάσεις και τις απόψεις τους τη συγκεκριμένη χρονική στιγμή.

Ο σχεδιασμός του ερωτηματολογίου της έρευνας έγινε στις δωρεάν φόρμες του Google οι οποίες παρείχαν ικανοποιητικές δυνατότητες για τη σύνταξη και μορφοποίησή του, αυτόματη αποθήκευση των αποτελεσμάτων σε αρχεία δεδομένων Excel, καθώς και οπτικοποίησή τους μέσω γραφημάτων. Το περιεχόμενο των ερωτήσεων ήταν αποτέλεσμα της συστηματικής βιβλιογραφικής ανασκόπησης που πραγματοποιήθηκε στο κυρίως μέρος της εργασίας. Μέσα από ανάλογες έρευνες που πραγματοποιήθηκαν σε αντίστοιχα ζητήματα, καθώς και μέσα από πλούσια αρθρογραφία, προέκυψαν οι ερωτήσεις που κλήθηκαν οι συμμετέχοντες να απαντήσουν. Για την μεθοδολογία της έρευνας χρησιμοποιήθηκε μη πιθανοτική δειγματοληψία ευκαιρίας, οπότε και συγκεντρώθηκε το δυνατό μεγαλύτερο δείγμα προσωπικού μέσω των διαθέσιμων ηλεκτρονικών διευθύνσεων. Επιπλέον στους ερωτηθέντες προτάθηκε να προσκαλέσουν και οι ίδιοι κάποιον συνάδελφό τους που θα ήταν πιθανώς πρόθυμος να συμπληρώσει το ερωτηματολόγιο (χιονοστιβάδα).

Το ερωτηματολόγιο χωρίστηκε σε δύο σκέλη, στο πρώτο οι ερωτηθέντες κλήθηκαν θα απαντήσουν σε 6 γενικές ερωτήσεις (δημογραφικά στοιχεία) ενώ ακολούθως στο κυρίως μέρος το ερωτηματολόγιο απαρτίστηκε από 14 ερωτήσεις που αφορούσαν το συγκεκριμένο ζητούμενο της έρευνας. Ενδεικτικά αναφέρουμε τις παρακάτω: Χρησιμοποιείτε υπολογιστή στο χώρο εργασίας σας? Κατά την προσωπική σας άποψη ο διαδικτυακός κίνδυνος αποτελεί μια σημαντική σύγχρονη απειλή για τις περισσότερες επιχειρήσεις, οργανισμούς και Ιδρύματα στον κόσμο? Ποιος νομίζετε πως είναι ο κύριος λόγος που τα Εκπαιδευτικά Ιδρύματα μπαίνουν στο στόχαστρο κυβερνοεπιθέσεων? Γνωρίζετε αν υπάρχει στο Εκπαιδευτικό Ίδρυμα όπου εργάζεστε κάποιο Σχέδιο Ασφαλείας που να περιλαμβάνει τις διαδικασίες που ακολουθούνται σε περιπτώσεις παραβίασης των συστημάτων?

Το είδος των ερωτήσεων που χρησιμοποιήθηκε ήταν κλειστού τύπου, αρκετές πολλαπλής επιλογής και μία ερώτηση με διατάξιμες απαντήσεις με τη μορφή στοιχείου Likert. Η επιλογή των ερωτήσεων κλειστού τύπου δεν ήταν τυχαία καθώς απαιτείται λιγότερος χρόνος για την συμπλήρωσή τους και επιπλέον μέσω των απαντήσεων σε ερωτήσεις τέτοιου τύπου είναι πιο εύκολη η σύγκριση των απαντήσεων και κατ' επέκταση εξάγονται ασφαλέστερα αποτελέσματα.

ΤΟ ΧΡΟΝΙΚΟ ΤΗΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗΣ ΣΤΟ ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

Στο σημείο αυτό παραθέτουμε το χρονολόγιο των γεγονότων της επικίνδυνης κυβερνοεπίθεσης που έπληξε παγκοσμίως οργανισμούς Ιδρύματα και επιχειρήσεις στην αρχή της χρονιάς, ανάμεσα στους οποίους συγκαταλέχθηκε και το Α. Π. Θ. Τα στοιχεία που παραθέτονται έχουν συλλεχθεί από συνεντεύξεις που δοθήκαν από τον αντιπρύτανη Έρευνας του ΑΠΘ κ. Λαόπουλο και τον τεχνικό διευθυντή του Κέντρου Ηλεκτρονικής Διακυβέρνησης κ. Σαλματζίδη.

Το πρώτο κρούσμα της επίθεσης καταγράφηκε στο Λονδίνο την Παρασκευή 12 Μαΐου 2017, στις 10:24 π. μ. (ώρα Ελλάδος) και ξεκίνησε να μεταδίδεται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (PC. MAG, 2017). Η παραβίαση εντοπίστηκε στις 11:29 πμ. στο Κέντρο Ηλεκτρονικής Διακυβέρνησης του Αριστοτελείου Πανεπιστημίου, καθώς πολλοί χρήστες της πλατφόρμας κατήγγειλαν το συμβάν, αφού διαπίστωσαν συμπτώματα παραβίασης των αρχείων τους. Διαπιστώθηκε αλλοίωση δεδομένων μέσω κρυπτογράφησης σε αφαιρούμενα μέσα αποθήκευσης που ήταν συνδεδεμένα στο δίκτυο και παράλληλα αφαιρέθηκαν κάποια αρχεία φακέλων τους (Documento.news, 2017).

Οι εμπλεκόμενοι χρήστες των υπολογιστών ενημερώθηκαν για το συμβάν μετά τις 16:00 μμ. με ειδική ανακοίνωση από το Κέντρο Ηλεκτρονικής Διακυβέρνησης, στο οποίο δίνονταν και οδηγίες αντιμετώπισής του. Διευκρινίστηκε επίσης πως το είδος που κακόβουλου λογισμικού από το οποία προσβλήθηκε το σύστημα ήταν το Ransomware με το όνομα WannaCry. Ο ιός WannaCry, εκμεταλλευόμενος κενά ασφαλείας των Windows (πρωτόκολλο

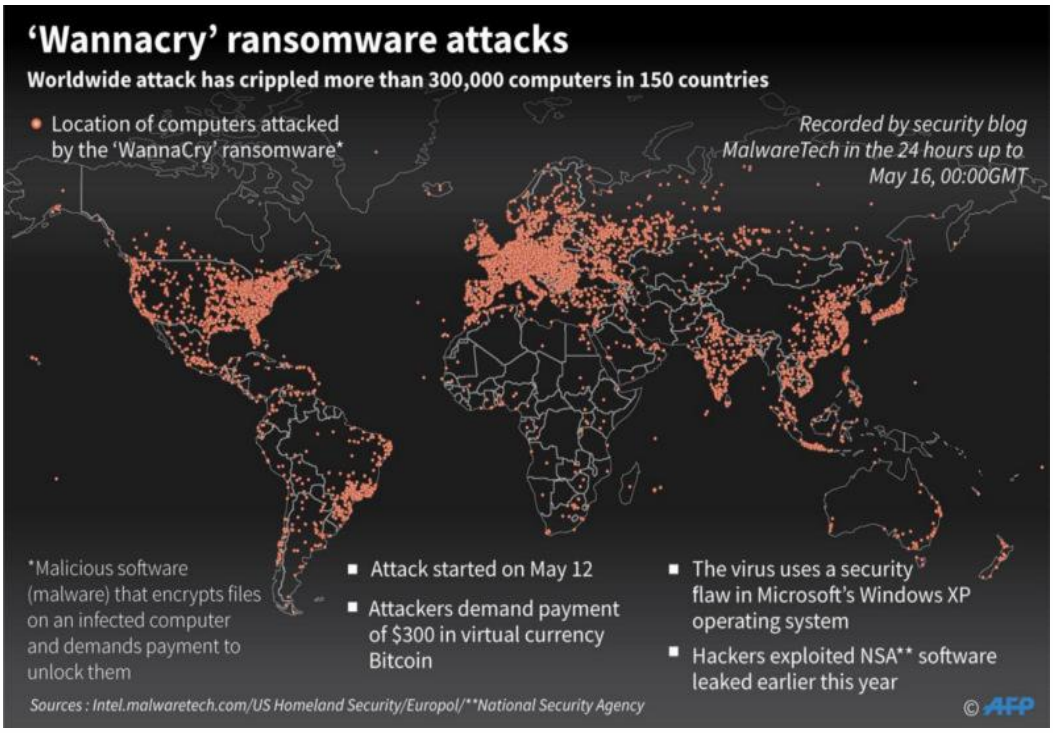
SBM) παρέλυσε τους υπολογιστές κρυπτογραφώντας τα αρχεία τους και απαιτώντας λύτρα για την επαναφορά τους, το ύψος των οποίων ξεκίνησε από τα 300 έφτασε μέχρι και τα 1. 200 δολάρια σε bitcoin τα οποία έπρεπε να πληρωθούν εντός προθεσμίας 6 ωρών (PC.MAG, 2017). Όπως βλέπουμε στην Εικόνα 1 οι υπολογιστές οι οποίοι είχαν πληγεί εμφάνιζαν στην οθόνη τους το χαρακτηριστικό μήνυμα απαίτησης των λύτρων Με την έγκαιρη επέμβαση του προσωπικού του Α.Π.Θ., περιορίστηκε η εξάπλωση της μόλυνσης και απομονώθηκαν από το δίκτυο τα προβληματικά τερματικά και μία θύρα. Ευτυχώς υπήρχε η μέριμνα τήρησης αντιγράφων ασφαλείας από τους περισσότερους χρήστες των συγκεκριμένων υπολογιστών, οπότε οι ζημίες από την κρυπτογράφηση δεν ήταν σοβαρές.

Εικόνα 1: Μήνυμα WannaCry στην οθόνη υπολογιστή.

Όσοι υπολογιστές είχαν εγκατεστημένο λειτουργικό πρόγραμμα Microsoft Office και δεν είχαν κάνει την τελευταία αναβάθμιση του κώδικα MS17-010, αντιμετώπισαν πρόβλημα. Από τους 12.000 υπολογιστές που αποτελούν το σταθερό δίκτυο του Πανεπιστημίου μολύνθηκαν 55 τερματικά, τα οποία είχαν παλιά λειτουργικά συστήματα (Windows2003,Win XP). Το Πανεπιστήμιο είχε αντιμετωπίσει ανάλογα περιστατικά παραβίασης δεδομένων και στο παρελθόν, όταν την τελευταία τριετία υπήρξαν δύο περιπτώσεις πιστοποιημένων χρηστών οι οποίοι εν αγνοία τους είχαν «κατεβάσει» στο σύστημα κακόβουλο λυτρισμικό λογισμικό, μολύνοντάς το.

Το συγκεκριμένο συμβάν του WannaCry, είναι η μεγαλύτερη διαχρονικά ψηφιακή επίθεση με στόχο 150 τουλάχιστον διαφορετικές χώρες και με περισσότερους από 300.000 ηλεκτρονικούς υπολογιστές σε ομηρία.. Μεταξύ των θυμάτων υπήρξαν πολύ μεγάλα ονόματα διεθνώς, όπως FedEx, Renault, Nissan, Deutsche Bank, Telefonica το Εθνικό Σύστημα Υγείας στην Αγγλία και

τη Σκωτία, καθώς και περισσότεροι από 1.000 υπολογιστές στο Υπουργείο Εσωτερικών της Ρωσίας, πάνω από 4.000 Εκπαιδευτικά Ερευνητικά Ιδρύματα στην Κίνα και Πανεπιστήμια της Ιταλίας. Στο Α. Π. Θ με την έγκαιρη επέμβαση των υπεύθυνων για την ασφάλεια των δικτύων ο κίνδυνος εξαλείφθηκε εντός 4 ωρών και 31 λεπτών από την στιγμή της κυβερνοεπίθεσης, ενώ το επόμενο πρωί ενημερώθηκε και το τμήμα δίωξης Ηλεκτρονικού Εγκλήματος. Στην Εικόνα 2 βλέπουμε οπτικοποιημένο και σε πραγματικό χρόνο το εύρος της επίθεσης.



Εικόνα 2: Οπτικοποίηση σε πραγματικό χρόνο της επίθεσης WnCry.

Από το χρονολόγιο των συμβάντων γίνεται κατανοητό, πως το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης ανταποκρίθηκε πλήρως στα δεδομένα της κυβερνοεπίθεσης, έδρασε άμεσα και αποτελεσματικά, τηρώντας συγκεκριμένες διαδικασίες όπως ακριβώς είχαμε αναφέρει στο κυρίως μέρος της εργασίας μας. Θεωρούμε λοιπόν, ότι είναι σε ετοιμότητα να αντιμετωπίσει κάθε πιθανό περιστατικό ασφαλείας και να ανταποκριθεί στη πρόκληση της συμμόρφωσής του στην νέα πραγματικότητα του G.D.P.R.