Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία και Ποιότητα*

Μεταπτυχιακή Διατριβή

Πρόληψη και Αντιμετώπιση Κακόβουλου Λογισμικού (Malware) στις Επιχειρήσεις: Σημασία Εκπαίδευσης και Ευαισθητοποίησης του Ανθρώπινου Δυναμικού στα Μέτρα Ασφάλειας των Πληροφοριακών Συστημάτων.

Αθανασία Κωνσταντίνου

Επιβλέπουσα Καθηγήτρια
Ιφιγένεια Γεωργίου

Φεβρουάριος 2016

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Οικονομικών Επιστημών και Διοίκησης

Μεταπτυχιακό Πρόγραμμα Σπουδών *Διοίκηση, Τεχνολογία και Ποιότητα*

Μεταπτυχιακή Διατριβή

Πρόληψη και Αντιμετώπιση Κακόβουλου Λογισμικού (Malware) στις Επιχειρήσεις: Σημασία Εκπαίδευσης και Ευαισθητοποίησης του Ανθρώπινου Δυναμικού στα Μέτρα Ασφάλειας των Πληροφοριακών Συστημάτων.

Αθανασία Κωνσταντίνου

Επιβλέπουσα Καθηγήτρια
Ιφιγένεια Γεωργίου

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στη Διοίκηση, Τεχνολογία και Ποιότητα από τη Σχολή Οικονομικών Επιστημών και Διοίκησης του Ανοικτού Πανεπιστημίου Κύπρου.

Φεβρουάριος 2016

Περίληψη

Κύριος στόχος της μεταπτυχιακής διατριβής μου είναι να αναπτυχθούν οι τρόποι πρόληψης και αντιμετώπισης των περιστατικών κακόβουλων λογισμικών, έτσι ώστε οι εταιρείες να περιορίσουν το φαινόμενο αυτό. Θα βοηθήσει τους οργανισμούς να κατανοήσουν τις απειλές που προέρχονται από περιστατικά malware και να μετριάσουν τους κινδύνους που συνδέονται με αυτά. Έχει διεξαχθεί έρευνα σε εταιρεία που ανήκει στον κλάδο Διαδικτύου και Τηλεπικοινωνιών, έτσι ώστε να δείξουμε στην πράξη το αν οι εργαζόμενοι γνωρίζουν για τα θέματα ασφαλείας των πληροφοριακών συστημάτων του οργανισμού, αν προστατεύονται από τυχόν περιστατικά κακόβουλων λογισμικών που έχουν υποστεί στο χώρο εργασίας τους και αν έχουν λάβει κάποιο είδος εκπαίδευσης. Δόθηκε έμφαση στο αν το ανθρώπινο δυναμικό πιστεύει πως θα είχε καλύτερα αποτελέσματα με το αν η εκπαίδευση ήταν θεωρητική εκπαίδευση ή θα ήταν μόνο μέσω πρακτικής προσέγγισης ή αν προτιμούσαν τον συνδυασμό των δύο.

Αρχικά, στο πρώτο κεφάλαιο θα δοθεί ο ορισμός του malware, και θα παρουσιαστεί μία σύντομη ιστορική αναδρομή περιπτώσεων κακόβουλων λογισμικών που έπληξαν διάφορες εταιρείες, καθώς θα παρουσιαστούν και οι επιπτώσεις που αντιμετωπίζουν οι οργανισμοί όταν έρθουν αντιμέτωποι με τα περιστατικά malware. Θα παρουσιαστούν οι παράγοντες εξάπλωσής των περιστατικών αυτών και θα κατηγοριοποιηθούν οι απειλές που μπορεί να προσβάλουν έναν οργανισμό.

Στο δεύτερο κεφάλαιο, παρέχονται συστάσεις για τη βελτίωση των μέτρων πρόληψης και αντιμετώπισης των περιστατικών malware και γίνεται συσχέτιση με το μεγάλο ρόλο που έχει η εκπαίδευση και η ευαισθητοποίηση του ανθρώπινου δυναμικού στην εφαρμογή των μέτρων ασφαλείας των πληροφοριακών συστημάτων. Βασικό συμπέρασμα είναι ότι η εκπαίδευση του ανθρώπινου δυναμικού σε πολιτικές ασφαλείας πληροφοριακών συστημάτων είναι πολύ σημαντική και θα αυξήσει την αποτελεσματικότητα της ασφάλειας του οργανισμού.

Στο τρίτο κεφάλαιο, ακολουθεί η εμπειρική έρευνα και τα συμπεράσματά της. Το δείγμα συνεντεύξεων ήταν 12. Και οι 12 συμμετέχοντες συμφωνούν πως ο ανθρώπινος παράγοντας είναι η μεγαλύτερη απειλή για τη μη σωστή χρήση των πληροφοριακών συστημάτων της εταιρείας και πως θα προτιμούσαν μία εκπαίδευση ή σειρά σεμιναρίων στα θέματα ασφάλειας των πληροφοριακών συστημάτων με συνδυασμό και των δύο προσεγγίσεων - θεωρίας και πρακτικής άσκησης.

Summary

The main focus of this graduate thesis is to develop the means of prevention and response for cases of malicious software - malware, so that the companies could be able to restrict this phenomenon. In this way the organization will have a clearer understanding of the threats coming from malware incidents; thus they could be able to limit any correlating danger. A research has been conducted in a Communication and Internet firm, in order to illustrate whether the regarding employees are aware of the issues of the information systems security of the organization, whether they are protected in cases of malicious software incidents that occurred at the working environment and If they had been in any way educated. The research focused on whether human resource believe that it would be better if the educational program is theoretical or practical or both.

In this first chapter of this dissertation, the definition of malware is given. Also, there will be a short historical description of cases of malicious software that harmed a significant number of firms and the consequences that the organization have to face when they are dealing with malware incidents. Moreover, there would be analyzes of the spread causes of those incidents and categorization of the threats affecting an organization.

The second chapter, focuses on ways of improving the mean of prevention and response in cases of malware incidents and there is a correlation between the role that the education and as such, the awareness of the human resource have to play for the application of protective measures of information systems. The main conclusion is that the training of human resource in information systems security policies is very important and will improve the efficiency of the organization's protection.

The third chapter demonstrates the empirical analysis and its results. The sample of the interviewers was 12. All of the 12 participants had agreed that the human factor is the most serious threat for the wrongful application of information systems of a firm and that they will prefer to have an educational program or a series of seminars related to issues of information system security in a combination of both theoretical and practical approaches.

Ευχαριστίες

Θα θελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια κα. Ιφιγένεια Γεωργίου κυρίως για την πολύτιμη βοήθεια και καθοδήγησή της σε όλη την διάρκεια της μεταπτυχιακής μου διατριβής.

Θα θελα επίσης να απευθύνω τις ευχαριστίες μου στους γονείς μου, στα αδέρφια μου, τη γιαγιά Γιαννούλα και τον παππού Αθανάση καθώς επίσης και στον αρραβωνιαστικό μου Γιώργο για την πολύτιμη συμπαράστασή τους και την υπομονή που έδειξαν. Επίσης, ευχαριστώ τους συμμετέχοντες της έρευνας, οι οποίοι ήταν ειλικρινής και πρόθυμοι.

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Στην σημερινή εποχή, η ραγδαία εξέλιξη της Τεχνολογίας της Πληροφορικής έχει επιφέρει τεράστιες αλλαγές στη ζωή των επιχειρήσεων. Η χρήση των υπολογιστών και του Διαδικτύου είναι τόσο διαδεδομένη σήμερα για τις επιχειρήσεις, όπου μπορεί να παρέχει εξίσου τεράστια οφέλη αλλά ταυτόχρονα μπορεί να αποτελέσει και μεγάλη απειλή. Οι διάφοροι τύποι κακόβουλων λογισμικών (malware) είναι μία από τις μεγαλύτερες απειλές που αντιμετωπίζει το Διαδίκτυο (Rizwan et al., 2011, Kruegel, 2012). Μια σοβαρή παραβίαση της ασφάλειας των πληροφοριακών συστημάτων οδηγεί σε πολλαπλά επιχειρησιακά προβλήματα και σοβαρές επιπτώσεις. Με τις ζημιές να ποικίλουν εξαιρετικά, είναι μερικές φορές δύσκολο για τα ίδια τα θύματα να εκτιμήσουν το συνολικό κόστος ενός περιστατικού.

Ο όρος «malware», είναι ένας γενικός όρος που χρησιμοποιείται από τους επαγγελματίες της ασφάλειας για την αναφορά κάθε λογισμικού που έχει σχεδιαστεί για να διεισδύει ή να βλάψει τα συστήματα ηλεκτρονικών υπολογιστών (είτε με εμφανή είτε με μη εμφανή τρόπο προς τον χρήστη), μη έχοντας εξουσιοδοτημένη πρόσβαση (Siponen &Oinas-Kukkonen, 2007, Edge et al., 2010, Rizwan et al., 2011).

Σύμφωνα με τη Rutkowska J., (2006) «το κακόβουλο λογισμικό μπορεί να αποκτήσει απομακρυσμένη πρόσβαση σε ένα πληροφοριακό σύστημα, καταγράφοντας και στέλνοντας δεδομένα του συστήματος σε μία τρίτη οντότητα χωρίς τη συγκατάθεση του χρήστη, αποκρύπτοντας ότι το σύστημα έχει παραβιαστεί, απενεργοποιώντας τους μηχανισμούς ασφάλειας και καταστρέφοντας το πληροφοριακό σύστημα ή αλλιώς επηρεάζοντας τα δεδομένα και την ακεραιότητα του συστήματος».

Το λογισμικό μπορεί να θεωρηθεί κακόβουλο λογισμικό ανάλογα με το σκοπό για τον οποίο δημιουργήθηκε και όχι από τα χαρακτηριστικά του. Αναφέρεται σε ένα πρόγραμμα που έχει εισαχθεί κρυφά σε ένα άλλο πρόγραμμα και είναι ειδικά σχεδιασμένο να διαταράσσει ή να εμποδίζει την λειτουργία του με την πρόθεση να καταστρέψει, αλλοιώσει ή συλλέξει δεδομένα, και να βάλει σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων του θύματος (Milosevic, 2013). Ακόμη, το λογισμικό αυτό μπορεί να είναι τόσο ισχυρό ώστε να έχει την ικανότητα να καταλάβει τον πλήρη έλεγχο της μολυσμένης τοποθεσίας (ξενιστή) και της σύνδεσης δικτύου, καθώς επίσης να απενεργοποιήσει τα firewalls και τα antivirus που είναι εγκαταστημένα σε αυτό (Rizwan et al., 2011).

1.1 Δράσεις Κακόβουλων Λογισμικών

Με το πέρασμα των χρόνων το «malware» συνεχίζει να εξελίσσεται και να αναπαράγεται απειλώντας έτσι τα πληροφοριακά συστήματα των οργανισμών με τις δράσεις του. Οι δράσεις του malware χωρίζονται σε τέσσερις κατηγορίες: η πρώτη αφορά την ενεργοποίηση από τον χρήστη άθελα του, η δεύτερη την ανατροπή των προστατευτικών τεχνολογιών, η τρίτη την εκτέλεση, και τέλος, η τέταρτη την διάδοση (Sherly & InduShobha, 2010). Συνέπεια αυτών, ήταν να κατασκευαστούν πιο ασφαλή συστήματα με λιγότερα κενά ασφαλείας και ικανά να ανταπεξέλθουν στις προκλήσεις που θέτουν οι διάφοροι τύποι επιθέσεων malware.

Οι τρόποι που το malware μπορεί να εισέλθει σε ένα υπολογιστή είναι με την λήψη δωρεάν (νόμιμου ή μη) λογισμικού από το Διαδίκτυο που περιέχει κρυφά κακόβουλο πρόγραμμα, με την επίσκεψη σε έναν ιστότοπο που έχει προσβληθεί από κακόβουλο πρόγραμμα, κάνοντας κλικ σε ένα ψεύτικο μήνυμα σφάλματος ή σε ένα αναδυόμενο παράθυρο που ξεκινά με μια λήψη κακόβουλου προγράμματος καθώς και το άνοιγμα ενός συνημμένου μηνύματος ηλεκτρονικού ταχυδρομείου που περιέχει κακόβουλο πρόγραμμα. Επίσης, το malware χρησιμοποιεί ιστοσελίδες, κοινωνικό λογισμικό, e-mail, φορητές μονάδες αποθήκευσης κλπ. για να μολύνει τους υπολογιστές των χρηστών. Οι προσεγγίσεις αυτές σε συνδυασμό με τις τακτικές που προσελκύουν και ξεγελούν τους χρήστες να ανοίξουν π.χ. ένα ύποπτο e-mail, οδηγεί στην εκτέλεση και την ενεργοποίηση του malware, αλλάζοντας τις ρυθμίσεις ασφαλείας, ανοίγοντας backdoors, κατεβάζοντας κακόβουλα αρχεία, κλπ (Sherly & InduShobha, 2010).

Το malware δημιουργείται για διάφορους σκοπούς, όπως την παραβίαση της ιδιωτικής ζωής για διάφορους ανήθικους λόγους, βανδαλισμούς, εγκλήματα, κατασκοπεία ή απλά και για φάρσες. Έτσι, ο αντίκτυπος του κακόβουλου λογισμικού σε ένα επιχειρηματικό

περιβάλλον μπορεί να είναι εκτεταμένος. Ως εκ τούτου, για τους σκοπούς της ασφάλειας του δικτύου, συνιστάτε στις επιχειρήσεις να κατανοήσουν τη σημασία της θέσπισης στρατηγικών πρακτικών πρόληψης και αντιμετώπισης.

1.2 Ιστορική Αναδρομή Επιθέσεων στις Επιχειρήσεις

Το malware των τελευταίων χρόνων διαφέρει αρκετά με εκείνο που συναντούσαμε τα πρώτα χρόνια, πλέον μεταδίδεται πολύ πιο γρήγορα. Αυτό οφείλεται αφενός στη φύση του νέου malware και στους τρόπους με τους οποίους μεταδίδεται. Αρχικά, οι συγγραφείς κακόβουλου λογισμικού δημιουργούσαν τα προγράμματά τους για διασκέδαση, για να αποδείξουν τις τεχνικές τους ικανότητες, και για να ενοχλήσουν τους χρήστες για λόγους εκδίκησης, φάρσας κλπ (Kruegel, 2012, Milosevic, 2013). Όταν πρωτοεμφανίστηκαν οι ιοί, ο μόνος τρόπος για να μολύνουν ένα σύστημα, ήταν με κάποιο ξενιστή, σ' αυτή την περίπτωση, τις δισκέτες. Το κακόβουλο λογισμικό, πλέον τις περισσότερες φορές χρησιμοποιείται από εγκληματίες του κυβερνοχώρου για το κέρδος, και τα προγράμματα που έχουν αναπτύξει έχουν σκοπό την υποκλοπή ευαίσθητων πληροφοριών, προσωπικών δεδομένων, την αποστολή spam, την αλλοίωση δεδομένων, την άρνηση παροχής υπηρεσιών κ.ά. (Kruegel, 2012, Milosevic, 2013). Ωστόσο, η Πληροφορική έχει εξελιχθεί σε μεγάλο βαθμό, κάτι το οποίο εκμεταλλεύτηκαν οι κατασκευαστές malware (Mell et al., 2005). Εκμεταλλεύτηκαν, λοιπόν, δίκτυα και διαδίκτυο για να έχουν πρόσβαση σε ακόμα περισσότερους υπολογιστές (Παπαθανάση, 2012). Εν ολίγοις, το κακόβουλο λογισμικό σήμερα είναι συχνά πιο δύσκολο να ανιχνευθεί, πιο επιζήμιο, και πιο δύσκολο να αφαιρεθεί από ότι στις προηγούμενες γενιές του (Furnell & Ward, 2004).

Υπάρχουν πολλές διαφορετικές απόψεις για το πότε ακριβώς δημιουργήθηκε καθώς και για το ποιος ήταν ο πρώτος ιός. Οι κακόβουλοι ιοί δεν είχαν βγει στο προσκήνιο μέχρι τη δεκαετία του 1980 όταν ο πρώτος υπολογιστής μολύνθηκε από τον ιό «Brain» το 1986, από δύο αδέλφια που ήθελαν να αποδείξουν ότι ο υπολογιστής δεν είναι μία ασφαλής πλατφόρμα και έτσι δημιούργησαν αυτό τον ιό που αντιγραφόταν μέσω δισκετών (Milosevic, 2013).

Το e-mail είναι το πιο δημοφιλές μέσο που χρησιμοποιείται από τους επιτιθέμενους για να παραπλανήσουν τους χρήστες. Η πρώτη διάδοση malware μέσω e-mail ανάγεται στο 1987 με την διάδοση ενός e-mail το οποίο ως θεμα είχε τις λέξεις «χριστουγεννιάτικο

δέντρο» κατηγορίας απειλής δούρειου ίππου. Είναι ωστόσο γνωστό ότι οι εταιρείες Univac και IBM είχαν δεχθεί τους ιούς «Pervading Animal» και «Christmas tree», όπου τους προκάλεσαν σημαντικά προβλήματα στο ηλεκτρονικό ταχυδρομείο (Kienzle & Elder, 2003).

Ο «Happy99» είναι ο πρώτος ιός ηλεκτρονικού ταχυδρομείου, ο οποίος εξαπλωνόταν ως συνημμένο και εντοπίστηκε το 1998. Εκείνη την εποχή τα φίλτρα ανεπιθύμητης αλληλογραφίας μόλις και μετά βίας υπήρχαν. Εάν ο χρήστης έκανε κλικ και εκτελούσε το συνημμένο, θα εμφανίζονταν στην οθόνη του πυροτεχνήματα, αναπαράγοντας τον ιό στέλνοντας στον σε όλες τις επαφές του χρήστη (Milosevic, 2013).

Στην ιστορία του malware σημαντικό βήμα ήταν η μηχανή μετάλλαξης (MtE) ιών, η οποία χρησίμευε στο να μεταλλάσει τους ιούς κάνοντας την ανίχνευσή τους πιο δύσκολη. Ο «WinVir» ήταν ο πρώτος ιός των Microsoft Windows και είχε την ικανότητα να μολύνει τα Windows PE (Portable εκτελέσιμα) αρχεία κάνοντας σε αυτά μικρές αλλαγές. Όταν τα αρχεία εκτελούνταν, ο «WinVir» έψαχνε για άλλα εκτελέσιμα αρχεία και τα μόλυνε και αυτά (Milosevic, 2013).

Το «Code Red» είναι το πρώτο worm στο Διαδίκτυο που ήρθε μετά το worm Morris, το οποίο είναι το πρώτο σκόπιμα γραμμένο worm (worm Morris 1988 ήταν κακόβουλο από ατύχημα). Το «Code Red» εξαπλώνεται το έτος 2000, σε όλο τον κόσμο μέσα σε λίγες ώρες (Milosevic, 2013).
Το «Fizzer» είναι ένα worm ηλεκτρονικού ταχυδρομείου που αναπτύχθηκε το 2003 με σκοπό το κέρδος. Κατά την περίοδο αυτή αλλάζει ο σκοπός των συγγραφέων malware που είναι το κέρδος. Το «Slammer» βρέθηκε στις 13 Σεπτεμβρίου 2003 και ήταν worm στο διαδίκτυο που χρησιμοποιεί την ευπάθεια του OpenSSL και είναι ένα από τα πρώτα malware που επιτέθηκε σε μηχανήματα Linux και Apache Servers (Slammer, 2009). Προκάλεσε μεγάλη ζημιά στο δίκτυο ATM της Bank of America για μερικές ημέρες καθώς επίσης και σε συστήματα ελέγχου πτήσεων για δυο αεροδρόμια αφού κάποιες πτήσεις καθυστέρησαν. Επίσης, προκάλεσε πρόβλημα στο πυρηνικό εργοστάσιο του Ohio (Milosevic, 2013).
Κατά τα έτη 2003 και 2004 ανακαλύφθηκαν τα τρία πιο καταστροφικά worms τα οποία ονομάζονται «slammer», «blaster» και «sasser» στο διαδίκτυο που έχουν εισαχθεί με σκοπό την δολιοφθορά των πληροφοριακών συστημάτων εργοστασίων, σταθμών

παραγωγής ηλεκτρικής ενέργειας, αεροδρομίων και άλλων συστημάτων μεταφορών (Milosevic, 2013).

Το «Mebroot», το 2008 άλλαξε τα γεγονότα αφού ένας υπολογιστής μπορούσε να μολυνθεί από διάφορες αναζητήσεις του χρήστη στο διαδίκτυο από ένα πρόγραμμα περιήγησης (browser). Χρησιμοποίησε exploit στον browser για να αποκτήσει πρόσβαση στο σύστημα, ενώ μία από τις πρώτες ιστοσελίδες που χρησιμοποιήθηκε για να διαδοθεί αυτό το κακόβουλο λογισμικό ήταν η επίσημη ιστοσελίδα της Μόνικα Μπελούτσι. Όταν το «Mebroot» αποκτούσε πρόσβαση στους υπολογιστές-στόχους εγκαθιστούσε rootkit το οποίο κατασκόπευε τι πληκτρολογούσε ο χρήστης και έστελνε τα δεδομένα στον εισβολέα (Milosevic, 2013).

Κατά το έτος 2010, συνέβη ένα μεγάλο βήμα στην εξέλιξη του malware. Το malware πλέον δεν έχει σκοπό μόνο προσωπικές ή οικονομικές πληροφορίες των επιχειρήσεων. Με την δημιουργία malware άρχισαν να ασχολούνται στρατιωτικές και αστυνομικές δυνάμεις, καθώς επίσης και οι μυστικές υπηρεσίες. Η κυβέρνηση των ΗΠΑ δήλωσε ότι η ρίψη βομβών και οι επιθέσεις malware στον κυβερνοχώρο θεωρούνται ως ισότιμα πράγματα. Έτσι, το καλοκαίρι του 2010 δημιουργήθηκε το «Stuxnet».

Οι επιθέσεις ασφαλείας σε μεγάλες και μικρομεσαίες επιχειρήσεις σήμερα βρίσκονται σε άνοδο. Το 2011, hackers παραβίασαν τις πιστωτικές κάρτες και τα προσωπικά δεδομένα για τουλάχιστον 70 εκατομμύρια χρήστες του Sony PlayStation Network. Καθώς επίσης και η RSA - Bedford, Mass που παρέχει ασφάλεια σε περισσότερους από 90% του Fortune 500, ήταν η ίδια σε κίνδυνο από hacker που εκμεταλλεύτηκε ένα κενό ασφαλείας στο συγκεκριμένο λογισμικό. Η Sony είχε 3.2 δισεκατομμύρια δολάρια καθαρή ζημιά για το έτος 2010-2011 από την επίθεση αυτή, καθώς επίσης και η RSA αντιμετώπιζε επίμονες ανησυχίες για το ότι τα προϊόντα ασφαλείας που παρέχει δεν είναι απολύτως αποτελεσματικά (Blum, 2011).

Ένα από τα πιο πρόσφατα malware είναι το «Φλόγα» που βρέθηκε το 2012, το οποίο μόλυνε τους περισσότερους υπολογιστές της Εγγύς και Μέσης Ανατολής και άνηκε στο Ισραήλ και στις Αμερικανικές μυστικές υπηρεσίες και το στρατό. Αυτό είναι ένα malware, όπου ο εισβολέας μπορεί να προσθέσει νέα modules από απόσταση, και εξαπλώνεται είτε μέσω θύρας USB ή δικτύου, ενώ χρησιμοποιεί rootkit εργαλείο για να

κρυφτεί στο μολυσμένο σύστημα. Είχε την ικανότητα να καταγράφει ήχο, βίντεο, κλήσεις Skype, την δραστηριότητα δικτύου, για να κλέψει αρχεία από το σκληρό δίσκο και να τα στείλει στον εισβολέα (Milosevic, 2013).

Εν έτη 2016, με την αυξανόμενη δημοτικότητα των ιστοτόπων κοινωνικής δικτύωσης όπως το Facebook, Twitter κλπ, προκύπτουν πολλές επιθέσεις malware, οι οποίες έχουν ως στόχο κυρίως το κέρδος και την δολιοφθορά. Μια άλλη τάση στις επιθέσεις malware της εποχής είναι οι VOIP επιθέσεις. Το κινητό τηλέφωνο έχει γίνει ένα κοινό εργαλείο για την πρόσβαση στο Διαδίκτυο και οι εγκληματίες του κυβερνοχώρου δίνουν ιδιαίτερη προσοχή σε αυτό. Οι επιτιθέμενοι τις χρησιμοποιούν για να συμμετάσχουν σε κλοπή δεδομένων και άλλες απάτες παρόμοιες με τα προβλήματα που εμφανίζονταν στα e-mail στο παρελθόν. Ακόμη, το Pay-Per-Click-Hijacking με το οποίο ξεγελούν τους χρήστες οι οποίοι χρεώνονται κάθε φορά που κάνουν κλικ, είναι ακόμη μια νέα μορφή malware που συναντάται στη σημερινή εποχή.

Έχουν περάσει πολλά χρόνια από την δημιουργία του πρώτου malware ηλεκτρονικών υπολογιστών. Οι σκοποί και τα κίνητρα για τη δημιουργία malware έχουν αλλάξει από την εκδίκηση και το κέρδος στην κατασκοπεία και την δολιοφθορά. Τα κέρδη εξακολουθούν να είναι ένα μεγάλο κίνητρο για την δημιουργία malware, και θα συνεχίσουν να είναι και στο μέλλον (Furnell & Ward, 2004, Milosevic, 2013).

1.3 Επιπτώσεις Κακόβουλων Λογισμικών

Κατ' αρχάς, οι επιθέσεις κακόβουλου λογισμικού μπορεί να έχουν ως αποτέλεσμα την απώλεια εσόδων. Αυτό μπορεί να συμβεί ως αποτέλεσμα μιας υποβαθμισμένης απόδοσης από το σύστημα ή το κόστος που μπορεί να έρθει από τις επισκευές ενός μολυσμένου συστήματος, καθώς επίσης και το κόστος της απώλειας δεδομένων και της κλοπής ταυτότητας, το οποίο μπορεί να είναι πολύ δαπανηρό.

Επί του παρόντος, δεν υπάρχουν έγκυρα στοιχεία σχετικά με το συνολικό κόστος από τα περιστατικά malware. Η ετήσια έρευνα για την ασφάλεια του ηλεκτρονικού εγκλήματος από το Computer Security Institute και το FBI (Gordon και Loeb, 2006) διαπίστωσε ότι οι επιθέσεις ιών είναι η κύρια αιτία των οικονομικών απωλειών στους οργανισμούς (μέση απώλεια ανά επιχείρηση των $167.713 το 2005). Η αξιοπιστία των άλλων στοιχείων είναι πιο αμφιλεγόμενη, αλλά συνήθως οι αριθμοί είναι της τάξεως

των δισεκατομμυρίων δολαρίων. Μια μελέτη που δημοσιεύθηκε τον Ιούλιο του 2000 από την έρευνα Information Week Pricewaterhouse Coopers εκτιμά ότι το κόστος του κακόβουλου λογισμικού έχει υπερβεί τα 1.5 τρισεκατομμύρια σε όλο τον κόσμο εκείνο το έτος. Ο αντίκτυπος στις επιχειρήσεις των ΗΠΑ με περισσότερους από 1000 εργαζόμενους εκτιμάται ότι είναι 266 δισεκατομμύρια δολάρια (Cavusoglu et al., 2004).

Κατά το ίδιο έτος, πραγματοποιήθηκαν επιθέσεις Distributed Denial of Service (DDoS) σε πολλούς γνωστούς δικτυακούς τόπους όπως το Amazon, το Yahoo και το eBay. Οι επιθέσεις αυτές πιθανόν να έγιναν μέσω botnets (Niccolai, 2000). Εκτιμάται ότι η ζημιά από αυτές τις επιθέσεις ήταν $1.2 δισεκατομμύρια. Η ζημιά αύτη προήλθε από την αρνητική συνέπεια στις τιμές των μετοχών, την απώλεια εσόδων από τις πωλήσεις και τη διαφήμιση, και τις επενδύσεις στις αναβαθμίσεις ασφαλείας των συστημάτων.

Έρευνα που πραγματοποιήθηκε από την Kaspersky Lab (2015), έδειξε ότι τα πιο κοστοβόρα είδη παραβιάσεων της ασφάλειας για επιχειρήσεις είναι η απάτη από εργαζομένους, η ψηφιακή κατασκοπεία, η εισβολή στα εταιρικά δίκτυα και οι αστοχίες εξωτερικών προμηθευτών. Στην έρευνα συμμετείχαν περισσότερες από 5.500 εταιρείες σε 26 χώρες. Κατά μέσο όρο, οι δαπάνες για την αποκατάσταση των ζημιών από ένα περιστατικό ασφάλειας ανέρχονται σε $551.000 για τις μεγάλες επιχειρήσεις και $38.000 για τις μικρές και μεσαίες επιχειρήσεις. Επίσης, πολλές επιχειρήσεις χάνουν έσοδα, λόγω της απώλειας επιχειρηματικών ευκαιριών καθώς και του χρόνου διακοπής της λειτουργίας των συστημάτων και των υπηρεσιών. Πέρα από την απώλεια εσόδων, πρέπει κάθε επιχείρηση να υπολογίσει και τις έμμεσες δαπάνες, δηλαδή των κονδυλίων που διαθέτουν οι επιχειρήσεις μετά την αποκατάσταση, αλλά εξακολουθεί να συνδέεται με μια παραβίαση ασφάλειας. Έτσι, εκτός από τα προαναφερθέντα ποσά, οι επιχειρήσεις καταβάλουν συνήθως από $8.000 (μικρομεσαίες) μέχρι και $69.000 (μεγάλες) για στελέχωση, κατάρτιση και αναβαθμίσεις υποδομών. Κατά μέσο όρο οι επιχειρήσεις που έχουν υποστεί παραβίαση πληρώνουν μέχρι και $204.750 όσο αφορά το πλήγμα που θα δεχθούν για τη φήμη της εταιρείας.

Εννέα στις δέκα επιχειρήσεις που έλαβαν μέρος στην έρευνα Kaspersky Lab (2015), ανέφεραν τουλάχιστον ένα περιστατικό ασφάλειας. Ωστόσο, δεν είναι όλα τα περιστατικά σοβαρά ή δεν οδηγούν απαραίτητα σε απώλεια ευαίσθητων δεδομένων. Μια σοβαρή παραβίαση ασφάλειας είναι συνηθέστερα το αποτέλεσμα επιθέσεων

κακόβουλου λογισμικού, επιθέσεων phishing, διαρροής δεδομένων από τους υπαλλήλους και εκμετάλλευσης τρωτών σημείων λογισμικού. Η κοστολόγηση παρέχει μια νέα ματιά στη σοβαρότητα των περιστατικών ασφάλειας και οι εκτιμήσεις για τις μικρομεσαίες και τις μεγάλες επιχειρήσεις είναι ελαφρώς διαφορετικές.
Οι μεγάλες εταιρείες καταβάλουν πολύ περισσότερα χρήματα όταν μια παραβίαση ασφάλειας προκύπτει λόγω αστοχιών ενός έμπιστου εξωτερικού συνεργάτη ή παρόχου. Στα κοστοβόρα είδη περιστατικών περιλαμβάνονται η απάτη από εργαζόμενους, η ψηφιακή κατασκοπεία και η εισβολή στο δίκτυο. Οι μικρομεσαίες επιχειρήσεις τείνουν να χάνουν ένα σημαντικό ποσό για σχεδόν όλα τα είδη παραβίασης, καταβάλλοντας υψηλά ποσά για την αποκατάσταση των ζημιών από ενέργειες κατασκοπείας, επιθέσεις DDoS και phishing.

Το malware μπορεί επίσης να επηρεάσει αρνητικά μια επιχείρηση βλάπτοντας το εμπορικό σήμα της, χάνοντας τους πελάτες της και την εμπιστοσύνη τους προς αυτήν, ενώ όταν τα συστήματα δεν λειτουργούν όπως αναμένεται οι πελάτες είναι δυσαρεστημένοι με τις υπηρεσίες της. Επιπλέον, μπορεί να οδηγήσει στην απώλεια πληροφοριών ή δεδομένων που μπορεί να είναι πολύ ζωτικής σημασίας για την καθημερινή λειτουργία του οργανισμού. Το malware μπορεί επίσης να έχει καταστροφικές συνέπειες, εάν επιτρέπει σε έναν hacker να διεισδύσει στο δίκτυο ενός οργανισμού. Αυτό συμβαίνει επειδή η πρόσβαση σε ευαίσθητες πληροφορίες για ένα οργανισμό ή για τους πελάτες του από μη εξουσιοδοτημένα άτομα ενδέχεται να οδηγήσει σε νομικές συνέπειες ή την πτώση της εταιρείας. Ο αντίκτυπος των γεγονότων malware διαφέρουν από τον ένα οργανισμό στον άλλο, καθώς αυτό εξαρτάται από το επίπεδο της άμυνας και αντιμετώπισης που έχει θέσει ο οργανισμός σε εφαρμογή.

Οι επιχειρήσεις που προσφέρουν ηλεκτρονικές υπηρεσίες έχουν πολλές επιπτώσεις από τη χρήση του κακόβουλου λογισμικού. Πολλές από αυτές έχουν έρθει αντιμέτωπες με DDoS επιθέσεις, και συχνά απαιτούνται να αγοραστούν όλο και πιο μεγάλες σε κόστος υπηρεσίες για τους ISPs, για να προστατέψουν την διαθεσιμότητα των υπηρεσιών που προσφέρουν. Οι επιτιθέμενοι κάνουν χρήση κακόβουλου λογισμικού με διάφορους μεθόδους για να αποκομίσουν έμπιστα δεδομένα πελατών (αριθμό πιστωτικής κάρτας κλπ) προκειμένου να τους εγγράψουν σε εταιρείες ηλεκτρονικού εμπορίου. Μάλιστα, μερικές εξελιγμένες μορφές malware κατάφεραν να νικήσουν τα μέτρα ασφαλείας διαδικτυακών ιστοτόπων τραπεζών, παρόλο που απαιτούσαν πολλαπλούς

παραμέτρους σχετικά με την αυθεντικοποίηση των πελατών τους, μέσω phishing e-mails. Συνήθως, επηρεάζονται οι πελάτες που χρησιμοποιούν τις υπηρεσίες του ηλεκτρονικού εμπορίου ωστόσο, είτε άμεσα είτε έμμεσα επηρεάζεται και η εταιρεία ηλεκτρονικού εμπορίου με επιπτώσεις στην φήμη της (Mell et al., 2005).

Επιπλέον, μπορεί η διάβρωση της εμπιστοσύνης και της αξιοπιστίας να έχει επιπτώσεις για τις κυβερνήσεις, τις επιχειρήσεις και τους καταναλωτές. Για παράδειγμα, οι υπηρεσίες της ηλεκτρονικής διακυβέρνησης, όπως το να συμπληρώσει κάποιος μέσω του διαδικτύου τη φορολογική του δήλωση ή των παροχών που του δίνονται από το κράτος, περιέχουν προσωπικά δεδομένα, τα οποία αν παραβιαστούν θα μπορούν να χρησιμοποιηθούν για τη διάπραξη απάτης. Άρα τα πληροφοριακά συστήματα σε μικρές επιχειρήσεις ή σε μεγάλους δημόσιους ή ιδιωτικούς τομείς οργανισμών μπορούν να χρησιμοποιηθούν για να υπάρξει πρόσβαση σε τέτοιες υπηρεσίες ηλεκτρονικής διακυβέρνησης ή ηλεκτρονικού εμπορίου.

1.4 Παράγοντες Εξάπλωσης Κακόβουλων Λογισμικών

Οι παράγοντες που ευνοούν την εξάπλωση του malware είναι τα κενά ασφαλείας / ευπάθεια λογισμικού, η μολυσματικότητα και ο ανθρώπινος παράγοντας (Παπαθανάση, 2012).

1.4.1 Ευπάθεια Λογισμικού

Στην ασφάλεια των πληροφοριακών συστημάτων η ευπάθεια του λογισμικού μπορεί να θεωρηθεί ως ελάττωμα, αδυναμία των διαδικασιών ασφαλείας ή λάθος στο σχεδιασμό του συστήματος που μπορεί να αξιοποιηθεί από έναν εισβολέα για να μεταβάλλει την κανονική συμπεριφορά του συστήματος και να έχει πρόσβαση σε δεδομένα. Καθώς ο αριθμός των συστημάτων λογισμικού αυξάνεται καθημερινά, ταυτόχρονα αυξάνεται και ο αριθμός αυτών των κενών ασφαλείας και είναι απλά θέμα χρόνου ότι κάποιος μπορεί να ξεκινήσει μια επίθεση της οποίας οι συνέπειες είναι απρόβλεπτες σε ζημιές και σε κόστος σε πολλούς από τους σύγχρονους οργανισμούς (Παπαθανάση, 2012).

1.4.2 Μολυσματικότητα

Η μολυσματικότητα έχει να κάνει με την αποτελεσματικότητα ενός ιού, δηλαδή το κατά πόσο μπορεί να μεταδοθεί εύκολα και αυτό εξαρτάται από την φύση του ιού, από τον

τρόπο κατασκευής του και τις λειτουργίες για τις οποίες σχεδιάστηκε να εκτελεί (Παπαθανάση, 2012).

1.4.3 Ανθρώπινος Παράγοντας

Μείζον πρόβλημα για τις εταιρείες, ανά τον κόσμο, αποτελούν, πλέον, οι εκ των έσω απειλές. Μεγάλος παράγοντας εισβολής και εξάπλωσης ενός malware είναι και ο ανθρώπινος παράγοντας. Κίνδυνοι μπορούν να προκληθούν καθώς οι χρήστες περιηγούνται σε ιστοσελίδες με κακόβουλο περιεχόμενο ή όταν κατεβάσουν κάποιο είδος απειλής χωρίς βέβαια να έχουν επίγνωση του πραγματικού περιεχομένου που εισάγουν στον υπολογιστή τους. Πολλές φορές οι χρήστες δεν είναι εκπαιδευμένοι κατάλληλα ή η ενημέρωσή τους δεν είναι συνεχής σχετικά με την αντιμετώπιση των κινδύνων. Μια λάθος εκτίμηση του χρήστη μπορεί να θέσει σε κίνδυνο τη λειτουργία του συστήματος και ας είναι πολύ καλά και κατάλληλα προστατευμένο (Sherly & InduShobha, 2010). Η ασφάλεια των πληροφοριών είναι η προστασία των πληροφοριών από ένα ευρύ φάσμα απειλών, προκειμένου να διασφαλίσει η επιχείρηση την ελαχιστοποίηση του επιχειρηματικού κινδύνου, καθώς και τη μεγιστοποίηση της απόδοσης των επενδύσεων και των επιχειρηματικών ευκαιριών (Sherly & InduShobha, 2010).

Σύμφωνα με την έρευνα της Kaspersky Lab (2015), περισσότερες από μία στις πέντε ευρωπαϊκές επιχειρήσεις, ποσοστό 21%, δηλώνει ότι έχει χάσει ευαίσθητα επιχειρηματικά δεδομένα λόγω «εσωτερικών απειλών» μέσα στους τελευταίους 12 μήνες. Μάλιστα, τα παγκόσμια δεδομένα δείχνουν ότι, για πρώτη φορά από το 2011, η τυχαία κοινή χρήση δεδομένων από το προσωπικό οδηγεί σε μεγαλύτερο βαθμό απώλειας δεδομένων σε σύγκριση με τις απώλειες εξαιτίας των τρωτών σημείων λογισμικού. Ενώ δηλαδή οι επιχειρήσεις σταδιακά κερδίζουν τη «μάχη» ενάντια στα τρωτά σημεία προγραμμάτων λογισμικού, η απώλεια δεδομένων αυξάνεται.
Άλλα παραδείγματα εσωτερικών απειλών, που οδηγούν σε περιστατικά απώλειας δεδομένων, σύμφωνα με την έρευνα, περιλαμβάνουν εσκεμμένες διαρροές δεδομένων από εργαζόμενους και σφάλματα στον τομέα της ασφάλειας από εξωτερικό προμηθευτή / συνεργάτη. Οι εταιρείες Τηλεπικοινωνιών κατέγραψαν το υψηλότερο ποσοστό (42%) τυχαίων διαρροών και κοινής χρήσης δεδομένων από το προσωπικό. Ο τομέας Κοινής Ωφέλειας & Ενέργειας ανέφερε το δεύτερο υψηλότερο ποσοστό (33%), με τον τομέα της Μεταποίησης να σημειώνει επίσης υψηλό ποσοστό (31%).

1.5 Κατηγορίες Απειλών Κακόβουλων Λογισμικών

Ο προσδιορισμός και η ταξινόμηση των απειλών είναι ζωτικής σημασίας για την οικοδόμηση αμυντικών μηχανισμών. Παρακάτω ταξινομούνται οι απειλές που έχουν να αντιμετωπίσουν οι επιχειρήσεις καθημερινά (Weaver et al., 2003):

1.5.1 Ιοί (Virus)

Απειλούν την παραγωγικότητα σε ένα σύστημα, και ο όρος χρησιμοποιείται συχνά για την ταξινόμηση όλων των malware. Αυτό που διακρίνει όμως έναν ιό από τις άλλες μορφές malware είναι η ικανότητά του να επαναλαμβάνεται το ίδιο μετά από την ακούσια αρχική ενεργοποίησή του από το χρήστη και να εξαπλώνεται σε άλλα αρχεία σε έναν υπολογιστή, με αποτέλεσμα να τα μολύνει (Edge et al., 2010). Αυτό-αντιγράφεται εισάγοντας αντίγραφα του εαυτού του σε προγράμματα υποδοχής ή αρχεία δεδομένων. Ο Fred Cohen, το 1985 περιέγραψε έναν ιό ως «ένα πρόγραμμα το οποίο μολύνει άλλα προγράμματα τροποποιώντας τον κώδικα τους, ώστε να περιλαμβάνουν μια έκδοση του εαυτού του…».

Οι ιοί συχνά προκαλούνται μέσω της αλληλεπίδρασης των χρηστών, όπως το άνοιγμα ενός αρχείου ή τρέχοντας ένα πρόγραμμα. Οι ιοί μπορούν να ταξινομηθούν σε compiled ιούς, οι οποίοι είναι ιοί που προσβάλλουν αρχεία τα οποία συνδέονται με εκτελέσιμα προγράμματα και σε interpreted ιούς, οι οποίοι είναι ιοί μακροεντολών που εκτελούνται από μια εφαρμογή. Οι ιοί μπορούν να προξενήσουν ζημιά στον υπολογιστή στον οποίο εγκαθίστανται, όπως καταστροφή προγραμμάτων, διαγραφή αρχείων, μορφοποίηση του σκληρού δίσκου ή και υποβάθμιση της απόδοσης του συστήματος. Οι ιοί των υπολογιστών μπορούν να αφαιρεθούν με την εγκατάσταση και τη λειτουργία προστασίας από ιούς ή anti-malware προγράμματα.

1.5.2 Σκουλήκια (Worms)

Είναι μολυσματικοί και αυτοαναπαραγόμενοι ιοί, αυτόνομα προγράμματα που εκτελούνται συνήθως χωρίς την παρέμβαση του χρήστη αφού αντιγράφονται αυτόματα, κάνοντας χρήση της υπάρχουσας δικτυακής υποδομής (π.χ. Τοπικά Δίκτυα – Δίκτυα WAN) ή και των υπηρεσιών του Internet (IRC chat, e-mail, newsgroups, κλπ) (Aycock, 2006). Ένα worn εκμεταλλεύεται μια ευπάθεια και τα κενά ασφαλείας είτε σε μια υπηρεσία δικτύου, είτε σε μια υπηρεσία μαζικής αλληλογραφίας για να διαδοθεί και

να μολύνει και άλλους υπολογιστές (Edge et al., 2010). Λόγω του ότι τα worms χρησιμοποιούν δικτυακές συνδέσεις για να εξαπλωθούν, μπορούν να έχουν υπερβολικά γρήγορη εξάπλωση και να δημιουργήσουν μεγάλη δικτυακή κίνηση, μειώνοντας την ταχύτητα ή μη επιτρέποντας τη νόμιμη πρόσβαση στο δίκτυο. Τα worms που μεταδίδονται μέσω διαδικτύου αποτελούν το πιο επικίνδυνο είδος malware. Μπορούν να αφαιρεθούν χρησιμοποιώντας εργαλεία αφαίρεσης κακόβουλου λογισμικού. Το εκτιμώμενο κόστος για την αντιμετώπιση του ιού τύπου worm σε κάθε εγκατάσταση κυμαίνεται από $200 έως πάνω από $53,000.

1.5.3 Δούρειοι Ίπποι (Trojan Horses)

Καταστροφικά προγράμματα που προσποιούνται ότι είναι μια χρήσιμη εφαρμογή, αλλά βλάπτουν τον υπολογιστή ή υποκλέπτουν στοιχεία αφού εγκατασταθούν. Αυτή η απειλή αντικαταστεί τα υπάρχοντα αρχεία είτε με κακόβουλες εκδόσεις ή προσθέτει νέα κακόβουλα αρχεία ξενιστή (Aycock, 2006, Παπαθανάση, 2012). Μόλις εγκατασταθεί, δημιουργεί μια κερκόπορτα (backdoor) στο σύστημα και δίνει πρόσβαση στον επιτιθέμενο (hacker), ο οποίος μπορεί στη συνέχεια να διενεργεί ποινικές πράξεις στον υπολογιστή-στόχο από έναν απομακρυσμένο σταθμό όπως την διαγραφή αρχείων, την κλοπή κωδικών πρόσβασης, την αποστολή κακόβουλων e-mail σε άλλους χρήστες κλπ. (Edge et al., 2010). Οι Δούρειοι ίπποι μπορούν να αφαιρεθούν με τη χρήση προγραμμάτων antivirus.

1.5.4 Mobile Malware - VOIP

Είναι ένα λογισμικό με κακόβουλη πρόθεση που μεταδίδεται από έναν απομακρυσμένο κεντρικό υπολογιστή σε έναν τοπικό κεντρικό υπολογιστή και στη συνέχεια εκτελείται στον τοπικό υπολογιστή, συνήθως χωρίς τη ρητή εντολή του χρήστη. Δημοφιλής γλώσσες για mobile malware είναι η Java, η ActiveX, η JavaScript και η VBScript (Souppaya και Scarfone, 2012).

Οι έξυπνες κινητές συσκευές, smartphones και tablets, αποτελούν χρήσιμο εργαλείο στα χέρια δισεκατομμυρίων χρηστών, καθώς χρησιμοποιούνται τόσο για επικοινωνία, όσο και για διασύνδεση και αποθήκευση δεδομένων. Οι συσκευές αυτές περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα, όπως λίστες επαφών, φωτογραφίες, οικονομικά στοιχεία και κωδικούς για ηλεκτρονικές τραπεζικές συναλλαγές, ενώ παράλληλα, προσφέρουν δυνατότητα σύνδεσης always-on στα κοινωνικά δίκτυα, λογαριασμούς e-mail και ενδεχομένως πρόσβαση στο εταιρικό δίκτυο του χρήστη. Αυτή η πολλαπλή

λειτουργικότητα που προσφέρουν γίνεται πόλος έλξης των εγκληματιών του κυβερνοχώρου.

Το κακόβουλο λογισμικό κινητών συσκευών (mobile malware) μπορεί να κάνει ό,τι και ένας ιός στον υπολογιστή. Για παράδειγμα, μπορεί να υποβαθμίσει την απόδοση του smartphone, να στείλει spam σε όλες τις επαφές, να διαγράψει αρχεία, κτλ. Μπορεί ακόμη να κάνει κλήσεις ή να στείλει SMS σε αριθμούς υψηλής χρέωσης (premium numbers) ή να κλειδώσει το κινητό, καθιστώντας το μη-λειτουργικό. Οι πιο συνηθισμένοι τρόποι μόλυνσης ενός κινητού είναι μέσω της λήψης ενός κακόβουλου συνημμένου (e-mail, κακόβουλη ιστοσελίδα, εφαρμογή από πηγή αμφιλεγόμενης ασφάλειας, κτλ.), μέσω κοινών συνδέσμων εφαρμογών κοινωνικής δικτύωσης ή/και εφαρμογών διαμοιρασμού αρχείων (peer-to-peer).

Σύμφωνα με την ALU (2014), οι μολύνσεις των έξυπνων κινητών συσκευών αυξήθηκαν με ρυθμό 25% το 2014, σε σύγκριση με το 20% του 2013. Σε παγκόσμιο επίπεδο, υπάρχουν σήμερα περίπου 16 εκατομμύρια έξυπνες κινητές συσκευές, οι οποίες έχουν μολυνθεί από κακόβουλο λογισμικό.
Οι απειλές κατά της ασφάλειας δεν αφορούν μόνο στις κινητές συσκευές, αλλά και στα δίκτυα κινητής τηλεφωνίας. Η ανάγκη για αναζήτηση νέων μεθόδων ασφάλειας που θα ενισχύσουν περαιτέρω τις μεθόδους που εφαρμόζονται σήμερα και θα διασφαλίζουν την απρόσκοπτη υπηρεσία με υψηλή ποιότητα, καθίσταται επιτακτική.

1.5.5 Κοινωνική Μηχανική (Phishing)

Μια σημαντική απειλή για την οργανωτική ασφάλεια των πληροφοριών είναι η αύξηση του αριθμού των περιστατικών που προκαλούνται από τις επιθέσεις κοινωνικής μηχανικής. Η κοινωνική μηχανική (Allen, 2006) είναι ένας γενικός όρος και ένα από τα ισχυρότερα όπλα στο οπλοστάσιο των επιτιθέμενων, που προσπαθούν να ξεγελάσουν τους χρήστες του διαδικτύου να αποκαλύψουν ευαίσθητες πληροφορίες ή να εκτελέσουν αρχεία που εμφανίζονται να είναι καλοήθεις ενώ στην πραγματικότητα είναι τύποι malware. Η αυξανόμενη τάση των web-based malware, επίσης γνωστή ως drive-by-download, η οποία ανακατευθύνει τον χρήστη σε μια μολυσμένη ιστοσελίδα, που επιχειρεί στη συνέχεια να εκμεταλλευτεί τα τρωτά σημεία και τελικά να εγκαταστήσει rootkits ή άλλα εργαλεία επιθέσεων, θέτει σε κίνδυνο πολλούς οργανισμούς.

Οι κλασικές κατηγορίες malware που παρουσιάστηκαν πιο πάνω δεν περιλαμβάνουν το phishing, το οποίο αναφέρεται στην παραπλανητική χρήση των ηλεκτρονικών υπολογιστών που βασίζεται στο ξεγέλασμα των ατόμων, έτσι ώστε να αποκαλύψουν ευαίσθητες προσωπικές πληροφορίες. Οι phishing επιθέσεις κινούνται κατά κύριο λόγο μέσω e-mails που παραπέμπουν τους χρήστες σε δόλιες ιστοσελίδες, οι οποίες με τη σειρά τους συλλέγουν αριθμούς τραπεζικών λογαριασμών, αριθμούς κοινωνικής ασφάλισης κλπ., όπου προορίζονται στο να εξαπατήσουν τους χρήστες και να αποκαλύψουν είτε προσωπικά δεδομένα είτε οικονομικές πληροφορίες (Jakobbson και Myers, 2006). Οι επιθέσεις phishing απευθύνονται σε στελέχη οργανισμών και άλλα άτομα που έχουν πρόσβαση σε πληροφορίες με ιδιαίτερο ενδιαφέρον ή αξία. Παραδείγματος χάριν, κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο φαίνεται να προέρχεται από μια αξιόπιστη πηγή, όπως μια τράπεζα ή την διοίκηση ενός οργανισμού. Ωστόσο, μια πιο προσεκτική ματιά στη διεύθυνση e-mail του αποστολέα θα μπορούσε να αποκαλύψει ότι είναι απάτη (Allen, 2006, Sherly & InduShobha, 2010).

Σύμφωνα με τα αποτελέσματα έρευνας της Kaspersky Lab (2013), ο αριθμός των χρηστών του Διαδικτύου που αντιμετώπισε επιθέσεις phishing τους τελευταίους μήνες του 2013, έχει αυξηθεί από 19,9 σε 37,3 εκατομμύρια. Τα Facebook, Yahoo, Google και Amazon είναι μεταξύ των κύριων στόχων των ψηφιακών εγκληματιών. Η έρευνα, που διεκπεραιώθηκε τον Ιούνιο του 2013 βασιζόμενη σε δεδομένα από την cloud υπηρεσία Kaspersky Security Network, δείχνει πως ό,τι κάποτε ήταν απλώς μια υποκατηγορία spam, έχει εξελιχθεί σε μία ραγδαία αυξανόμενη ψηφιακή απειλή. Στην πραγματικότητα, το email δεν αποτελεί πια τον πλέον κοινό μηχανισμό αποστολής των phishing emails. Για παράδειγμα, μόνο το 12% όλων των καταγεγραμμένων επιθέσεων phishing πραγματοποιήθηκε μέσω spam emails. Το υπόλοιπο 88% των περιστατικών προήλθε από links που οδηγούσαν σε σελίδες phishing, και τις οποίες οι χρήστες επισκέφτηκαν χρησιμοποιώντας ένα web browser, ή ένα σύστημα ανταλλαγής μηνυμάτων, όπως το Skype ή άλλους messengers. Πάνω από το 20% όλων των επιθέσεων phishing μιμήθηκε τράπεζες και άλλους χρηματοπιστωτικούς οργανισμούς. Οι ιστοσελίδες των American Express, PayPal, Xbox live, Twitter κ.λπ. βρέθηκαν ανάμεσα στους κορυφαίους 30 στόχους.

1.5.6 DDoS Επιθέσεις

Επιθέσεις άρνησης εξυπηρέτησης ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς χρήστες. Οι επιθέσεις αυτές αυξάνονται σύμφωνα με την έρευνα της Kaspersky Lab (2014), το 1ο τρίμηνο του 2015, οι ψηφιακοί εγκληματίες πραγματοποίησαν, συνολικά, 23.095 επιθέσεις DDoS, οι οποίες έπληξαν στόχους σε 76 χώρες, μέγεθος υψηλότερο κατά 15%, σε σχέση με τις 66 χώρες, που καταγράφηκαν στο 4ο τρίμηνο του 2014. Η Κίνα, οι ΗΠΑ και ο Καναδάς ήταν οι χώρες, που επηρεάστηκαν περισσότερο από αυτές τις επιθέσεις. Οι επιχειρήσεις στον τομέα της Πληροφορικής υποφέρουν περισσότερο από τις επιθέσεις DDoS. Παγκοσμίως, το 49% των εκπροσώπων του κλάδου της Πληροφορικής ανέφερε ότι έχει αντιμετωπίσει τουλάχιστον μία επίθεση DDoS, κατά το τελευταίο έτος. Όπως προκύπτει από τη σχετική έρευνα, ψηλά στην κατάταξη βρίσκονται και άλλες επιχειρήσεις, που στηρίζονται στην παροχή online υπηρεσιών, όπως εταιρείες ηλεκτρονικού εμπορίου (44%), τηλεπικοινωνιακοί οργανισμοί (44%) και μέσα μαζικής ενημέρωσης (42%). Οι χρηματοοικονομικές επιχειρήσεις βρίσκονται, επίσης, μεταξύ των οργανισμών, που δέχονται πιο συχνά επιθέσεις DDoS (39%). Σημαντικές οικονομικές απώλειες, που κατά μέσο όρο κυμαίνονται από $52.000 έως $444.000, ανάλογα με το μέγεθος της επιχείρησης, μπορεί να κοστίσει σε μία εταιρεία μία επίθεση DDoS στους online πόρους της.

Το μέγεθος του προβλήματος αναδεικνύει έρευνα των Kaspersky Lab (2014), η οποία επισημαίνει ότι για πολλούς οργανισμούς, τα κόστη αυτά έχουν σοβαρές επιπτώσεις στον ισολογισμό μιας εταιρείας, αλλά ταυτόχρονα βλάπτουν και τη φήμη της, αφού συνεργάτες και πελάτες χάνουν τη δυνατότητα πρόσβασης στους online πόρους της. Το 38% των εταιρειών, που δέχτηκε επίθεση DDoS, δεν ήταν σε θέση να διεκπεραιώσει βασικές λειτουργικές δραστηριότητες, ενώ το 33% των ερωτηθέντων αναφέρθηκε στην απώλεια επιχειρηματικών ευκαιριών και συμβολαίων. Σύμφωνα με την έρευνα, το 61% των θυμάτων επιθέσεων DDoS έχασε προσωρινά την πρόσβαση σε κρίσιμες πληροφορίες. Το 38% των εταιρειών δεν ήταν σε θέση να διεκπεραιώσει βασικές λειτουργικές δραστηριότητες, ενώ το 33% των ερωτηθέντων αναφέρθηκε στην απώλεια επιχειρηματικών ευκαιριών και συμβολαίων. Επιπλέον, για το 29% των περιστατικών DDoS, μια επιτυχημένη επίθεση είχε αρνητικό αντίκτυπο στην εταιρική

πιστοληπτική ικανότητα, ενώ στο 26% των περιπτώσεων προκάλεσε αύξηση των ασφαλίστρων.

1.5.7 Blended Επιθέσεις

Χρησιμοποιούν πολλαπλές μεθόδους λοίμωξης ή μετάδοσης. Για παράδειγμα, ένας συνδυασμός μεθόδους μόλυνσης μέσω πολλαπλασιασμό των ιών και των worms (Souppaya & Scarfone, 2012).

Κεφάλαιο 2

Πρακτικές Πρόληψης και Αντιμετώπισης Επιθέσεων Κακόβουλου Λογισμικού

Στο παρόν κεφάλαιο θα αναπτυχθούν οι πρακτικές πρόληψης και αντιμετώπισης των περιστατικών malware, δείχνοντας έτσι την σημαντικότητα και των δύο για τους οργανισμούς.

2.1 Πρακτικές Πρόληψης

Οι οργανισμοί θα πρέπει να σχεδιάσουν και να εφαρμόσουν προσαρμοσμένες μεθόδους πρόληψης των περιστατικών malware ανάλογα με το περιβάλλον του κάθε οργανισμού. Οι μέθοδοι πρόληψης ενός οργανισμού των περιστατικών malware είναι η ενσωμάτωση πολιτικής, τα προγράμματα εκπαίδευσης και ευαισθητοποίησης για το προσωπικό και γενικά για τους χρήστες, οι προσπάθειες μετριασμού της ευπάθειας και των απειλών και η χρήση αμυντικής αρχιτεκτονικής (Souppaya & Scarfone, 2012).

2.1.1 Πολιτική Οργανισμού

Αν ο οργανισμός δεν αναφέρει εκτιμήσεις πρόληψης malware στις πολιτικές του, είναι απίθανο να έχει τα σωστά και επιθυμητά αποτελέσματα πρόληψης. Οι πολιτικές ασφάλειας των Πληροφοριακών Συστημάτων, διαφέρουν από οργανισμό σε οργανισμό, και περιλαμβάνει το σκοπό και τους στόχους της πολιτικής ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των πληροφοριακών συστημάτων του οργανισμού. Η πολιτική ενός οργανισμού που σχετίζεται με την

πρόληψη malware πρέπει να παρέχει ευελιξία στην εφαρμογή της, ενώ ταυτόχρονα να είναι αρκετά σαφής και συγκεκριμένη. Η πολιτική αυτή θα πρέπει να περιλαμβάνει διατάξεις που σχετίζονται και με εργαζομένους από απόσταση, τόσο και εκείνων που χρησιμοποιούν υπολογιστές οι οποίοι ελέγχονται από τον οργανισμό καθώς επίσης και εκείνους που χρησιμοποιούν υπολογιστές εκτός ελέγχου του οργανισμού όπως φορητές συσκευές, υπολογιστές στο σπίτι κλπ.

Συνιστάται στον οργανισμό να εφαρμόζει και να ακολουθεί τακτικά πολιτική που να σχετίζεται με την πρόληψη των περιστατικών malware. Διατηρώντας τους υπολογιστές και τα λογισμικά που χρησιμοποιεί ο οργανισμός ενημερωμένα και δημιουργώντας λογαριασμούς χρηστών, οι οποίοι να μην είναι λογαριασμός διαχειριστή όπου αυτό είναι δυνατό έτσι ώστε να έχουν διαφορετικές ρυθμίσεις ασφαλείας είναι μια σωστή αρχή πρόληψης. Επίσης, πρέπει να ακολουθούνται και τα ακόλουθα θέματα πολιτικής όπως η σάρωση των εξωτερικών μέσων όπως usb, δίσκοι κλπ. για malware πριν να χρησιμοποιηθούν, καθώς επίσης και η σάρωση των συνημμένων αρχείων email πριν ανοιχτούν γιατί πολλές φορές ενδέχεται να περιέχουν κρυφά κάποιο επιζήμιο κακόβουλο πρόγραμμα.

Προτείνεται από τους Souppaya και Scarfone (2012) σε κάθε οργανισμό να περιορίσει ή να απαγορεύσει την χρήση περιττού λογισμικού, να απαγορεύσει στους υπαλλήλους του την αποστολή και τη λήψη ορισμένων τύπων αρχείων π.χ., αρχεία .exe μέσω e-mail, καθώς και να περιορίσει ή να απαγορεύσει την χρήση αφαιρούμενων μέσων π.χ., flash drives, κυρίως σε κεντρικούς υπολογιστές που βρίσκονται σε υψηλό κίνδυνο μόλυνσης. Επιπλέον, χρειάζεται προσοχή από τους υπαλλήλους κάθε οργανισμού η ανταλλαγή ή το κατέβασμα αρχείων χρησιμοποιώντας τις μεθόδους κοινής χρήσης αρχείων που χρησιμοποιούνται συχνά για να μεταφέρουν malware π.χ., υπηρεσίες κοινής χρήσης αρχείων. Σημαντική πολιτική είναι ο περιορισμός ή η απαγόρευση της χρήσης προσωπικών κινητών συσκευών που ανήκουν στα δίκτυα του οργανισμού για τηλεργασία ή απομακρυσμένη πρόσβαση, έτσι ώστε να μειωθεί το ενδεχόμενο πρόσληψης ιού στα συστήματα και δίκτυα του οργανισμού.

Οι οργανισμοί χρειάζονται να υιοθετήσουν ένα επίπεδο προσοχής για την είσοδο σε άγνωστους ιστότοπους ή αναδυόμενα παράθυρα που ισχυρίζονται ότι προσφέρουν δωρεάν λογισμικό. Απαραίτητη πολιτική ασφάλειας είναι η εγκατάσταση προληπτικού

λογισμικού όπως λογισμικό προστασίας από ιούς, λογισμικό φιλτραρίσματος περιεχομένου, που απαιτούνται για κάθε τύπο υποδοχής όπως τον e-mail server, τον web server, τον φορητό υπολογιστή, τα smart phones κλπ., και κάθε τύπο εφαρμογής όπως τον e-mail client, τον web browser κλπ.

Οι κωδικοί πρόσβασης είναι ένα κρίσιμο συστατικό της ασφάλειας των πληροφοριών των εταιρειών. Μία κακή επιλογή κωδικού μπορεί να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση και την εκμετάλλευση του ονόματος της εταιρείας. Οι πολιτικές που πρέπει να εφαρμόσει κάθε εταιρεία σε αυτό το τομέα είναι (SANS Policy Team, 2014 α,β):

- Δημιουργία ισχυρών κωδικών, οι οποίοι να περιέχουν 12 αλφαριθμητικούς χαρακτήρες, να περιέχουν πεζά και κεφαλαία γράμματα, να περιέχουν τουλάχιστον ένα αριθμό και ένα ειδικό χαρακτήρα (σημεία στίξης).
- Οι κωδικοί να μην περιέχουν λέξεις που μπορεί οποιοσδήποτε να εντοπίσει σε ένα λεξικό, δηλαδή να είναι λέξεις οι οποίες δεν είναι υπαρκτές, να μην περιέχουν προσωπικές πληροφορίες όπως ημερομηνίες γέννησης, ονόματα, αριθμούς τηλεφώνων κλπ., να μην περιέχουν πληροφορίες της εταιρείας, π.χ. διεύθυνση, κτίριο κλπ., να μην περιέχουν συνηθισμένες λέξεις γραμμένες προς τα πίσω όπως π.χ. terces – secret, ούτε να είναι λέξεις όπως password123, welcome123 κλπ. Επίσης, να μην είναι λέξεις όπως abcde, aabbcc, qwerty, 123.321 κλπ.
- Δεν πρέπει ποτέ οι χρήστες να αποθηκεύουν κωδικούς πρόσβασης στο browser τους και να μην το έχουν σαν σημείωση σε ένα χαρτί στον υπολογιστή, ούτε σαν note στο desktop του υπολογιστή.
- Πρέπει οι κωδικοί να είναι σύμφωνοι με το πρόγραμμα, αν π.χ. το πρόγραμμα ζητάει και σημείο στίξης, ή και κάποιο αριθμό θα πρέπει να είναι συμβατοί.
- Να μην χρησιμοποιούνται ίδιοι κωδικοί πρόσβασης με αυτούς στο σπίτι, να είναι διαφορετικοί αυτοί της εταιρείας και να μην είναι ίδιοι για όλα τα προγράμματα που χρησιμοποιούν. Επίσης, να χρησιμοποιούνται διαφορετικοί κωδικοί για την είσοδο σε κάθε σύστημα, έτσι ώστε αν χαθεί ένας κωδικός να μη δημιουργηθεί πρόβλημα και στα υπόλοιπα συστήματα.
- Όλοι οι κωδικοί πρόσβασης θα πρέπει να αλλάζονται τουλάχιστον σε τριμηνιαία βάση.
- Δεν πρέπει να μοιράζονται οι κωδικοί σε άλλους υπαλλήλους, πρέπει να είναι απολύτως εμπιστευτικοί.

- Δεν πρέπει ποτέ αν ζητηθεί στους χρήστες να δόσουν κωδικούς και πληροφορίες για την εταιρεία μέσω email ή μέσω οποιουδήποτε ηλεκτρονικού μέσου, ούτε και από το τηλέφωνο.
- Όποιος χρήστης έχει υποψιαστεί ότι έχει παραβιαστεί ο κωδικός πρόσβασης σε οποιοδήποτε πρόγραμμα της εταιρείας θα πρέπει να αναφέρει το περιστατικό στο υπεύθυνο άτομο.

Αναμφισβήτητα οι χρήστες πρέπει να χρησιμοποιούν κάποια πρωτόκολλα ασφαλείας στις ασύρματες συνδέσεις τους, έτσι ώστε να είναι πιο δύσκολο σε εισβολείς να έχουν πρόσβαση στις ασύρματες συσκευές και στις πληροφορίες των επιχειρήσεων. Οι πολιτικές που θα πρέπει να εφαρμοστούν σε αυτό το τομέα είναι (SANS Policy Team, 2014 γ):

- Όλες οι ασύρματες συσκευές που συνδέονται στο όνομα δικτύου της εταιρείας θα πρέπει να χρησιμοποιούν πρωτόκολλα όπως: - Extensible Authentication Protocol (EAP-FAST): γρήγορος και ασφαλής έλεγχος ταυτότητας χρήστη, - Translate Layer Security (EAP-TLS): πιστοποίηση ταυτότητας χρήστη.
- Χρήση Temporal Key Integrity Protocol (TKIP) είτε το προηγμένο σύστημα κρυπτογράφησης (AES), επίσης υπάρχει και η επιλογή των δύο (TKIP/AES).
- Για την χρήση Bluetooth πρέπει να χρησιμοποιούνται Secure Simple Pairing με ενεργή κρυπτογράφηση.
- Το όνομα δικτύου (SSID) θα πρέπει να είναι διαφορετικό από το όνομα της εταιρείας. Έτσι, ώστε αν υπάρχει παράβαση να μην είναι υπεύθυνη και να στοχοποιηθεί η εταιρεία.
- Όσο αφορά τηλεργαζόμενους ή υπαλλήλους ενωμένους σε vpn δίκτυο, χρειάζεται να ενεργοποιήσουν wifi protected access pre-shared key (WPA-PSK – μυστικό κλειδί 20 χαρακτήρων), EAP-FAST, EAP-TLS, να γίνει αλλαγή του προεπιλεγμένου ονόματος δικτύου SSID, επίσης να γίνει αλλαγή στο όνομα χρήστη και κωδικό χρήστη.

Αν κάποια ασύρματη συσκευή ή κάποιος τηλεργαζόμενος μολυνθεί από κάποιο ιό, θα προκαλέσει μεγάλη ζημιά και στην εταιρεία, θα υποκλαπούν δεδομένα και πληροφορίες της, οι οποίες είναι εμπιστευτικές, μπορούν οι ιοί αυτοί να μεταδοθούν σε ολόκληρό το δίκτυο της εταιρείας.

Επίσης, επιτρέποντας την εγκατάσταση εφαρμογών από τους χρήστες στα συστήματα της εταιρείας, υπάρχει κίνδυνος ευαίσθητα δεδομένα και εμπιστευτικές πληροφορίες της εταιρείας να παραβιαστούν, επίσης προγράμματα και υπολογιστές να μολυνθούν από

κακόβουλα λογισμικά. Οι πολιτικές που θα πρέπει να εφαρμόσουμε σε αυτό το τομέα είναι (SANS Policy Team, 2014 δ):

- Δεν θα πρέπει να γίνεται εγκατάσταση λογισμικών που δεν αποτελούν μέρος των λογισμικών της εταιρείας.
- Σε περίπτωση που κάποιος χρήστης χρειάζεται κάποιο λογισμικό θα πρέπει πρώτα να διερευνάται από το αρμόδιο τμήμα Πληροφορικής, το οποίο θα πρέπει να εγκρίνει για να παραχωρηθεί η πρόσβαση.
- Το τμήμα Πληροφορικής θα είναι υπεύθυνο για τις άδειες λογισμικού, τις δοκιμές και την εγκατάσταση του λογισμικού στους υπολογιστές της εταιρείας.

Οι οργανισμοί έχουν σημειώσει σημαντική πρόοδο στην εφαρμογή αποτελεσματικών τεχνολογιών ασφάλειας και διαδικασιών, αλλά υπάρχει ένα κενό στην ενσωμάτωση αυτών των προσπαθειών με τους ανθρώπους. Η τεχνολογική πολιτική και η πολιτική ασφαλείας δεν μπορούν να προστατεύσουν τα περιουσιακά στοιχεία των οργανισμών από τις επιθέσεις στον κυβερνοχώρο. Η τεχνολογία είναι χρήσιμη μόνο εάν εγκριθεί και γίνει αποδεκτή από τους ανθρώπους του οργανισμού (Siponen, 2000). Οι άνθρωποι παίζουν σημαντικό ρόλο στη διαμόρφωση της αποτελεσματικότητας των πολιτικών ασφάλειας των πληροφοριών σε έναν οργανισμό (Sherly & InduShobha, 2010).

Η έλλειψη όμως της ενημέρωσης σχετικά με τις πολιτικές ασφαλείας και των βέλτιστων πρακτικών έχει αναγνωριστεί από πολλούς μελετητές ασφάλειας ως μια σημαντική αιτία της αποτυχίας (Siponen, 2000, Puhakainen, 2006). Οι διαδικασίες κατάρτισης και ενημέρωσης πρέπει να αλλάζουν τακτικά, έτσι ώστε να παραμένουν επίκαιρες στο μεταβαλλόμενο περιβάλλον των οργανισμών. Αυτό απαιτεί συνεχή εκπαίδευση σε θέματα ασφάλειας για όλα τα επίπεδα ενός οργανισμού (Sherly & InduShobha, 2010).

2.1.2 Προγράμματα Ευαισθητοποίησης

Ο λήθαργος των χρηστών προς τις πρακτικές ασφαλείας, σε συνδυασμό με την επιθετικότητα των spammers και των hackers, είναι ένας πολύ επικίνδυνος συνδυασμός. Ωστόσο, οι οργανισμοί θα πρέπει να γνωρίζουν ότι δεν έχει σημασία πόσο μεγάλη προσπάθεια που κατέβαλαν για την πρόληψη των περιστατικών malware, τα περιστατικά θα εξακολουθούν να συμβαίνουν αν οι χρήστες δεν είναι ενημερωμένοι και κατάλληλα εκπαιδευμένοι στις πολιτικές ασφαλείας του οργανισμού (Sherly & InduShobha, 2010).

Τα προγράμματα ευαισθητοποίησης των οργανισμών θα πρέπει να περιλαμβάνουν κατευθύνσεις για τους χρήστες και το προσωπικό για την πρόληψη των περιστατικών malware. Βασικά στάδια των προγραμμάτων αυτών, συνιστάται να είναι τα εξής (OECD, 2002):

1. Ενημέρωση

Οι χρήστες πρέπει να ενημερώνονται για τους τρόπους εισαγωγής και μόλυνσης των υπολογιστών, γενικά τις κατηγορίες των απειλών οι οποίες αναφέρθηκαν πιο πάνω, τους κίνδυνους και τις επιπτώσεις στον οργανισμό που δημιουργεί ένα malware καθώς και την αδυναμία των τεχνικών ελέγχων για την πρόληψη των περιστατικών αυτών. Ο κάθε οργανισμός χρειάζεται να ενημερώνει τους χρήστες για την διαδικασία αντιμετώπισης των περιστατικών malware, για το πώς να μπορούν να προσδιορίσουν το πλήθος των υπολογιστών που μπορούν να μολυνθούν και την ζημιά που θα προκληθεί, για το πώς να καταγγείλουν ένα ύποπτο περιστατικό και για το πώς θα το χειριστούν.

Οι οργανισμοί χρειάζεται επίσης, να ενημερώνουν τους χρήστες σχετικά με τις τεχνικές κοινωνικής μηχανικής όπως το phishing που χρησιμοποιούνται για να ξεγελάσουν τους χρήστες στο να αποκαλύψουν πληροφορίες. Οι συστάσεις του οργανισμού προς τους χρήστες, δηλαδή τους υπαλλήλους του θα πρέπει να είναι το να μην απαντάνε ποτέ σε αιτήματα για οικονομικές ή προσωπικές πληροφορίες μέσω email. Αντ' αυτού, να επικοινωνούν με το άτομο ή τον οργανισμό στον νόμιμο αριθμό τηλεφώνου ή την ιστοσελίδα του. Επίσης, να μην χρησιμοποιούν τα στοιχεία επικοινωνίας που παρέχονται στο email, και να μην κάνουν κλικ σε οποιαδήποτε συνημμένα ή υπερ-συνδέσμους. Να μην δίνουν ποτέ τους κωδικούς πρόσβασης, PIN, ή άλλους κωδικούς πρόσβασης σαν απάντηση σε email ή ανεπιθύμητα αναδυόμενα παράθυρα και να εισάγουν αυτές τις πληροφορίες μόνο στο νόμιμο ιστότοπο ή εφαρμογή. Να μην ανοίγουν ύποπτα συνημμένα αρχεία email, ακόμη και αν προέρχονται από γνωστούς αποστολείς. Αν ληφθεί ένα απροσδόκητο συνημμένο, να επικοινωνούν με τον αποστολέα μέσω τηλεφώνου για να επιβεβαιωθούν ότι είναι ασφαλή. Καθώς επίσης, να μην απαντούν σε οποιαδήποτε ύποπτα ή ανεπιθύμητα ηλεκτρονικά μηνύματα (Siponen, 2000).

2. Ευθύνη

Όλοι οι συμμετέχοντες χρειάζεται να κατανοήσουν ότι είναι υπεύθυνοι για την ασφάλεια των πληροφοριακών συστημάτων και δικτύων του οργανισμό στον οποίο εργάζονται (OECD, 2002).

3. Ανταπόκριση

Οι συμμετέχοντες θα πρέπει να ενεργούν κατά τρόπο έγκαιρο και συντονισμένο για την πρόληψη, ανίχνευση και αντιμετώπιση των περιστατικών malware (OECD, 2002). Είναι εξίσου σημαντικό να δοθούν κίνητρα στους χρήστες για να ενσωματώσουν μια κουλτούρα ασφάλειας. Δεδομένου ότι η ασφάλεια αποτελεί δευτερεύοντα στόχο για τους χρήστες, δεν έχουν πάντα το κίνητρο να συμπεριφέρονται με ασφαλή τρόπο (Siponen, 2000, Stanton et al., 2005). Οι Culnan et al. (2008) τονίζουν ότι τα προγραμμάτα ευαισθητοποίησης είναι απαραίτητα για τη μείωση των κινδύνων που απορρέουν από τους υπολογιστές στο σπίτι και τις φορητές συσκευές που χρησιμοποιούνται σε μη ασφαλή δίκτυα μακριά από τον οργανισμό. Οι εργαζόμενοι πρέπει να κατανοήσουν τη σημασία της ασφάλειας των πληροφοριών, και να ενσωματώσουν μια κουλτούρα ασφάλειας όχι μόνο στο εσωτερικό του οργανισμού αλλά και έξω (Sherly & InduShobha, 2010).

4. Ηθική

Οι συμμετέχοντες θα πρέπει να σέβονται τα νόμιμα συμφέροντα των άλλων.

5. Δημοκρατία

Η ασφάλεια των πληροφοριακών συστημάτων και των δικτύων θα πρέπει να είναι συμβατή με τις βασικές αξίες μιας δημοκρατικής κοινωνίας (OECD, 2002).

6. Αξιολόγηση κινδύνου

Οι συμμετέχοντες θα πρέπει να διεξάγουν εκτιμήσεις κινδύνου. Οι επιχειρήσεις αντιμετωπίζουν σήμερα, το τιτάνιο έργο της δοκιμής, της ανάλυσης κώδικα χειροκίνητα και της παρακολούθησης του συνολικού επιπέδου του κινδύνου. Για πολλές επιχειρήσεις, τουλάχιστον δεκάδες χιλιάδες γραμμές κώδικα, χρειάζονται να επιθεωρούνται και αν βρεθεί κάποια που να είναι ευάλωτη, αφήνοντας σημαντικές πληροφορίες σε κίνδυνο, χρειάζεται να ληφθούν άμεσα μέτρα για την αντιμετώπιση των αδυναμιών (OECD, 2002, Blum, 2011).

7. Εφαρμογή σχεδίου ασφάλειας

Οι συμμετέχοντες μέσω των προγραμμάτων ευαισθητοποίησης χρειάζεται να κατανοήσουν πως η ενσωμάτωση της ασφάλειας των πληροφοριακών συστημάτων και δικτύων του οργανισμού είναι βασικό στοιχείο για τις επιχειρησιακές λειτουργίες (OECD, 2002). Οι οργανισμοί θα πρέπει να εκπαιδεύσουν τους υπαλλήλους να συνεχίσουν τις πρακτικές ασφάλειας πέρα από τη φυσική σφαίρα της οργάνωσης. Το μεταβαλλόμενο περιβάλλον εργασίας απαιτεί οποτεδήποτε και οπουδήποτε επικοινωνία μέσω διάφορων κινητών συσκευών. Δεδομένης της αύξησης της τηλεργασίας του εργατικού δυναμικού, στόχος των οργανισμών απαιτείται να είναι και η προστασία των συστημάτων εκτός του οργανισμού που χρησιμοποιούνται απομακρυσμένα (Cisco, 2006). Επιπλέον, ο υπολογιστής στο σπίτι ενός εργαζομένου μπορεί να χρησιμοποιηθεί και από άλλα μέλη της οικογένειας, τα οποία δεν είναι εκπαιδευμένα στην ασφάλεια των υπολογιστών από τις διάφορες απειλές που υπάρχουν. Οι οργανισμοί επίσης μπορούν να συμβάλουν στη βελτίωση της ασφάλειας των υπολογιστών που χρησιμοποιούν οι εργαζόμενοι στο σπίτι παρέχοντάς τους εργαλεία ασφάλειας, όπως anti-virus και firewalls σε μειωμένη τιμή (Sherly & InduShobha, 2010).

8. Διαχείριση ασφάλειας

Οι συμμετέχοντες χρειάζεται να υιοθετήσουν μια ολοκληρωμένη προσέγγιση για τη διαχείριση της ασφάλειας (Siponen, 2000). Για την αποφυγή των περιστατικών malware πρέπει να απαγορευτεί στο προσωπικό του κάθε οργανισμού να ανοίγει ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή συνημμένα, ή να κάνουν κλικ σε άγνωστους συνδέσμους ή εφαρμογές από μη έμπιστες πηγές, από άγνωστους ή γνωστούς αποστολείς, ή να επισκέπτονται ιστοσελίδες που είναι πιθανό να περιέχουν κακόβουλο περιεχόμενο. Η σωστή τακτική για την αποφυγή των περιστατικών αυτών είναι και το να μην κάνουν κλικ σε ύποπτα αναδυόμενα παράθυρα του web browser που χρησιμοποιεί ο συγκεκριμένος οργανισμός, να μην ανοίγουν αρχεία με επεκτάσεις αρχείων που είναι πιθανό να συνδέονται με κακόβουλο λογισμικό όπως π.χ., .bat, .com, .exe, .pif, .vbs. Επίσης, να μην απενεργοποιήσουν τους μηχανισμούς ελέγχου ασφάλειας κακόβουλου λογισμικού (π.χ. το λογισμικό προστασίας από ιούς, το λογισμικό φιλτραρίσματος περιεχομένου, το προσωπικό τείχος προστασίας κλπ) και να μην γίνεται χρήση από μη εξουσιοδοτημένα άτομα μόνο χρήση από άτομα που βρίσκονται σε επίπεδο διαχειριστή λογαριασμών.

9. Επανεκτίμηση

Οι συμμετέχοντες επίσης, χρειάζεται να επανεξετάσουν και να επαναξιολογήσουν την ασφάλεια των πληροφοριακών συστημάτων και δικτύων, και να προβούν στις κατάλληλες τροποποιήσεις των πολιτικών ασφάλειας, των πρακτικών, των μέτρων και των διαδικασιών (OECD, 2002).

Αν και η ευαισθητοποίηση είναι αναγκαία για τη συμμετοχή των τελικών χρηστών στο πλαίσιο των προσπαθειών της ασφάλειας, κάνεις δεν εγγυάται τη συμμόρφωση των εργαζομένων με τις πολιτικές ασφάλειας (Sherly & InduShobha, 2010). Οι οργανισμοί λοιπόν, δεν θα πρέπει να βασίζονται στην ευαισθητοποίηση των χρηστών ως κύρια μέθοδο της πρόληψης των περιστατικών malware. Αντ' αυτού, τα προγράμματα ευαισθητοποίησης θα πρέπει να συμπληρώνουν τις τεχνικές ελέγχου (που περιγράφονται στην συνέχεια του άρθρου) για να παρέχουν πρόσθετη προστασία έναντι στα περιστατικά αυτά (OECD, 2002).

2.1.3 Περιορισμός Ευπάθειας

Η ευπάθεια περιλαμβάνει τα εξής χαρακτηριστικά: τα λάθη και τα κενά ασφαλείας που υπάρχουν σε ένα σύστημα. Η πρόσβαση κάποιου εισβολέα σε αυτά τα λάθη και η δυνατότητα να εκμεταλλευτεί τα κενά αυτά έχουν ως αποτέλεσμα να τίθεται σε κίνδυνο η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πόρων του συστήματος. Τα κενά ασφαλείας προκύπτουν από προγραμματιστικά σφάλματα που μπορεί να προκλήθηκαν κατά την ανάπτυξη του συστήματος. Σκοπός των κατασκευαστών malware είναι να μεταδοθεί το προϊόν τους όσο το δυνατόν πιο εύκολα και όσο το δυνατόν σε περισσότερους στόχους, εκμεταλλευόμενοι τα κενά ασφαλείας με τη μεγαλύτερη δημοτικότητα (Παπαθανάση, 2012).

Οι οργανισμοί χρειάζεται να έχουν τεκμηριώσει τις διαδικασίες για τον περιορισμό των τρωτών σημείων που θα μπορούσε να εκμεταλλευτεί ένα malware. Μία ευπάθεια μπορεί να περιοριστεί με μία ή περισσότερες μεθόδους, όπως είναι η εφαρμογή patches για την ενημέρωση του λογισμικού ή την αναμόρφωση του (π.χ., απενεργοποιώντας μια ευάλωτη υπηρεσία) καθώς και με τον κατάλληλο συνδυασμό τεχνικών, συμπεριλαμβανομένων των τεχνολογιών αυτοματισμού ασφαλείας. Τεχνολογίες αυτοματισμού ασφαλείας μπορούν να χρησιμοποιήσουν λίστες ελέγχου για την

εφαρμογή ρυθμίσεων που βελτιώνουν το προεπιλεγμένο επίπεδο ασφαλείας και την συνεχή παρακολούθησή τους για την βεβαίωση ότι είναι ακόμα σε συμμόρφωση με τις ρυθμίσεις του πίνακα ελέγχου.

Εάν ένα περιστατικό συμβεί, προνόμιο θα είναι να ελαχιστοποιηθεί το ύψος της ζημιάς που το κακόβουλο λογισμικό μπορεί να προκαλέσει. Οι οργανισμοί θα πρέπει να εφαρμόσουν μέτρα όπως η εξάλειψη ανεπιθύμητων αρχείων, η αφαίρεση ή η αλλαγή των ονομάτων χρηστών και κωδικών πρόσβασης προεπιλογής στα λειτουργικά συστήματα και τις εφαρμογές του οργανισμού, έτσι ώστε να μειώσουν περαιτέρω την ύπαρξη περιστατικών malware.

Για τον περιορισμό της ευπάθειας απαραίτητα μέτρα που απαιτείται να λάβει σοβαρά υπόψη του ο οργανισμός είναι η απενεργοποίηση αυτόματης εκτέλεσης εκτελέσιμων αρχείων (π.χ. AutoRun), η αλλαγή των τύπων προεπιλεγμένων αρχείων που χρησιμοποιούνται πιο συχνά από περιστατικά malware καθώς και η απενεργοποίηση περιττών χαρακτηριστικών και δυνατοτήτων από τα προγράμματα ηλεκτρονικού ταχυδρομείου, τους φυλλομετρητές (web browser), τους επεξεργαστές κειμένου κλπ, ιδιαίτερα εκείνων που είναι συνήθως αντικείμενο εκμετάλλευσης από malware.

Όταν ληφθούν τα παραπάνω μέτρα τότε θα περιοριστεί κατά πολύ η ευπάθεια από τα συστήματα και το δίκτυο του οργανισμού.

Ευπάθεια – Κίνδυνοι	%
Οι χρήστες επισκέπτονται ιστοσελίδες που θα μπορούσαν να εισάγουν κακόβουλο λογισμικό στο δίκτυο (της επιχείρησης)	51
Ένας νέος ιός, worm ή Trojan που εισέρχεται μέσω e-mail και βλάπτει το δίκτυο, τα δεδομένα, κλπ.	41
Ένας νέος ιός, worm ή Trojan που εισέρχεται μέσω μιας κινητής συσκευής βλάπτει το δίκτυό, τα δεδομένα, κλπ.	39

Ένας νέος ιός, worm ή Trojan ο οποίος εισέρχεται μέσω άμεσων μηνυμάτων βλάπτει το δίκτυό σας, δεδομένων, κλπ.	29

Πίνακας 1. Αισθητοί κίνδυνοι από ποικίλα προβλήματα ασφαλείας - % Αντιμετώπιση σοβαρού ή πολύ σοβαρού κινδύνου (Rizwan et al., 2011).

2.1.4 Περιορισμός Απειλής

Πολλοί οργανισμοί έχουν στραφεί σε ιστοσελίδες κοινωνικής δικτύωσης όπως το Facebook και το Twitter για την ανταλλαγή πληροφοριών μεταξύ των εργαζομένων τους. Ως εκ τούτου, οι οργανισμοί πρέπει να εξετάσουν επίσης τον τρόπο που εμπλέκονται οι εργαζόμενοι τους με αυτές τις ιστοσελίδες έτσι ώστε να μετριάσουν τις απειλές των περιστατικών malware (Sherly & InduShobha, 2010).

Για να περιοριστεί η απειλή γενικά, απαιτείται πρώτα να ανιχνευτεί και στην συνέχεια να γίνει προσπάθεια από τον οργανισμό να το σταματήσει προτού να επηρεάσει τις διαδικασίες του οργανισμού και να πραγματοποιήσει τους καταστροφικούς του στόχους.

Για να αποφύγει ένας οργανισμός την μόλυνση το δίκτυο υπολογιστών του με ιούς, θα μπορούσε να περιορίσει την χρήση των υπηρεσιών του ηλεκτρονικού ταχυδρομείου μόνο στο προσωπικό διαχείρισης και να απαγορεύσει το άνοιγμα των συνημμένων αρχείων. Αυτό όμως είναι ένα σοβαρό εμπόδιο για την ανάπτυξη των σύγχρονων επιχειρηματικών πρακτικών και δεν θα μπορούσε να αποτελέσει λύση. Η πιο αποτελεσματική μέθοδος για προστασία από κακόβουλο λογισμικό είναι η εγκατάσταση ενός antivirus σαρωτή (Μπίρδα, 2012).

Επιβάλλεται στους οργανισμούς η ανάπτυξη λογισμικών προστασίας από ιούς για όλους τους κεντρικούς υπολογιστές τους, επίσης και η εγκατάσταση πρόσθετων τεχνικών έλεγχου χρήσιμες για τον περιορισμό απειλής όπως είναι τα συστήματα αποτροπής εισβολέων (Intrusion Prevention System – IPS) και συστήματα ανίχνευσης

εισβολέων (Intrusion Detection System IDS), τα firewalls, το φιλτράρισμα περιεχομένου και οι εφαρμογές whitelisting.

2.1.5 Χρήση Αμυντικής Αρχιτεκτονικής

Οι οργανισμοί χρειάζεται να εξετάσουν πιθανές τροποποιήσεις της αμυντικής αρχιτεκτονικής που χρησιμοποιούν έτσι ώστε να μετριάσουν τα περιστατικά malware που εξακολουθούν να συμβαίνουν.

Η χρήση των εργαλείων αφαίρεσης κακόβουλου λογισμικού είναι όλο και πιο διαδεδομένη και μπορεί να καταπολεμήσει και να αφαιρέσει όλα τα είδη malware. Υψηλής ποιότητας λογισμικό προστασίας από τους ιούς με χαμηλό κόστος που θα μπορούσαν να εγκαταστήσουν μικρές και μεγάλες επιχειρήσεις είναι τα συστήματα κλώνος (clone systems), το Tenable Security Network καθώς και Qualys (Blum, 2011).

Υπάρχουν τρεις σημαντικές τεχνικές που μπορούν να μετριάσουν τα περιστατικά malware. Η πρώτη τεχνική, η τεχνική sandboxing είναι ένα πρότυπο ασφαλείας όπου οι εφαρμογές εκτελούνται μέσα σε ένα ελεγχόμενο περιβάλλον που περιορίζει τις ενέργειες των εφαρμογών που μπορούν να εκτελέσουν έτσι ώστε να απομονωθούν οι απειλές από άλλες εφαρμογές. Μια άλλη τεχνική είναι ο διαχωρισμός browser, ο οποίος περιλαμβάνει τη χρήση διαφορετικών προγραμμάτων περιήγησης στο Web για διαφορετικούς τύπους πρόσβασης σε ιστοσελίδες (εταιρικές εφαρμογές, γενική πρόσβαση, κλπ.) οι χρήστες μπορούν να χρησιμοποιήσουν ένα εμπορικό σήμα του browser για τις εταιρικές εφαρμογές και ένα άλλο εμπορικό σήμα του browser για όλες τις άλλες εφαρμογές. Αυτό διαχωρίζει τα ευαίσθητα εταιρικά δεδομένα μέσα σε ένα browser, από τα δεδομένα μέσα στο άλλο browser, παρέχοντας καλύτερη προστασία των εταιρικών δεδομένων και μειώνοντας την πιθανότητα ότι το malware θα επηρεάσει εταιρικές εφαρμογές. Τέλος, ο διαχωρισμός μέσω της τεχνικής virtualization μπορεί να χρησιμοποιηθεί από ένα οργανισμό για να διαχωρίσει εφαρμογές και λειτουργικά συστήματα, με πολύ μεγάλη αυστηρότητα. Για παράδειγμα, ένας οργανισμός μπορεί να έχει ένα λειτουργικό σύστημα π.χ. για εταιρικές εφαρμογές και ένα άλλο λειτουργικό σύστημα για όλες τις άλλες δραστηριότητες, συμπεριλαμβανομένης της περιήγησης στο web. Συμπερασματικά, η χρήση των παραπάνω αμυντικών αρχιτεκτονικών από τους οργανισμούς, μειώνονται οι επιπτώσεις των περιστατικών malware.

2.2 Πρακτικές Αντιμετώπισης

Η διαδικασία της αντιμετώπισης ενός περιστατικού malware αποτελείται από τις εξής κύριες στρατηγικές: την προετοιμασία, την ανίχνευση και την ανάλυση, τον περιορισμό / την εξάλειψη / αποκατάσταση και τη δραστηριότητα μετά το περιστατικό (post-incident activity) (Souppaya & Scarfone, 2012).

2.2.1 Στρατηγική Προετοιμασίας

Η αρχική φάση της αντιμετώπισης ενός συμβάντος κακόβουλου λογισμικού, δηλαδή το στάδιο της προετοιμασίας**,** αποτελεί την εκτέλεση προκαταρκτικών δραστηριοτήτων οι οποίες αποσκοπούν στην ετοιμότητα του οργανισμού να αντιμετωπίσει πιθανά περιστατικά malware έχοντας ως στόχο αρχικά να τα ανιχνεύσει αλλά και να τα αποφύγει, να μπορέσει να περιορίσει τον κίνδυνο, να τα εξαλείψει και να αποκαταστήσει τα συστήματα που υπέστησαν βλάβη.

Οι προκαταρκτικές αυτές δραστηριότητες λοιπόν, αφορούν την δημιουργία και την διατήρηση σχετικών γνώσεων με το κακόβουλο λογισμικό μέσα στην ομάδα αντιμετώπισης περιστατικών κακόβουλου λογισμικού (ειδικών ασφαλείας), οι οποίες πρέπει να αποκτήσουν γνώσεις και πλήρη κατανόηση των μεθόδων μόλυνσης και εξάπλωσης που χρησιμοποιεί το malware. Οι ειδικοί ασφαλείας οφείλουν να γνωρίζουν τα λογισμικά και εργαλεία ανίχνευσης που διαθέτει ο οργανισμός, αλλά και να έχουν την ικανότητα να αναλύουν τα υποστηρικτικά δεδομένα και να αναγνωρίζουν τα χαρακτηριστικά των απειλών καθώς επίσης και την ικανότητα να αξιολογούν τις πιθανές επιπτώσεις ώστε να είναι σε θέση να προτείνουν λύσεις για τον περιορισμό, την εξάλειψη και την αποκατάσταση των συστημάτων. Πολύ χρήσιμο ακόμη για έναν οργανισμό είναι οι ειδικοί ασφαλείας που διαθέτει να είναι καλοί γνώστες προγραμματισμού ώστε ο οργανισμός να μπορεί να βασιστεί πάνω τους για την διαχείριση των ευπαθειών του, για νέους ιούς που πιθανόν να εμφανιστούν κτλ.

Εκτός από τα παραπάνω θα πρέπει να παρέχεται στους διαχειριστές ασφαλείας σχετική εκπαίδευση (εκπαιδευτικά ενημερωτικά προγράμματα) και εξάσκηση, ώστε να μάθουν νέους τρόπους για να χτίσουν και να διατηρήσουν τις γνώσεις αυτές. Μια πιθανή λύση θα ήταν οι διαχειριστές συμβάντων / περιστατικών να δουλέψουν προσωρινά ως antivirus engineers ώστε να αποκτήσουν περεταίρω νέες τεχνικές

γνώσεις και να εξοικειωθούν περισσότερο με τις διαδικασίες και τις πρακτικές αντιμετώπισης.

Μια άλλη προκαταρκτική ενέργεια στο στάδιο της προετοιμασίας είναι η ανάπτυξη συγκεκριμένων πολιτικών και διαδικασιών για τη διαχείριση συγκεκριμένων συμβάντων κακόβουλου λογισμικού αλλά και για θέματα που αφορούν την ανίχνευση ευπαθειών, τη φυσική ασφάλεια, τον έλεγχο πρόσβασης, τα διάφορα προγράμματα που χρησιμοποιούνται για την ανίχνευση και άμυνα, τα paches, τις ενημερώσεις κ.ά (Souppaya & Scarfone, 2012).

Επίσης, σημαντικό παράγοντα στο στάδιο της προετοιμασίας είναι η απόκτηση των απαραίτητων εργαλείων (υλικού και λογισμικού) και των πόρων ώστε να βοηθηθεί η διαχείριση αντιμετώπισης περιστατικών κακόβουλο λογισμικού. Ένας οργανισμός θα πρέπει να διασφαλίσει ότι διαθέτει τα κατάλληλα εργαλεία καθώς και τους πόρους εκείνους που θα τον βοηθήσουν στην διαχείριση των περιστατικών malware, ώστε να είναι καλύτερα και καταλληλότερα προετοιμασμένος (εργαλεία ανάλυσης, συστήματα, και άλλοι σχετικοί πόροι).

Η διευκόλυνση της επικοινωνίας και του συντονισμού μέσα στον οργανισμό είναι επίσης πολύ σημαντικός παράγοντας στην καλή προετοιμασία για την αντιμετώπιση τέτοιων περιστατικών. Ένα από τα πιο κοινά προβλήματα στην διαχείριση ενός περιστατικού κακόβουλου λογισμικού είναι η φτωχή επικοινωνία και συντονισμός των όσων εμπλέκονται στην διαχείριση του περιστατικού, λόγω περιορισμένης εικόνας του συμβάντος ή κατανόησης της κατάστασης. Για να βελτιωθεί η επικοινωνία και ο συντονισμός θα πρέπει ο οργανισμός να ορίσει εκ των προτέρων μερικά άτομα ή μια μικρή ομάδα που θα είναι υπεύθυνη για το συντονισμό της ανταπόκρισης του οργανισμού σε περιστατικά κακόβουλου λογισμικού. Ο συντονιστής θα πρέπει να διατηρεί συνεχή επίγνωση της κατάστασης συγκεντρώνοντας όλες τις σχετικές πληροφορίες, να λαμβάνει αποφάσεις που είναι προς όφελος του οργανισμού, και να μεταβιβάζει τις σχετικές πληροφορίες και αποφάσεις σε όλα τα εμπλεκόμενα μέρη εγκαίρως.

Ο ανθρώπινος παράγοντας σε περιστατικά κακόβουλου λογισμικού έχει ιδιαίτερη σημασία, γι' αυτό σε όλα τα εμπλεκόμενα μέρη που αυτοί είναι οι χρήστες θα πρέπει να

τους δοθούν οι κατάλληλες οδηγίες για το πώς να αποφύγουν τυχόν μολύνσεις, για το πώς να αναγνωρίζουν τα σημάδια κάποιας μόλυνσης, και τι θα πρέπει να κάνουν σε περίπτωση που ο ξενιστής τους έχει μολυνθεί. Ο συντονιστής πρέπει επίσης να παρέχει τεχνικές κατευθυντήριες γραμμές και οδηγίες σε όλο το προσωπικό για περιορισμό, εξάλειψη και αποκατάσταση, καθώς και εκ μέρους της διαχείρισης να δίνει τακτικές ενημερώσεις σχετικά με την κατάσταση της ανταπόκρισης στο συμβάν, αλλά και των σημερινών και πιθανών μελλοντικών επιπτώσεων του συμβάντος. Ο συντονιστής επίσης, θα πρέπει να αλληλεπιδρά με εξωτερικούς φορείς, όπως άλλες ομάδες αντιμετώπισης περιστατικών που αντιμετωπίζουν παρόμοια προβλήματα malware.

2.2.2 Στρατηγική Ανίχνευσης και Ανάλυσης

Η δεύτερη φάση για την αντιμετώπιση περιστατικών malware είναι εκείνη της ανίχνευσης και ανάλυσης. Η «ανίχνευση εισβολών» ορίζεται ως το πρόβλημα του εντοπισμού πράξεων που έχουν σαν σκοπό να διαβάλλουν την ακεραιότητα, την αξιοπιστία ή την διαθεσιμότητα ενός υπολογιστικού πόρου (Κρασανάκη, 2010).

Οι οργανισμοί θα πρέπει να προσπαθήσουν να εντοπίζουν και να επικυρώσουν τα περιστατικά malware όσο το συντομότερο δυνατόν, ώστε να ελαχιστοποιηθεί ο αριθμός των ξενιστών που θα μολυνθούν και η ζημιά που έχει υποστεί ο οργανισμός. Επίσης, τα περιστατικά αυτά πρέπει να καταγραφούν και να παρατηρηθούν. Η μελέτη της συμπεριφοράς του malware μπορεί να γίνει είτε ενεργά, δηλαδή εκτελώντας το malware, είτε forensically, δηλαδή εξετάζοντας τον μολυσμένο ξενιστή για να αποδειχθεί η ύπαρξη κακόβολου λογισμικού στον οργανισμό. Αυτό περιλαμβάνει αναγνώριση χαρακτηριστικών της δραστηριότητας του κακόβουλου λογισμικού εξετάζοντας τις πηγές ανίχνευσης, όπως antivirus, συστήματα πρόληψης εισβολών και τεχνολογίες διαχείρισης ασφάλειας πληροφοριών κτλ.

Οι διαχειριστές του συμβάντος μέσα στον οργανισμό θα πρέπει να διαθέτουν τις ικανότητες ώστε να μπορούν να αποφασίσουν για τον τύπο, την έκταση και την προτεραιότητα που θα πρέπει να δώσουν στο συμβάν. Μερικές κατευθυντήριες γραμμές που οι ειδικοί ασφαλείας και οι χρήστες των συστημάτων θα πρέπει να ακολουθούν ώστε να αναγνωρίζουν τα χαρακτηριστικά του κάθε περιστατικού, των μολυσμένων ξενιστών, και να βάζουν την κατάλληλη προτεραιότητα αντιμετώπισης και

ανάλυσης στα συμβάντα κακόβουλου λογισμικού είναι τα παρακάτω (Souppaya & Scarfone, 2012):

Οι ειδικοί ασφαλείας μέσα στον οργανισμό οφείλουν να έρχονται σε επαφή με τους προμηθευτές λογισμικού αντιμετώπισης malware ώστε να ενημερώνονται σχετικά με τις τελευταίες σημαντικές απειλές malware και να ενημερώνουν κατάλληλα τους χρήστες / υπαλλήλους του οργανισμού καθώς και να εγγραφούν στις συμβουλευτικές λίστες malware (malware advisory mailing lists) ώστε να λαμβάνουν άμεσα προειδοποιήσεις για νέες απειλές που θα μπορούσαν να επηρεάσουν τον οργανισμό τις επόμενες μέρες ή ακόμη και ώρες. Επιπρόσθετα, οι ειδικοί ασφαλείας θα μπορούσαν να ενημερωθούν και από τις αναφορές για το νέο malware από τις λίστες αλληλογραφίας γενικής ασφάλειας (general security mailing lists) καθώς και από συναδέλφους τους σε άλλους οργανισμούς οι οποίοι έχουν ήδη πληγεί από κάποιο περιστατικό malware.

Ένα άλλο μέτρο που μπορούν να λάβουν οι επιχειρήσεις είναι να πληρώσουν για τις υπηρεσίες έγκαιρης προειδοποίησης και ανάλυσης των αναδυόμενων απειλών με σκοπό την παροχή αξιόπιστων πληροφοριών.

Επιτακτική ανάγκη για κάθε οργανισμό αποτελεί η ανάλυση κάθε ύποπτου περιστατικού που έτυχε σε αυτόν και η επικύρωση ότι πρόκειται πράγματι για κακόβουλο λογισμικό. Η ανάλυση ενός περιστατικού κάποιες φορές απαιτεί εκτεταμένες τεχνικές γνώσεις και εμπειρία από τους ειδικούς για να επικυρωθεί ένα συμβάν ότι προκλήθηκε από malware, ειδικά όταν το malware είναι καινούριο και άγνωστο.

Σημαντικό είναι οι οργανισμοί να έχουν την ικανότητα να ανιχνεύουν και να αναγνωρίζουν ποιοί ξενιστές έχουν μολυνθεί από κακόβουλο λογισμικό, ώστε να υποστούν τις κατάλληλες ενέργειες για περιορισμό, εξάλειψη και αποκατάσταση. Οι οργανισμοί πρέπει να εξετάσουν προσεκτικά τα ζητήματα ταυτοποίησης των ξενιστών προτού συμβεί κάποιο περιστατικό κακόβουλου λογισμικού μεγάλης κλίμακας, ώστε να είναι προετοιμασμένοι να χρησιμοποιήσουν πολλαπλές στρατηγικές για ταυτοποίηση των μολυσμένων ξενιστών. Επίσης, οι οργανισμοί θα πρέπει να επιλέξουν ένα επαρκώς ευρύ φάσμα προσεγγίσεων ταυτοποίησης (identification approaches) και να αναπτύξουν διαδικασίες και τεχνικές ικανότητες για να εκτελέσουν κάθε επιλεγμένη

προσέγγιση αποτελεσματικά όταν εμφανιστεί κάποιο περιστατικό κακόβουλου λογισμικού.

Στο πλαίσιο της ανάλυσης και της διαδικασίας της επικύρωσης λοιπόν, οι διαχειριστές ασφαλείας πρέπει να προσδιορίσουν τα χαρακτηριστικά της δραστηριότητας του malware εξετάζοντας τις πηγές ανίχνευσης. Η κατανόηση των χαρακτηριστικών αυτών είναι πολύ χρήσιμη για τη χορήγηση της κατάλληλης προτεραιότητας στο κάθε περιστατικό και για το σχεδιασμό πιο αποτελεσματικού περιορισμού, εξάλειψης και αποκατάστασης. Επίσης, σημαντικό είναι οι ειδικοί ασφαλείας να συνεργάζονται άψογα με όλους τους εμπλεκόμενους στα συστήματα των οργανισμών με σκοπό να εντοπιστούν οι πηγές δεδομένων οι οποίες μπορούν να βοηθήσουν στο να ανιχνευθούν πληροφορίες malware, αναγνωρίζοντας και τι τύπους πληροφορίας κάθε πηγή δεδομένων μπορεί να καταγράφει.

Τα χαρακτηριστικά που πρέπει να αναγνωριστούν είναι η κατηγορία του malware (π.χ. virus, worm κτλ), τις υπηρεσίες και τους ξενιστές που έχουν μολυνθεί, τις ευπάθειες που εκμεταλλεύτηκε το malware, ποιες είναι οι εκδόσεις των λειτουργικών συστημάτων, συσκευών, εφαρμογών κλπ. που επηρεάστηκαν, με ποιό τρόπο το malware μολύνει το σύστημα και πώς το επηρεάζει, πώς μεταδίδεται και τέλος με ποιό τρόπο μπορεί να αφαιρεθεί.

Εκτός από τις προφανείς πηγές δεδομένων, όπως το λογισμικό προστασίας από ιούς (antivirus), χειριστές περιστατικών malware θα πρέπει να γνωρίζουν και να χρησιμοποιούν δευτερεύουσες τεχνικές ανίχνευσης, όπως είναι firewall, συστήματα ανίχνευσης εισβολών (IDS-Intrusion Detection Systems), συστήματα πρόληψης εισβολών (IPS-Intrusion Prevention Systems), προγράμματα Antispyware, anti-adware κτλ.

2.2.3 Στρατηγική Περιορισμού, Εξάλειψης και Αποκατάστασης

Το επόμενο στάδιο της αντιμετώπισης είναι το στάδιο του περιορισμού, της εξάλειψης και της αποκατάστασης ενός περιστατικού malware (Souppaya & Scarfone, 2012).

Ο περιορισμός ενός συμβάντος κακόβουλου λογισμικού έχει δυο κύρια μέρη: να σταματήσει την εξάπλωση του κακόβουλου λογισμικού, επίσης να αποτρέψει και να

σταματήσει περεταίρω βλάβες στους ξενιστές. Σχεδόν κάθε περιστατικό κακόβουλου λογισμικού απαιτεί περιοριστικές ενέργειες. Κατά την αντιμετώπιση ενός περιστατικού, είναι σημαντικό για έναν οργανισμό να αποφασίσει ποιές θα είναι οι περιοριστικές μέθοδοι αντιμετώπισης που θα χρησιμοποιήσει. Οι στρατηγικές περιορισμού πρέπει να υποστηρίζουν τους χειριστές περιστατικών στην επιλογή των κατάλληλων συνδυασμών των μεθόδων περιορισμού με βάση τα χαρακτηριστικά της συγκεκριμένης κατάστασης.

Από την πλευρά της επιχείρησης θα ήταν χρήσιμο να παρέχονται οδηγίες στους χρήστες για το πώς να αναγνωρίζουν μολύνσεις και ποιά μέτρα πρέπει να λάβουν σε περίπτωση που κάποιος ξενιστής μολυνθεί, ωστόσο οι οργανισμοί δεν θα πρέπει να βασίζονται κατά κύριο λόγο στους χρήστες για περιστατικά που περιέχουν κακόβουλο λογισμικό.
Σε περίπτωση που το κακόβουλο λογισμικό δεν μπορεί να αναγνωριστεί και δεν περιλαμβάνεται από ενημερωμένο λογισμικό προστασίας από ιούς (antivirus), οι οργανισμοί χρειάζεται να είναι προετοιμασμένοι στο να χρησιμοποιούν άλλα εργαλεία ασφαλείας για να το συμπεριλάβουν. Οι οργανισμοί θα πρέπει επίσης, να είναι έτοιμοι να υποβάλουν αντίγραφα από το άγνωστο malware στους προμηθευτές του λογισμικού ασφαλείας τους για να το αναλύσουν, καθώς επίσης και να έλθουν σε επαφή με αξιόπιστους οργανισμούς αντιμετώπισης περιστατικών και πωλητές antivirus όταν χρειάζονται περαιτέρω καθοδήγηση στην διαχείριση νέων απειλών.
Επιπρόσθετα, οι οργανισμοί χρειάζεται να είναι προετοιμασμένοι να τοποθετήσουν επιπλέον προσωρινούς περιορισμούς στη συνδεσιμότητα του δικτύου που περιέχεται το περιστατικό malware, όπως αναστολή της πρόσβασης στο διαδίκτυο ή φυσική αποσύνδεση των ξενιστών από τα δίκτυα, αναγνωρίζοντας τις επιπτώσεις τις οποίες μπορούν να έχουν στις οργανωτικές λειτουργίες. Επίσης, οι οργανισμοί θα πρέπει να είναι προετοιμασμένοι να κλείσουν ή να μπλοκάρουν υπηρεσίες που χρησιμοποιούνται από το κακόβουλο λογισμικό ενώ χρειάζεται να κατανοήσουν τις συνέπειες ενός τέτοιου εγχειρήματος. Συνιστάται στους οργανισμούς να είναι έτοιμοι να ανταποκριθούν στα προβλήματα που προκαλούνται από άλλους οργανισμούς απενεργοποιώντας τις δικές τους υπηρεσίες κατά τη διάρκεια αντιμετώπισης ενός περιστατικού malware.

Ο πρωταρχικός στόχος της εξάλειψης ενός περιστατικού malware είναι η κατάργηση του κακόβουλου λογισμικού από τους μολυσμένους ξενιστές. Λόγω της ενδεχόμενης

ανάγκης για εκτεταμένες προσπάθειες εξάλειψης, οι οργανισμοί χρειάζεται να είναι προετοιμασμένοι στο να χρησιμοποιήσουν ποικιλία συνδυασμών τεχνικών εξάλειψης συγχρόνως για διαφορετικές καταστάσεις. Επίσης, θα πρέπει να εξετάσουν την εκτέλεση δραστηριοτήτων ευαισθητοποίησης οι οποίες θέτουν προσδοκίες για προσπάθειες εξάλειψης και αποκατάστασης. Αυτές οι δραστηριότητες μπορούν να είναι χρήσιμες για τη μείωση του στρες που μπορούν να προκαλέσουν μεγάλα περιστατικά κακόβουλου λογισμικού.

Σε περίπτωση που ένας ή περισσότεροι επιτιθέμενοι αποκτήσουν πρόσβαση επιπέδου διαχειριστή στο σύστημα, ή υπάρχει ελεύθερη πρόσβαση σε όλους σε επίπεδο διαχειριστή, ή ορισμένα αρχεία ανακυκλώθηκαν κατά τη διάρκεια της μόλυνσης, ή το σύστημα είναι ασταθές και μη λειτουργικό μετά το στάδιο της εξάλειψης τότε ο οργανισμός θα πρέπει να σκεφτεί σοβαρά την ανοικοδόμηση του συστήματος ενώ εάν δεν έχει τα προαναφερθέντα χαρακτηριστικά τότε ο οργανισμός είναι προτιμότερο στο να προβεί σε μια τυπική εξάλειψη, διαφορετικά θα πρέπει να ανοικοδομήσει το σύστημα.

Οι δύο κύριες πτυχές της αποκατάστασης από περιστατικά malware είναι 1) η αποκατάσταση της λειτουργικότητας και των δεδομένων των μολυσμένων ξενιστών και 2) η κατάργηση των προσωρινών μέτρων περιορισμού. Οι οργανισμοί θα πρέπει να εξετάσουν προσεκτικά το χειρότερο πιθανό σενάριο και να καθορίσουν τον τρόπο αποκατάστασης που πρέπει να πραγματοποιείται, συμπεριλαμβανομένης της ανακατασκευής των παραβιασμένων ξενιστών είτε από το μηδέν είτε από αντίγραφα ασφαλείας (backups).

Ο προσδιορισμός του πότε πρέπει να καταργηθούν τα προσωρινά μέτρα περιορισμού, όπως της αναστολής των υπηρεσιών ή της συνδεσιμότητας, είναι συχνά μια δύσκολη απόφαση κατά τη διάρκεια μεγάλων περιστατικών malware. Οι ομάδες αντιμετώπισης περιστατικών malware πρέπει να προσπαθήσουν και να κοπιάσουν να κρατήσουν τα μέτρα περιορισμού στη θέση τους μέχρι ο εκτιμώμενος αριθμός των μολυσμένων ξενιστών και των ευάλωτων σε μολύνσεις ξενιστών να είναι επαρκώς χαμηλός ώστε τα πιθανά μετέπειτα περιστατικά να είναι μικρής σημασίας. Ωστόσο, ακόμη και αν η ομάδα αντιμετώπισης περιστατικών θα πρέπει να αξιολογήσει τους κινδύνους για την αποκατάσταση των υπηρεσιών ή της συνδεσιμότητας, η διοίκηση χρειάζεται τελικά να

είναι υπεύθυνη για τον προσδιορισμό του τι πρέπει να γίνει με βάση τις συστάσεις της ομάδας αντιμετώπισης του περιστατικού και να κατανοήσει επίσης τις επιπτώσεις στην επιχείρηση για τη διατήρηση των μέτρων περιορισμού.

2.2.4 Post-Incident δραστηριότητα

Επειδή ο χειρισμός των περιστατικών κακόβουλου λογισμικού μπορεί να είναι εξαιρετικά δαπανηρός, είναι ιδιαίτερα σημαντικό για τους οργανισμούς να προβούν σε αξιόπιστη εκτίμηση των διδαγμάτων που έλαβαν μετά από σοβαρά περιστατικά malware για να αποτραπούν παρόμοια περιστατικά που μπορεί να συμβούν μελλοντικά. Η καταγραφή των μαθημάτων που πήραν από τον χειρισμό τέτοιων περιστατικών θα πρέπει να βοηθήσουν τον οργανισμό να βελτιώσει τις ικανότητες του στο χειρισμό και στις άμυνες malware, συμπεριλαμβανομένης της αναγνώρισης των απαραίτητων αλλαγών στην πολιτική ασφάλεια, στις διαμορφώσεις του λογισμικού, στην ανάπτυξη λογισμικού ανίχνευσης και στην πρόληψη malware.

Επίσης, θα μπορούσαν να γίνουν αλλαγές στα προγράμματα ευαισθητοποίησης των χρηστών ώστε να μειωθεί ο αριθμός των μολύνσεων. Ακόμη, ίσως χρειαστεί να επαναδιαμορφωθεί το λογισμικό (λειτουργικά συστήματα, εφαρμογές) ώστε να υποστηρίζονται οι αλλαγές στις πολιτικές ασφαλείας που έχουν γίνει (Souppaya & Scarfone, 2012).

Κεφάλαιο 3

Εμπειρική Έρευνα

Για το εμπειρικό κομμάτι της μεταπτυχιακής διατριβής αυτής, διεξάχθηκαν συνεντεύξεις για την συλλογή των πιο κάτω αποτελεσμάτων. Ο σκοπός της έρευνας είναι να δούμε στην πράξη αν το ανθρώπινο δυναμικό των εταιρειών γνωρίζει την σημασία και τις επιπτώσεις που μπορεί να προκαλέσει ένα περιστατικό malware και τον αντίκτυπο που θα έχει προκαλέσει στην επιχείρηση. Επίσης, σκοπός είναι να δούμε πόσο σημαντικό είναι για το ανθρώπινο δυναμικό να εκπαιδευτεί και να ευαισθητοποιηθεί στα μέτρα ασφάλειας των πληροφοριακών συστημάτων.

Η συνέντευξη είναι η μέθοδος που έχει σκοπό να οργανώσει μια σχέση προφορικής επικοινωνίας ανάμεσα σε δύο πρόσωπα, εκείνο που κάνει την συνέντευξη και τον ερωτώμενο, έτσι ώστε να επιτρέψει στον πρώτο τη συλλογή όσο των περισσότερων πληροφοριών από το δεύτερο πάνω σε ένα συγκεκριμένο θέμα. Ο τύπος της συνέντευξης που χρησιμοποιήθηκε στην έρευνα αυτή είχε πλήρως δομημένη μορφή, δηλαδή τα ερωτήματα και η διατύπωση τους είχαν καθοριστεί πριν από τη συνέντευξη. Οι περισσότερες ερωτήσεις ήταν ανοικτές, δεν είχαν δηλαδή προκαθοριστεί στο έντυπο της συνέντευξης πιθανές απαντήσεις για επιλογή. Όλες οι ερωτήσεις γίνονταν πάντα με την ίδια σειρά και με την ίδια διατύπωση για όλους τους ερωτώμενους. Όλες οι απαντήσεις για τον καθένα ερωτώμενο καταγράφονταν σε ξεχωριστό έντυπο.

Προκειμένου να έχει επιτυχία η χρήση της συνέντευξης, ακολουθήθηκαν κάποιοι κανόνες όπως το ότι καθορίστηκε μέρος και χρόνος συνάντησης που να μπορεί να βολεύει και τους δύο, η συνέντευξη έγινε σε άκρως επαγγελματικό κλίμα. Η εταιρεία που επιλέχθηκε ανήκει στον κλάδο των Δικτύων και Τηλεπικοινωνιών και το δείγμα συνεντεύξεων ήταν 12. Από τις 12 συνεντεύξεις, οι 6 ήταν από άτομα που έχουν σπουδάσει κάτι σχετικό με Πληροφορική, Δίκτυα και Τηλεπικοινωνίες, Μηχανικοί

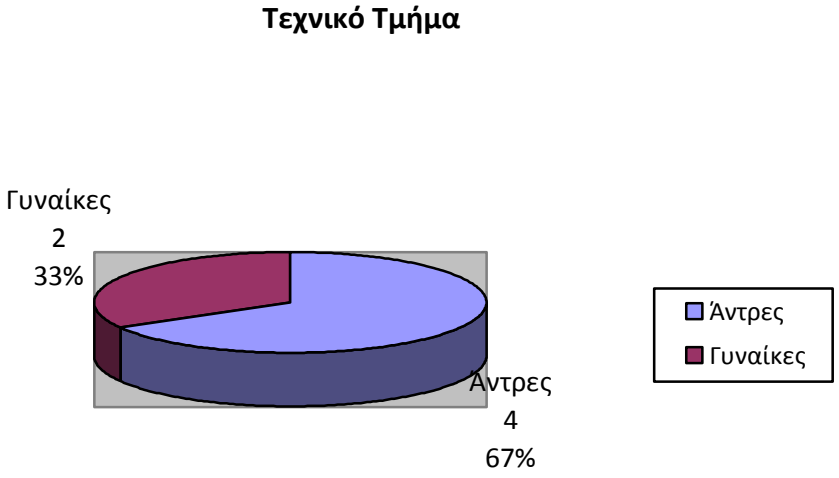
Υπολογιστών και οι 6 ήταν άτομα που δεν έχουν σπουδάσει κάτι σχετικό. Δηλαδή, τα 6 άτομα είναι στο τμήμα της Τεχνικής Υποστήριξης και οι υπόλοιποι 6 από το τμήμα του Λογιστηρίου και Πληροφοριών, και τα 12 άτομα χρησιμοποιούν τα ίδια συστήματα, τον ίδιο ιστότοπο για email, το Διαδίκτυο και όλη η δουλειά τους είναι μπροστά από ένα υπολογιστή. Η διάρκεια των συνεντεύξεων ήταν περίπου δύο με τρεις βδομάδες. Οι συνεντεύξεις αυτές, αποτελούν τον ακρογωνιαίο λίθο πάνω στον οποίο πρόκειται να εξαχθούν τα τελικά συμπεράσματα.

3.1 Αποτελέσματα

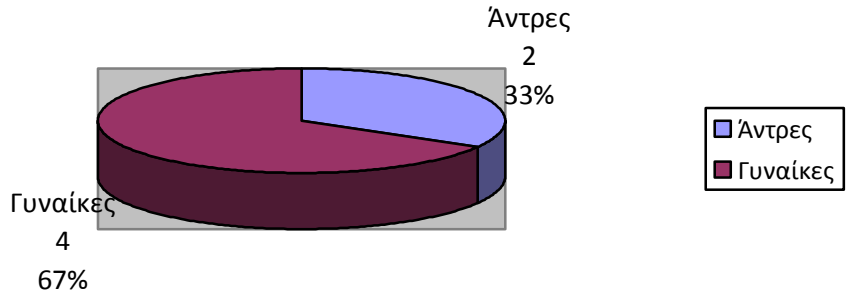
Δημογραφικά στοιχεία:

Οι συμμετέχοντες είχαν το δικαίωμα να παραμείνουν ανώνυμοι. Στο Παράρτημα Α, παρατίθενται όλες οι ερωτήσεις της συνέντευξης.

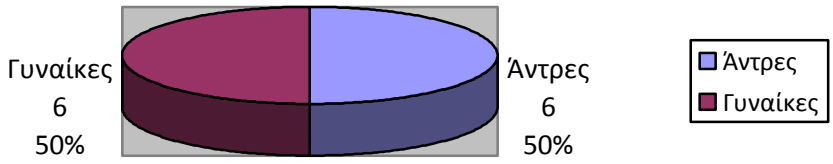
Στο τεχνικό τμήμα της εταιρείας εργάζονται 3 γυναίκες και 15 άντρες, επιλέχθηκαν τυχαία 6 άτομα, οι 2 από αυτές είναι γυναίκες και οι 4 άντρες. Στο τμήμα Λογιστηρίου και Πληροφοριών εργάζονται 8 γυναίκες και 4 άντρες, επιλέχθηκαν πάλι τυχαία 6 άτομα, οι 4 γυναίκες και οι 2 άντρες. Σύνολο, είχαμε 6 γυναίκες και 6 άντρες και από τα δύο τμήματα. Όλοι οι συμμετέχοντες είναι μόνιμοι υπάλληλοι στην εταιρεία με 7 μήνες έως και 6 χρόνια υπηρεσίας.



Τμήμα Λογιστηρίου και Πληροφοριών

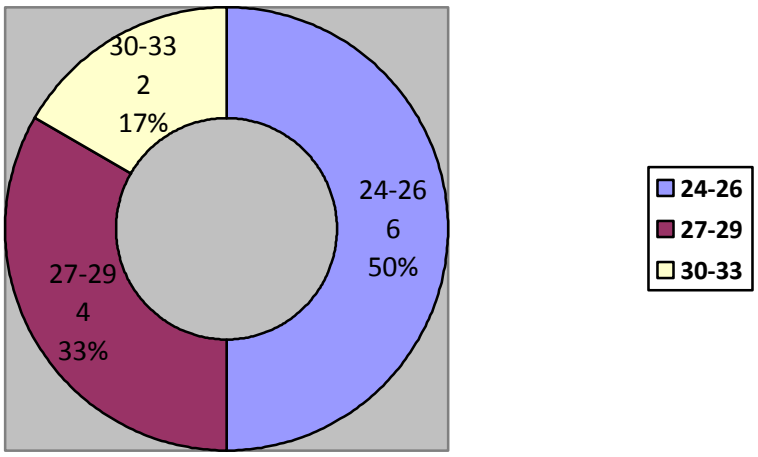


Τμήμα Λογιστηρίου και Πληροφοριών και Τεχνικό Τμήμα

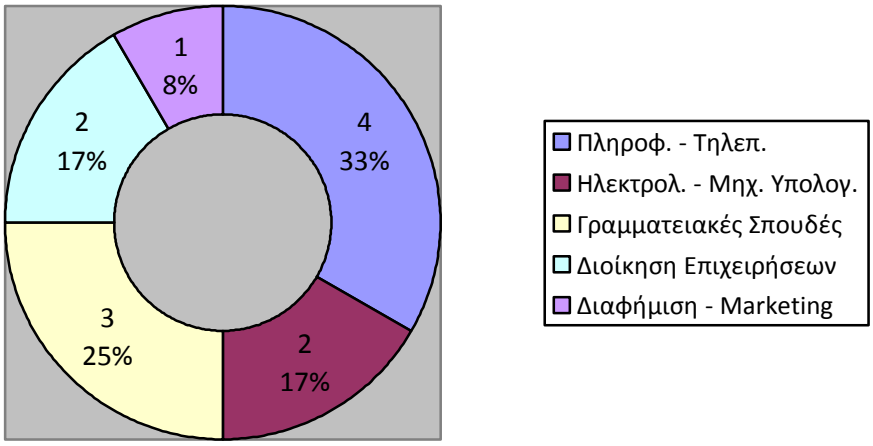


Πιο κάτω είναι δύο γραφήματα τα οποία δείχνουν τα φάσμα ηλικίας των ερωτώμενων και το είδος σπουδών που ακολούθησαν. Το φάσμα ηλικιών κυμαίνονται από 24 – 33 χρονών. Οι κλάδοι σπουδών του ανθρώπινου δυναμικού είναι αρκετοί π.χ. Πληροφορική και Τηλεπικοινωνίες, Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών, Γραμματειακές σπουδές, Διοίκηση Επιχειρήσεων και PR Advertising & Marketing.

Φάσμα Ηλικιών



Σπουδές



Ερωτήσεις και Απαντήσεις:

Ερώτηση 1 – Ο στόχος της μεταπτυχιακής διατριβής μου έχει να κάνει με το πόσο σημαντική είναι η εκπαίδευση και η ευαισθητοποίηση του Ανθρώπινου Δυναμικού στα μέτρα ασφαλείας των Πληροφοριακών Συστημάτων των εταιρειών. Εσείς τι πιστεύετε για αυτό; Ο ανθρώπινος παράγοντας έχει μέρος ευθύνης για την σωστή χρήση των συστημάτων της εταιρείας;

Απαντήσεις από το Τεχνικό Τμήμα:

- Έχει μεγάλο μέρος ευθύνης γιατί η πιθανόν λανθασμένη ή ανεύθυνη χρήση των συστημάτων μπορεί να προκαλέσει σοβαρά προβλήματα, όχι μόνο στην ομαλότητα της λειτουργίας της επιχείρησης αλλά και να απειλήσει την ασφάλεια των συστημάτων καθώς επίσης και των δεδομένων της επιχείρησης αλλά και των πελατών.
- Σίγουρα ο ανθρώπινος παράγοντας έχει σημαντικό μέρος ευθύνης για την σωστή χρήση των συστημάτων της εταιρείας, καθώς χρησιμοποιεί τα συστήματα σε καθημερινή βάση και οποιοδήποτε λάθος ή ιός μπορεί να εισβάλει διαμέσου της χρήσης σε ένα σύστημα και ίσως να επηρεάζει και τους υπόλοιπους χρήστες.
- Την μεγαλύτερη ευθύνη. Η μη σωστή χρήση, κατάρτιση και ενημέρωση στην σωστή χρήση των συστημάτων οδηγούν σε προβλήματα.
- Σίγουρα ο ανθρώπινος παράγοντας παίζει ρόλο για τη σωστή χρήση των συστημάτων μιας εταιρείας, αφού για τη σωστή χρήση των συστημάτων απαιτείται σωστή εκπαίδευση και καθοδήγηση μεταξύ των ατόμων της εταιρείας.
- Εν μέρει ναι αφού ο ίδιος τα χρησιμοποιεί και τα δουλεύει, αλλά αυτό έχει να κάνει σχέση και με την εταιρεία που πρέπει να έχει ελέγξει το δίκτυο και τα προβλήματα και τις αδυναμίες των λογισμικών για να προλάβουν κάτι τέτοιο.
- Συμφωνώ απόλυτα. Η σωστή ενημέρωση και η εκπαίδευση του προσωπικού είναι απαραίτητη στις εταιρείες και ειδικά για την ασφάλεια και την προστασία του κάθε εργαζομένου.

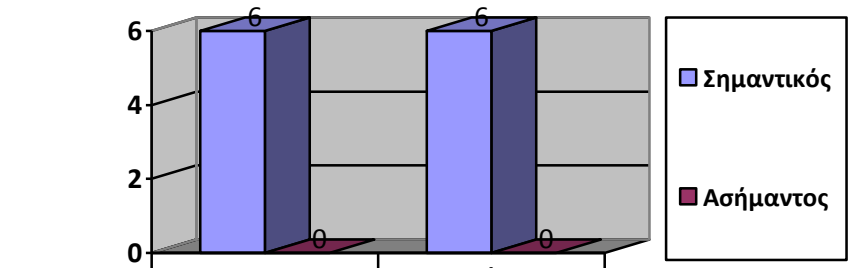
Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Σίγουρα έχει μέρος της ευθύνης. Όσο καλύτερη είναι η εκπαίδευση των υπαλλήλων που χρησιμοποιούν τα συστήματα μιας εταιρείας, τόσο μεγαλύτερη οικειότητα θα έχουν με τα προβλήματα που πιθανόν να προκύψουν ή αντιμετωπίζουν.
- Συμφωνώ, ο ανθρώπινος παράγοντας έχει μερίδιο ευθύνης στη σωστή χρήση των συστημάτων εντός της εταιρείας.
- Φυσικά. Ο ανθρώπινος παράγοντας έχει το μεγαλύτερο μέρος ευθύνης λόγω του ότι είναι ο χρήστης και ο κύριος λόγος που εκτίθεται η εταιρεία σε κινδύνους. Η

λανθασμένη χρήση των συστημάτων, η χρήση τους για προσωπικούς σκοπούς, πολλές φορές λόγω απροσεξίας ή άγνοιας μπορεί να είναι επιβλαβές στο σύστημα. Ο οποιοσδήποτε μπορεί να ανοίξει κάποιο αρχείο ή να κατεβάσει κάποιο κακόβουλο πρόγραμμα και να μολύνει και τους υπόλοιπους υπολογιστές καθώς και το δίκτυο της εταιρείας.

- Ναι έχει μεγάλο μέρος της ευθύνης αυτής λόγω του ότι η εκπαίδευση βασίζεται στην εξέλιξη της τεχνολογίας στην οποία πρέπει όλοι να προσαρμοζόμαστε και να εκπαιδευόμαστε βάση αυτής.
- Σίγουρα είναι πολύ σημαντικός ο ανθρώπινος παράγοντας για τη σωστή χρήση των συστημάτων της εταιρείας, γιατί με τα σημερινά δεδομένα η τεχνολογία συνεχώς αναπτύσσεται με γρήγορους ρυθμούς έτσι και ο άνθρωπος πρέπει να την ακολουθεί για να διευκολύνεται στην διεκπεραίωση της εργασίας του.
- Ο ανθρώπινος παράγοντας είναι πολύ σημαντικός για τη σωστή χρήση συστημάτων της εταιρείας καθώς είναι έμμεσα ο κύριος εμπλεκόμενος.

Σημαντικότητα Ανθρώπινου Παράγοντα στην σωστή χρήση των συστημάτων της εταιρείας



	Τεχνικό Τμήμα	Τμήμα Λογιστηρίου και
Σημαντικός	6	6
Ασήμαντος	0	0

Ερώτηση 2 - Αν σας δινόταν η ευκαιρία να εξηγήσετε με λίγα λόγια τον όρο malware / κακόβουλο λογισμικό, πως θα τον ορίζατε;

Απαντήσεις από το Τεχνικό Τμήμα:

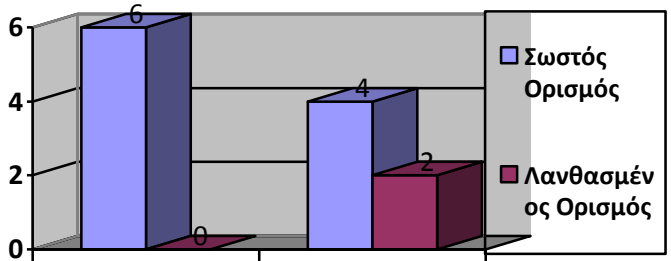
- Λογισμικό το οποίο εκτελεί ανεπιθύμητες ενέργειες στα συστήματα. Ένα σύστημα μπορεί να μολυνθεί με ποικίλους τρόπους. Υπάρχουν πολλά είδη τέτοιου λογισμικού που μπορούν να προκαλέσουν πληθώρα επιθέσεων παθητικών ή ενεργητικών.
- Λογισμικό το οποίο μπορεί να καταστρέψει ή να προκαλέσει ζημιές σε ένα σύστημα μπορεί να είναι ένας ιός ή οτιδήποτε άλλο.
- Μια σειρά από εντολές (κώδικας) στην μορφή κάποιου αρχείου, όπως ένα συνηθισμένο πρόγραμμα που αποσκοπεί στην απόσπαση πληροφοριών ή στην καταστροφή αρχείων του υπολογιστή.
- Ένα κακόβουλο λογισμικό μπορεί να είναι κάποιος ιός που μπορεί να προσβάλλει τα αρχεία ενός υπολογιστή και επίσης μπορεί να κάνει τον υπολογιστή εξαιρετικά αργό.
- Τα λογισμικά που αποσκοπούν σε επιθέσεις κατά της εμπιστευτικότητας, της ακεραιότητας ή/και της διαθεσιμότητας των συστημάτων.
- Είναι κάποιο είδος κώδικα που εκτελεί εντολές, οι οποίες ως επί το πλείστον είναι κακόβουλες, δηλαδή μπορεί να υποκλέψει δεδομένα ή να προκαλέσει πρόβλημα στην λειτουργικότητα κάποιας συσκευής (π.χ. υπολογιστής).

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Θεωρείται ένα λογισμικό το οποίο δημιουργείται κακόβουλα και μπορεί να αποκτήσει πρόσβαση ή να προκαλέσει πρόβλημα σε ένα ηλεκτρονικό υπολογιστή χωρίς να το γνωρίζει ο κάτοχος της συσκευής.
- Είναι είδος ιών που προσβάλλουν υπολογιστές και γενικότερα ηλεκτρονικές συσκευές.
- Λογισμικό το οποίο μπορεί να κάνει ζημιά στο δίκτυο ή στον υπολογιστή. Να προκαλέσει απώλεια αρχείων ή δεδομένων. Η χρήση του διαδικτύου ή άλλων εφαρμογών χωρίς την έγκριση του διαχειριστή για διάφορους σκοπούς που έχουν κατά κύριο στόχο να προκαλέσουν ζημιά στην εταιρεία.
- Δεν γνωρίζω τι ακριβώς είναι αυτό, όμως μπορώ να σκεφτώ ότι είναι κάποιο λογισμικό το οποίο επηρεάζει τα συστήματα της εταιρείας όσο αφορά τις αποφάσεις που παίρνει ένας εργοδότης.

- Αν και δεν γνωρίζω τι είναι ο όρος αυτός υποθέτω ότι μπορεί να είναι ένα πρόγραμμα το οποίο εισβάλλει με κακόβουλο τρόπο στο σύστημα και παίρνει πληροφορίες από το δικό μας λογισμικό.
- Δεν γνωρίζω αλλά πιστεύω ότι μπορεί να είναι πρόγραμμα το οποίο δίνει κακές πληροφορίες στους χειριστές των προγραμμάτων αυτών.

Γνώση ορισμού malware



	Τεχνικό Τμήμα	Τμήμα Λογιστηρίου και
Σωστός Ορισμός	6	4
Λανθασμένος Ορισμός	0	2

Ερώτηση 3 - Έχετε έρθει ποτέ αντιμέτωπος/η με κάποιο περιστατικό malware (πως/ποτε αν θυμάστε/τι έγινε/τι περιστατικό ήταν);

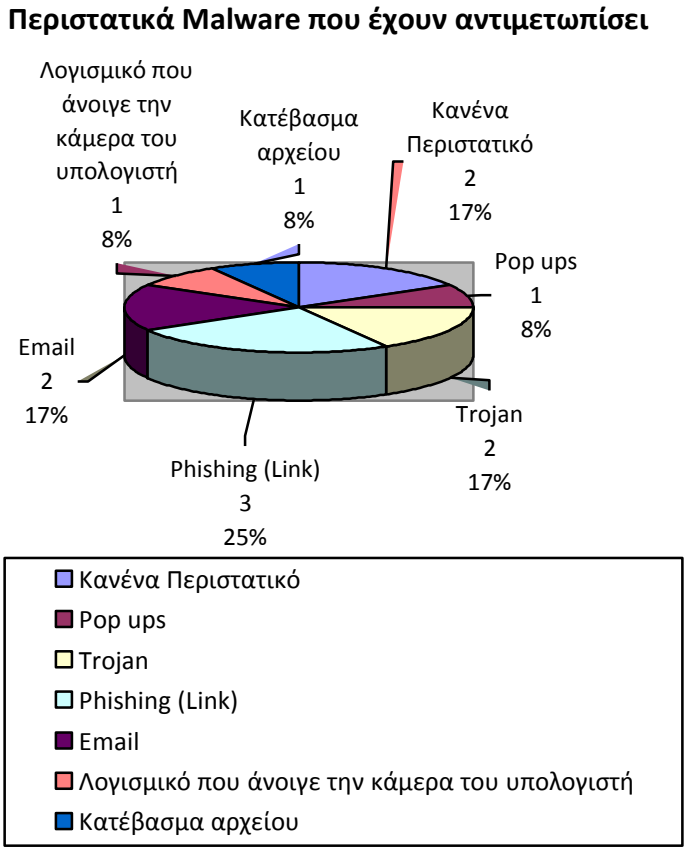
Απαντήσεις από το Τεχνικό Τμήμα:

- Ναι, εμφανίστηκε ξαφνικά πρόγραμμα που χρησιμοποιεί την κάμερα του υπολογιστή, ενώ δεν το είχα εγκατεστημένο ξεκίνησε να λειτουργεί, ανοίγοντας το πρόγραμμα και την κάμερα του υπολογιστή.
- Όχι, δεν έτυχε κάποιο περιστατικό
- Ναι, αντιμετώπισα κάποιο περιστατικό malware πριν αρκετά χρόνια, ήταν κακόβουλο λογισμικό Trojan από ένα torrent file.
- Ναι. Πριν 1-2 χρόνια όταν κυκλοφορούσε στο διαδίκτυο ο ιός της αστυνομίας, ο οποίος κλείδωνε τον browser και δεν σε άφηνε να έχεις πρόσβαση στον υπολογιστή αν δεν πλήρωνες ένα ποσό το οποίο φαινόταν ως πρόστιμο από την αστυνομία.

- Ναι, μέσω email είχα κάνει κλικ σε ένα link, το οποίο ζητούσε στοιχεία του λογαριασμού μου.
- Ναι, άνοιξε από μόνος του ο browser, καθώς χρησιμοποιούσα το διαδίκτυο μου εμφάνισε παράθυρο από αστυνομία όπου ζητούσε κάποια προσωπικά στοιχεία. Επίσης, ένας πελάτης έστειλε στο δίκτυο της εταιρείας άθελά του κακόβουλο λογισμικό που επηρέασε τον server της εταιρείας. Με αποτέλεσμα να μπλοκάρουμε για λίγες ώρες τα ip των εταιρειών μέχρι να λυθεί το συγκεκριμένο θέμα.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Όχι, δεν θυμάμαι πρόσφατα να έχω αντιμετωπίσει κάποιο περιστατικό malware.
- Ναι με trojan. Όταν χρησιμοποίησα το ίδιο usb που ήταν συνδεδεμένο σε υπολογιστή που είχα φέρει από το σπίτι.
- Προφανώς κατά την διάρκεια που κατέβασα κάποιο αρχείο είχε εγκατασταθεί κάποιο delta search το οποίο είναι γνωστό malware. Αντικατέστησε το google.com που ήταν το κύριο search engine του browser μου και όποια αναζήτηση και να έκανα έπρεπε αναγκαστικά να ανοίξει μέσω αυτού του προγράμματος. Ακόμα και αν το άλλαζα όταν έκλεινα το browser και το ξανάνοιγα γινόταν το ίδιο.
- Πάτησα σε ένα link και ο υπολογιστής γέμισε διαφημίσεις και μπλόκαρε το πρόγραμμα περιήγησης του υπολογιστή.
- Άνοιξα ένα email που έδειχνε πως ήταν από την εταιρεία και ζητούσε προσωπικά δεδομένα όπως κωδικούς πρόσβασης, τα έδωσα και μετά δεν μπορούσα να μπω κανονικά στο λογισμικό της εταιρείας.
- Ναι, όταν ανοίγω τον browser που χρησιμοποιώ ανοίγουν συχνά σελίδες τις οποίες δεν του έδωσα εντολή να τις ανοίξει.



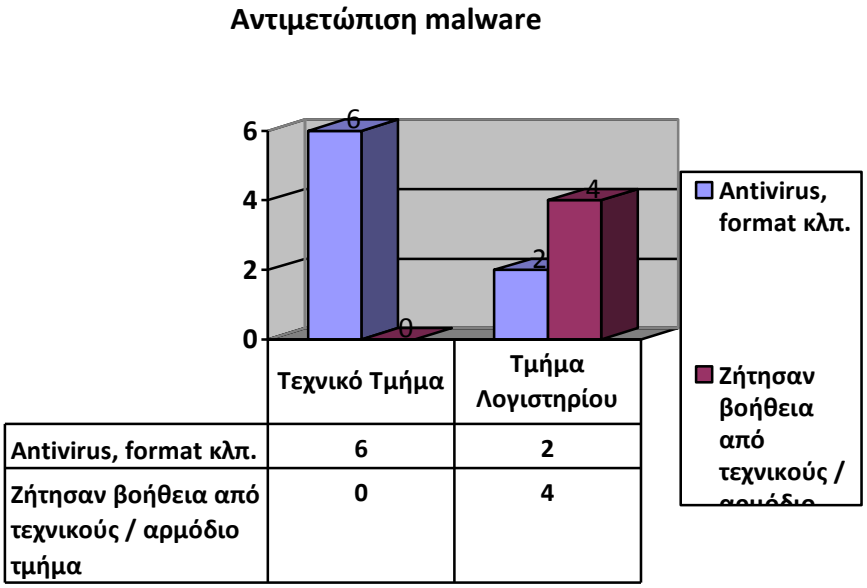
Ερώτηση 4 - Ποια ήταν η πρώτη σας αντίδραση και πως προσπαθήσατε να το αντιμετωπίσετε ή πως θα προσπαθούσατε να το αντιμετωπίσετε σε περίπτωση που αντιμετωπίζατε τέτοιου είδους περιστατικό;

Απαντήσεις από το Τεχνικό Τμήμα:

- Κλείσιμο του προγράμματος, backup και format.
- Ανάλογα με το περιστατικό, θα έκανα τις απαραίτητες ενέργειες, το πιο πιθανόν σαν μία πρώτη κίνηση να έκανα σάρωση του υπολογιστή με κάποιο antivirus.
- Αντιμετώπισα τα περιστατικό αυτό με ψυχραιμία κάνοντας σάρωση όλο τον υπολογιστή με ένα πρόγραμμα antivirus.
- Πανικοβλήθηκα στην αρχή, αλλά με google search βρήκα με ποιους τρόπους μπορείς να ξεφορτωθείς τον συγκεκριμένο ιό και κατάφερα να τον αφαιρέσω.
- Ανησύχησα και έβαλα αμέσως antivirus, η απειλή βρέθηκε και λύθηκε το θέμα.
- Είχα ξανά ακούσει για το συγκεκριμένο, άρα δεν με είχε ανησυχήσει. Δεν είχα δώσει κάποια στοιχεία και ο τρόπος για να φύγει ήταν με antivirus.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Θα αποταθώ σε ένα τεχνικό υπολογιστών για επιδιόρθωση και καθαρισμό του υπολογιστή.
- Πήρα τον υπολογιστή σε τεχνικό το έκανε Format (δεν γνωρίζω για πιο λόγο) και μου εγκατέστησε νέο antivirus.
- Αρχικά προσπάθησα να το κάνω uninstall. Μετά όταν είδα ότι δεν λειτουργεί ένα απλό uninstall έψαξα λύσεις μέσω του google και forums και δοκίμασα αρκετά πράγματα. Μετά από κάποια ώρα η ιδανική λύση φαινόταν να είναι το format.
- Επικοινώνησα με ένα αρμόδιο άτομο το οποίο έχει γνώση σε αυτό και επανάφερε ότι είχε επηρεαστεί.
- Αγχώθηκα και το ζήτησα βοήθεια από το αρμόδιο τμήμα και μου άλλαξαν αμέσως κωδικούς.
- Μου προκάλεσε εντύπωση, έβαλα antivirus και λύθηκε.



	Τεχνικό Τμήμα	Τμήμα Λογιστηρίου
Antivirus, format κλπ.	6	2
Ζήτησαν βοήθεια από τεχνικούς / αρμόδιο τμήμα	0	4

Ερώτηση 5 - Έχετε σκεφτεί ποτέ ποιες επιπτώσεις μπορεί να έχει ένα περιστατικό malware;

Απαντήσεις από το Τεχνικό Τμήμα:

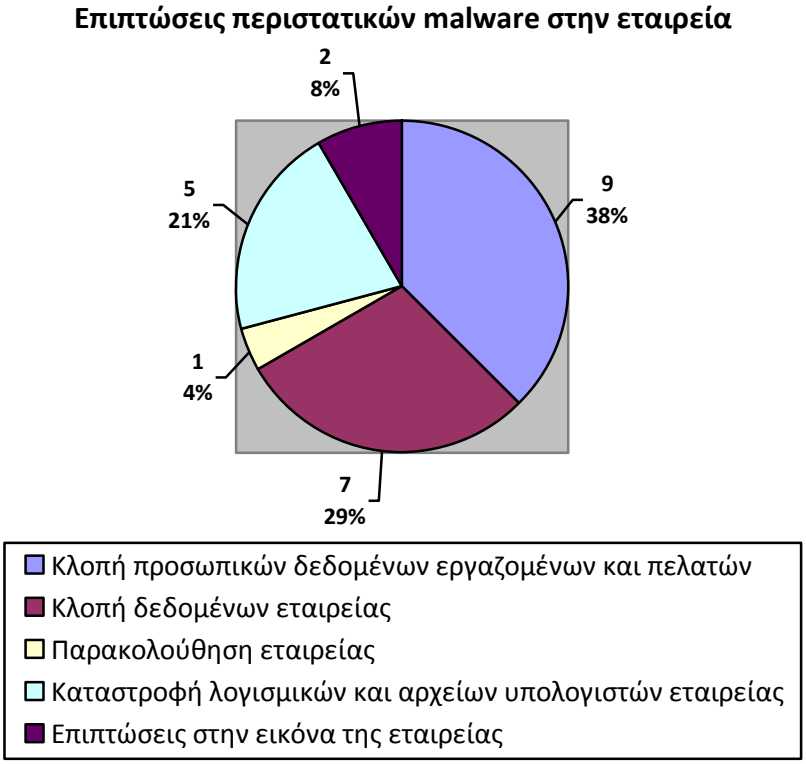
- Ναι, κλοπή προσωπικών δεδομένων των πελατών, κλοπή δεδομένων της επιχείρησης (οικονομικών δεδομένων, μελλοντικά πλάνα της επιχείρησης κ.α.).
- Μέσω ενός ιού ή spyware ένας κακόβουλος εισβολέας μπορεί να καταφέρει να εισβάλει στα συστήματα και να προκαλέσει αρκετά προβλήματα ή να παρακολουθεί την επιχείρηση και να τις κλέψει σημαντικά γι' αυτή δεδομένα.
- Οι πιο σοβαρές επιπτώσεις είναι η απόσπαση ευαίσθητων πληροφοριών όπως προσωπικά δεδομένα και κωδικοί πρόσβασης και καταστροφή hardware και αρχείων των υπολογιστών της εταιρείας.
- Η σημαντικότερες για μένα επιπτώσεις είναι η υποκλοπή προσωπικών και απόρρητων δεδομένων και οι επιπτώσεις στη εικόνα του οργανισμού προς τα έξω. Θα χρειαστεί αρκετός χρόνος για την αποκατάσταση της αξιοπιστίας του.
- Η υποκλοπή προσωπικών δεδομένων και αρχείων και η ζημιά λογισμικού υπολογιστή.
- Να υποκλαπούν προσωπικές πληροφορίες όπως usernames και passwords, αριθμούς πιστωτικών καρτών κλπ. των εργαζομένων αλλά και ατόμων όπου σχετίζεται η εταιρεία, επίσης ζημία στο δίκτυο της εταιρείας και στους υπολογιστές της.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Να αποκτήσει πρόσβαση σε αρχεία με στοιχεία των πελατών που είναι εμπιστευτικά και να καταστρέψει συστήματα που χρησιμοποιεί μια εταιρεία και να δημιουργήσει τεράστιο πρόβλημα.
- Θεωρώ ότι οι πιο πιθανές επιπτώσεις είναι να υποκλαπούν πληροφορίες και δεδομένα όσον άφορα την εταιρεία και τις λειτουργίες της και προσωπικά δεδομένα των υπαλλήλων της εταιρείας.
- Ναι. Η απώλεια αρχείων και η χρησιμοποίηση της βάσης δεδομένων της εταιρείας όσο αφόρα τους πελάτες κτλ. Ζημιά στο δίκτυο και στους υπολογιστές της εταιρείας.
- Αυτό για μια εταιρεία θα ήταν καταστροφικό λόγω του ότι στα λογισμικά της κάθε εταιρείας αποθηκεύονται σημαντικά δεδομένα τα οποία αφορούν τους κανονισμούς και τις αρχές μιας εταιρείας οπόταν το να υποκλαπούν από κάποιον θα ήταν ότι χειρότερο. Επίσης, αυτό θα έχει σημαντικές επιπτώσεις και στην εικόνα της εταιρείας. Για παράδειγμα, αν ένας πελάτης ζητήσει συγκεκριμένα

αρχεία τα οποία ή διαγράφηκαν ή τροποποιήθηκαν. Σε περίπτωση υποκλοπής θα πρέπει άμεσα μια εταιρεία να επικοινωνήσει με κάποιο αρμόδιο για να επιλύσει το πρόβλημα.

- Σε ένα τέτοιο περιστατικό πρέπει ο κάθε οργανισμός κατά την γνώμη μου να είναι έτοιμος να αντιμετωπίσει και να προλάβει να μην χαθούν σημαντικά αρχεία της εταιρείας και των εργαζομένων από το σύστημα οι οποίες θα έχουν σοβαρές επιπτώσεις προς τον οργανισμό.
- Ο κάθε οργανισμός κατά την γνώμη μου πρέπει να είναι έτοιμος να αντιμετωπίσει: την απόσπαση πληροφοριών της εταιρείας του που αυτό θα έχει σοβαρές επιπτώσεις και να μην χάσει σημαντικά αρχεία π.χ. αρχεία πελατών, συνεργατών, προμηθευτών κλπ.



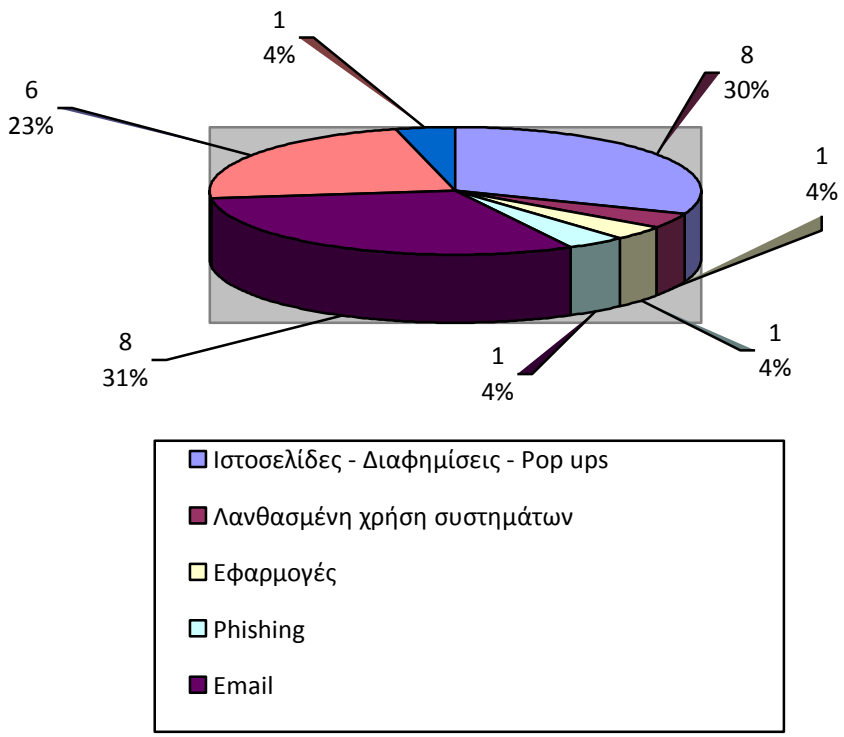
Ερώτηση 6 - Ποιες πιστεύετε πως είναι οι καθημερινές απειλές λήψης κακόβουλου λογισμικού / malware;

Απαντήσεις από το Τεχνικό Τμήμα:

- Το internet και η λανθασμένη ή αμελής χρήση των συστημάτων της εταιρείας από το ανθρώπινο δυναμικό.
- Οι σελίδες που επισκεπτόμαστε ή διάφορα link που μπορεί να ανοίγουμε στο email μας.
- Email, Downloading Files, Streaming unauthorized websites.
- Spam mails, Phishing, Pop ups.
- Διαφημίσεις σε ιστοσελίδες, email, διάφορες εφαρμογές, κατέβασμα αρχείων από αμφιβόλου ποιότητας πηγές.
- Με την βοήθεια κάποιας εξωτερικής συσκευής όπως usb ή εξωτερικός δίσκος, επίσης και μέσω email.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Μέσω email το κυριότερο πιστεύω, μέσω σελίδων που βγάζουν διαφημιστικά μηνύματα και πατούν ανυποψίαστοι οι χρήστες, μέσω αρχείων που μπορεί να κατεβάσει κάποιος χρήστης και δεν το ελέγχει με κάποιο antivirus που έχει εγκατεστημένο στον υπολογιστή.
- Απειλές είναι τα emails που λαμβάνουμε και τα αρχεία που κατεβάζουμε καθώς επίσης και τα sites τα όποια επισκεπτόμαστε.
- Attachments μέσω email. Download προγραμμάτων. Χρήση ιστοσελίδων που αυτόματα μπορεί να κατεβάσουν κάτι.
- Όταν ανοίγεις αρχεία τα οποία δεν γνωρίζεις αν έχουν κάποιο είδος κακόβουλου λογισμικού τα οποία όμως πρέπει να τα ανοίξεις για να πάρεις κάποιες πληροφορίες από τα συγκεκριμένα αρχεία.
- Μία απειλή που πιστεύω ότι έχουμε καθημερινά για κακόβουλο λογισμικό είναι η λήψη μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου.
- Οι καθημερινές απειλές λήψης κακόβουλου λογισμικού είναι όταν σου στέλνουν κάποια αρχεία και δεν ξέρεις αν έχουν μέσα ή όχι κακόβουλο λογισμικό και έτσι τα ανοίγεις.



Ερώτηση 7 - Ο ανθρώπινος παράγοντας είναι απειλή; Τι γνώμη έχετε;

Απαντήσεις από το Τεχνικό Τμήμα:

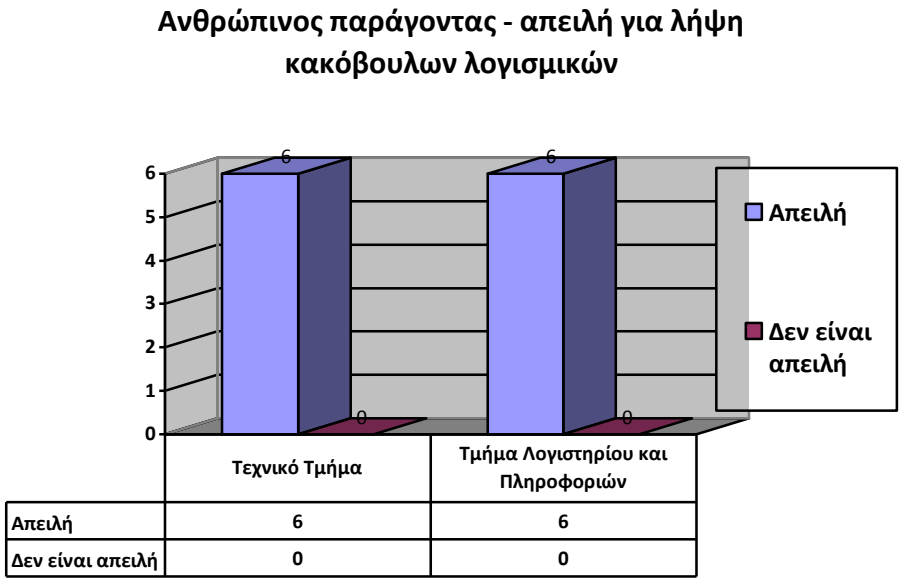
- Ναι, γιατί αν δεν λαμβάνονται σοβαρά υπόψη οι κανονισμοί ασφαλείας από το ανθρώπινο δυναμικό και δεν υπάρχει οργανωμένο πλαίσιο πρόληψης με βάση τον ανθρώπινο παράγοντα, τότε οι πιθανότητες εκδήλωσης κάποιας απειλή αυξάνονται. Επίσης, ανειδίκευτο προσωπικό, δυσαρεστημένοι υπάλληλοι ή πελάτες μπορούν επίσης να αποτελέσουν απειλή.
- Επηρεάζει καθώς κάποιες φορές πολλά από το malware τα δημιουργούν άνθρωποι που έχουν εταιρείες antivirus για να πουλήσουν το προϊόν τους ή να τα στέλνουν σκόπιμα. Επίσης, ανάλογα με την χρήση που κάνουμε ευθυνόμαστε για ένα κακόβουλο λογισμικό που εισβάλει στον υπολογιστή μας.
- Η μη σωστή χρήση και η μη γνώση στην σωστή πρόληψη ενάντια των κακόβουλων προγραμμάτων οδηγούν στα πιο σοβαρά προβλήματα. Η νο.1 απειλή για τα πληροφοριακά συστήματα είναι ο ίδιος ο χρήστης τους.

- Ο ανθρώπινος παράγοντας είναι απειλή αφού με το τρόπο του εσκεμμένα ή άθελα (λόγο αφέλειας ή άγνοιας) μπορεί να συμβάλει στην δημιουργία ή και εγκατάσταση ενός malware σε ένα σύστημα. Πολλές φορές εσκεμμένα άνθρωποι προσπαθούν να επιτεθούν σε ένα οργανισμό με σκοπό προσωπικούς, οικονομικούς και επαγγελματικούς λόγους. Από την άλλη πλευρά η άγνοια πολλών ανθρώπων μπορεί να συντελέσει στην ολοκλήρωση της επίθεσης μέσω malware αφού ανοίγουν για παράδειγμα οποιαδήποτε mails λαμβάνουν από άγνωστους αποστολείς.
- Ναι, ο ανθρώπινος παράγοντας είναι απειλή από τη στιγμή που μέσω δικής του επιλογής, έστω και κατά λάθος γίνεται λήψη τέτοιου είδους κακόβουλου λογισμικού.
- Ναι, εφόσον χρησιμοποιεί το σύστημα. Είναι οπωσδήποτε απειλή γιατί όλα αυτά τα δημιουργεί ο ανθρώπινος παράγοντας για να εκτελέσουν μία κακόβουλη ενέργεια.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Ο ανθρώπινος παράγοντας θεωρείται η μεγαλύτερη και κυρίως η μόνη απειλή αφού αυτός δημιουργεί κάποιο κακόβουλο λογισμικό με σκοπό να προκαλέσει πρόβλημα σε κάποια εταιρεία ή να αποκτήσει πρόσβαση σε κάποια αρχεία.
- Θεωρώ ότι είναι απειλή γιατί από τους ανθρώπους δημιουργούνται και η μη σωστή ενημέρωση και πρόληψη βοήθα στην διάδοση και στην προώθηση των συγκεκριμένων κακόβουλων λογισμικών.
- Είναι μεγάλη απειλή, αφού στις πλείστες των περιπτώσεων είναι ο κύριος λόγος για τέτοιου είδους επιθέσεις.
- Ναι ο ανθρώπινος παράγοντας είναι απειλή γιατί το κακόβουλο λογισμικό δημιουργείτε από τους ανθρώπους, έτσι ώστε να υποκλέψουν και να αλλοιώσουν στοιχεία και δεδομένα μιας εταιρείας για δική τους χρήση με σκοπό να επιβληθούν με κάποιο τρόπο στην διαχείριση της εταιρείας.
- Σίγουρα ο ανθρώπινος παράγοντας είναι απειλή γιατί με τη σημερινή τεχνολογία ο άνθρωπος μπορεί να διεισδύσει οπουδήποτε και να πάρει οποιεσδήποτε πληροφορίες με την κατάλληλη εκπαίδευση.

- Φυσικά και ο ανθρώπινος παράγοντας είναι απειλή γιατί εύκολα μπορεί κάποιος να σε εκθέσει προς τα έξω παίρνοντας κάποια προσωπικά στοιχεία που αφορούν εσένα ή και τον οργανισμό τον οποίο εκπροσωπείς.



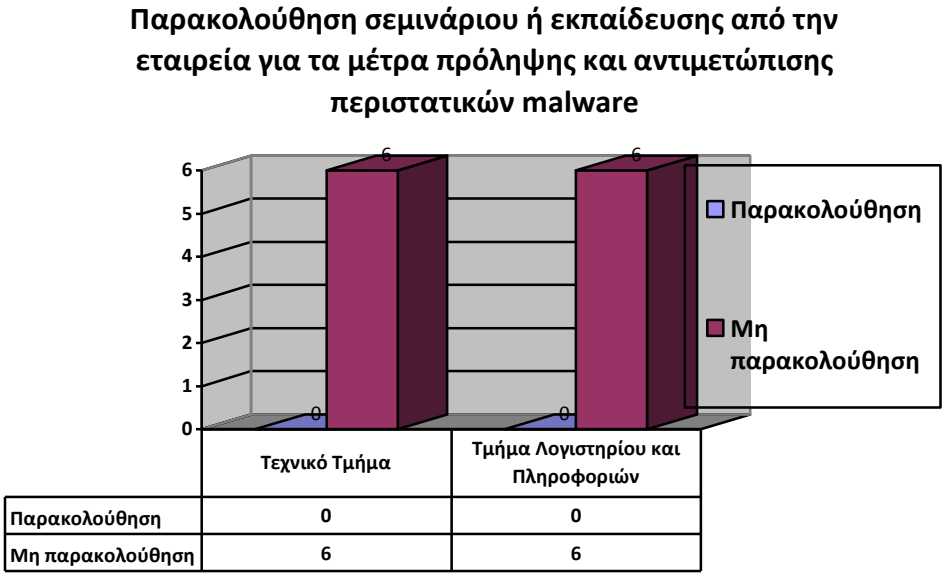
Ερώτηση 8 - Σας έχει γίνει κάποιο σεμινάριο ή κάποια εκπαίδευση από την εταιρεία για τα μέτρα πρόληψης και αντιμετώπισης των περιστατικών malware;

Απαντήσεις από το Τεχνικό Τμήμα:

- Όχι, ότι γνωρίζω το κατέχω μέσω της εμπειρίας και της ενασχόλησης με το αντικείμενο.
- Όχι ακόμα δεν έχει γίνει τέτοια εκπαίδευση σε μένα. Δεν γνωρίζω πιο παλιά.
- Όχι, δεν μας έχει γίνει κάποια εκπαίδευση, η γνώση μας κυρίως για τέτοια κακόβουλα λογισμικά και τους τρόπους που μπορεί να προσβάλουν ένα υπολογιστή, προκύπτει μέσα από την ακαδημαϊκή μας κατάρτιση.
- Όχι.
- Όχι και καλό θα ήταν να γίνει από τη στιγμή που ο υπολογιστής που έχω τα δεδομένα και τα αρχεία μου χρησιμοποιείται και από άλλους συναδέλφους που πιθανόν να είναι πιο απρόσεκτοι σε τέτοιου είδους θέματα.
- Όχι, δεν έχει ασχοληθεί καθόλου η εταιρείας μου με το συγκεκριμένο θέμα.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Όχι.
- Όχι δυστυχώς δεν έχει γίνει κάποια ενημέρωση.
- Όχι. Έχω μόνο κάποιες περιορισμένες γνώσεις από προσωπική εμπειρία και έρευνα.
- Όχι δεν μας έχει γίνει κάποιο σεμινάριο όσο αφορά τέτοια περιστατικά οπόταν δεν γνωρίζω πως μπορώ να αντιμετωπίσω τέτοιο περιστατικό μόνη μου.
- Όχι δεν μας έχουν προτείνει ποτέ για ένα τέτοιο σεμινάριο ούτε μας έχει γίνει κάποια εκπαίδευση από την εταιρεία αλλά καλό θα ήταν να μας γίνει.
- Όχι δεν μας έχει γίνει κάποιο σεμινάριο ή κάποια εκπαίδευση από την εταιρεία μας για τα μέτρα αυτά, αλλά από όσον γνωρίζουμε κάποια μηνύματα ηλεκτρονικού ταχυδρομείου που έρχονται όταν μας φαίνονται απειλητικά δεν τα ανοίγουμε.



Ερώτηση 9 - Πιστεύετε πως ένα τέτοιο σεμινάριο ή εκπαίδευση θα βοηθούσε ή σας έχει βοηθήσει στην ορθή χρήση των συστημάτων και την αποφυγή τέτοιων περιστατικών;

Απαντήσεις από το Τεχνικό Τμήμα:

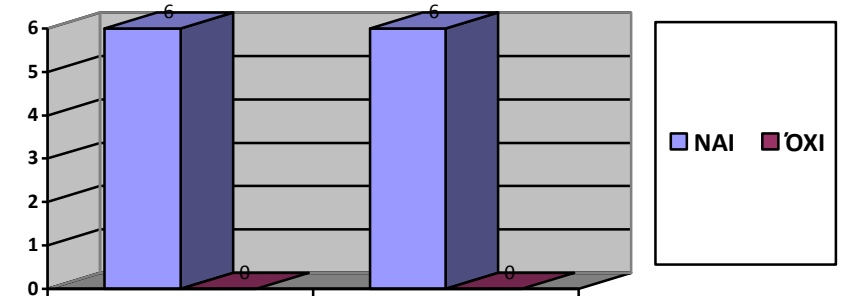
- Σίγουρα θα βοηθούσε γιατί οι απειλές αυξάνονται και εξελίσσονται και γι' αυτό θα έπρεπε να υπάρχει τακτική ενημέρωση και εκπαίδευση, έτσι ώστε να είμαστε ενήμεροι για κάθε νέα απειλή και για το πώς θα την αντιμετωπίσουμε έγκαιρα. Καλύτερη «θεραπεία» άλλωστε, είναι η πρόληψη.
- Νομίζω πως ναι θα ήταν αρκετά εποικοδομητικό για όλους, καθώς με αυτό τον τρόπο θα ήταν πιο λίγες οι απειλές malware και πιο εύκολη η αντιμετώπιση καθώς γνωρίζοντας για κάτι μπορείς πιο εύκολα να το αντιμετωπίσεις.
- Ναι σίγουρα θα βοηθούσε ένα τέτοιο σεμινάριο ή εκπαίδευση από την εταιρεία, γιατί μέσω αυτού/ής πιστεύω θα μπορούσαν να αναλυθούν αρκετά περιστατικά malware, να ειπωθούν παρόμοιες εμπειρίες μεταξύ των παρευρισκομένων και να επισημανθούν σημαντικά μέτρα πρόληψης και αντιμετώπισης. Πάντα με την προϋπόθεση όμως πως η εκπαίδευση θα γίνει από κάποιο αρκετά καταρτισμένο στο συγκεκριμένο θέμα.
- Ένα τέτοιο σεμινάριο ή εκπαίδευση θα συνέβαλλε θετικά στον περιορισμό ή ακόμη και την αποφυγή περιστατικών malware, αφού με τη σωστή ενημέρωση μπορείς να διακρίνεις πιο εύκολα τους κινδύνους σε τέτοιες περιπτώσεις και δεν πέφτεις εύκολα σε παγίδες.
- Ναι, θα βοηθούσε
- Ναι, θα ήταν σωστό να γίνει έτσι ώστε να μπορούμε προληπτικά να προστατέψουμε τόσο της εταιρεία όσο και τον εργαζόμενο. Θα βοηθούσε για την αποφυγή διαγραφής δεδομένων αλλά και πιθανής κατάρρευσης όλου του συστήματος.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Σίγουρα, η εκπαίδευση πάντα προλαμβάνει προβλήματα που δημιουργούνται μέσα από την άγνοια και ειδικά σε ότι έχει να κάνει με ηλεκτρονικά συστήματα.
- Σίγουρα θα βοηθούσε στην αποφυγή τέτοιων περιστατικών.
- Φυσικά αν και στην Κύπρο δεν θεωρώ ότι δίνεται κάποια βάση σε αυτό τον τομέα. Σε μια μέση εταιρεία στην Κύπρο, εάν ασχολείται κάποιο τμήμα της εταιρείας με αυτό το θέμα είναι μόνο το Ι.Τ., αν υπάρχει καν.
- Ναι, πιστεύω πως θα βοηθούσε ένα τέτοιο σεμινάριο γιατί είναι σημαντικό να εξελισσόμαστε και να γνωρίζουμε καινούργια πράγματα ειδικά όταν έχουμε να κάνουμε με λογισμικά στον χώρο της εργασίας μας.

- Ένα τέτοιο σεμινάριο ή εκπαίδευση σίγουρα θα μας βοηθούσε στην αποφυγή τέτοιων περιστατικών και στην ορθή χρήση των συστημάτων και έτσι η εργασία μας θα εκτελείτο με λιγότερο άγχος στο ότι μπορεί να μας αποσπάσουν οποιαδήποτε πληροφορία από το σύστημά μας.
- Σίγουρα ένα τέτοιο σεμινάριο ή εκπαίδευση θα βοηθούσε πάρα πολύ την ορθή χρήση των συστημάτων και την αποφυγή τέτοιων περιστατικών, έτσι ώστε να προστατευτούμε από κάθε είδος απειλής.

Σεμινάριο ή εκπαίδευση θα βοηθούσε στην αποφυγή τέτοιων περιστατικών;



	Τεχνικό Τμήμα	Τμήμα Λογιστηρίου και Πληροφοριών
ΝΑΙ	6	6
ΌΧΙ	0	0

Ερώτηση 10 - Είναι σημαντικό κατά την γνώμη σας να εκπαιδευτείτε για τα μέτρα αυτά έτσι ώστε να είστε πιο ευαισθητοποιημένοι στα θέματα ασφαλείας Π.Σ της εταιρείας όπου εργάζεστε;

Απαντήσεις από το Τεχνικό Τμήμα:

- Είναι σημαντικό γιατί είναι προτιμότερο να προλάβεις ένα περιστατικό malware παρά να προσπαθήσεις να το αντιμετωπίσεις, που πιθανόν κιόλας να είναι πλέον αργά. Σίγουρα ένα κατάλληλα εκπαιδευμένο προσωπικό αποκτά νέες δεξιότητες, αποκτά αυτοπεποίθηση και είναι πιο αποδοτικό.
- Θεωρώ ότι με αυτό τον τρόπο με το να εκπαιδευτεί το προσωπικό θα γνωρίζει και θα μπορεί πιο εύκολα να αναγνωρίσει ένα κακόβουλο λογισμικό και αν τυχόν

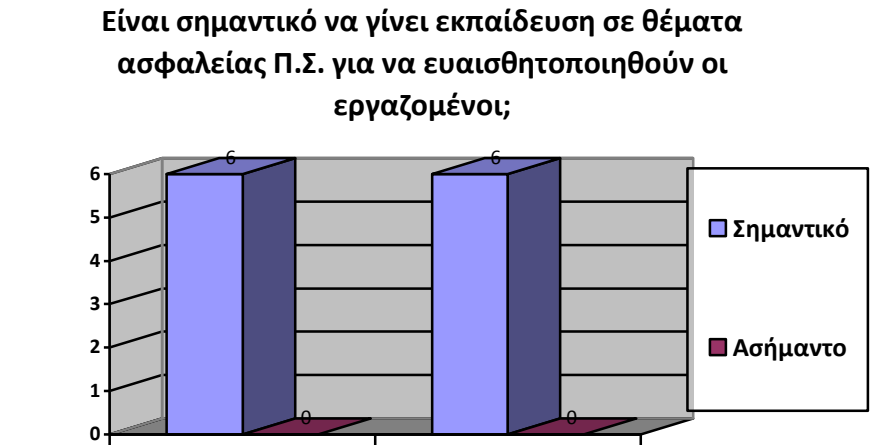
έρθει αντιμέτωπος με κάτι τέτοιο θα γνωρίζει και σίγουρα πώς να το αντιμετωπίσει.

- Ναι είναι σημαντικό γιατί με αυτό τον τρόπο και μέσα από την γνώση που θα πάρουν οι εργαζόμενοι, η εταιρεία μπορεί να προστατεύσει τα πληροφοριακά της συστήματα και να μειώσει τα εταιρικά της έξοδα.
- Είναι πολύ σημαντική η εκπαίδευση και η απόκτηση γνώσεων σε τέτοιες περιπτώσεις, αφού η σωστή χρήση των συστημάτων σε συνδυασμό με τη σωστή ενημέρωση των υπαλλήλων σε τέτοια θέματα μπορεί να μειώσει σε αρκετό βαθμό την πιθανότητα επιτυχούς επίθεσης από malware, αφού θα είμαστε πιο προσεκτικοί και θα γνωρίζουμε με ποιους πιθανούς τρόπους μπορεί να προσληφθούμε από κάποιο malware.
- Πιθανώς ναι για να ξέρουμε τι ακριβώς θα κάνουμε σε περίπτωση που έρθουμε αντιμέτωποι με μία τέτοια κατάσταση.
- Είναι πάρα πολύ σημαντικό να υπάρχει ενημέρωση και εκπαίδευση, έτσι ώστε να μπορούν όλοι να δουλεύουν χωρίς να υπάρχει ρίσκο τόσο για την εταιρεία όσο και για τον εργαζόμενο.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Ναι, πάντα η γνώση των θεμάτων ασφαλείας είναι από τις πιο σημαντικές εκπαιδεύσεις που πρέπει να γίνονται σε κάθε υπάλληλο μιας εταιρείας για αποφυγή δυσάρεστων προβλημάτων όσον αφορά την ασφάλεια.
- Ναι θεωρώ ότι θα ήμασταν όλοι πιο ευαισθητοποιημένοι.
- Ναι. Είναι κάτι ενδιαφέρον που είναι καλό να γνωρίζουν οι υπάλληλοι μιας εταιρείας αφού τις πλείστες φορές που εκθέτουν την εταιρεία σε κίνδυνο δεν το αντιλαμβάνονται καν.
- Ναι είναι αρκετά σημαντικό πιστεύω γιατί με βάση τις γνώσεις τις οποίες θα λάβουμε θα μπορούσαμε να αντιμετωπίσουμε μόνοι μας ένα τέτοιο περιστατικό χωρίς να χρειαστεί να καλέσουμε κάποιο ειδικό και θα μπορούσαμε να προστατεύσουμε τα δεδομένα και αρχεία της εταιρείας μας.
- Σίγουρα θα ήταν σημαντικό να εκπαιδευτούμε για να γνωρίζουμε και εμείς τα θέματα ασφαλείας για να μπορούμε να προστατεύσουμε τα συστήματα και τα αρχεία μας.

- Ναι είναι πολύ σημαντικό να εκπαιδευτούμε για τα μέτρα αυτά, έτσι ώστε να είμαστε πιο ευαισθητοποιημένοι.



Ερώτηση 11 - Θα προτιμούσατε να εκπαιδευόσασταν ή να εκπαιδευτείτε μόνο από σεμινάρια μαθαίνοντας και για πιο θεωρητικά ζητήματα ή μόνο μέσω πρακτικής;

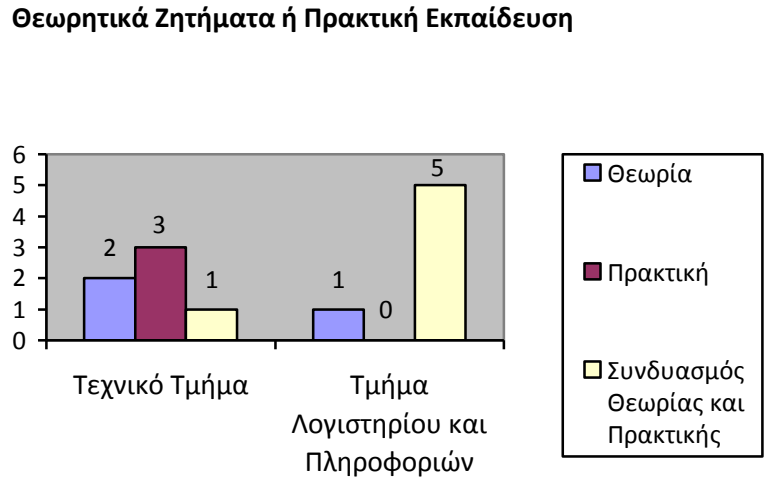
Απαντήσεις από το Τεχνικό Τμήμα:

- Θεωρώ πιο αποτελεσματικό θα ήταν να δημιουργείται ένα θεωρητικό υπόβαθρο.
- Τα θεωρητικά νομίζω ότι είναι πιο κουραστικά και στο τέλος δεν σου μένουν και πολλά. Νομίζω ότι μέσα από την πρακτική σου μένουν πιο πολλά πράγματα.
- Σίγουρα το πιο επιθυμητό θα ήταν να αναλυθούν πρώτα θεωρητικά κάποια μέτρα πρόληψης και αντιμετώπισης των κακόβουλων λογισμικών και να συνδυαστεί αυτό και με την πρακτική επίδειξη ενός ήδη προσβαλλόμενου υπολογιστή από κάποιο malware για περαιτέρω εμπειρική γνώση.
- Θα προτιμούσα αρχικά να γίνει μια θεωρητική προσέγγιση μέσω σεμιναρίων που να περιγράφει τους τρόπους αποφυγής τέτοιων επιθέσεων και τους τρόπους πρόληψης από τέτοιες επιθέσεις.
- Μόνο μέσω πρακτικής άσκησης θα ήταν αρκετή, γιατί έτσι θα τα θυμόμαστε καλύτερα.

- Μέσω πρακτικής για πιο άμεση εκπαίδευση.

Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Και θεωρητικά και πρακτικά, γιατί αν δεν αντιμετωπίσεις στην πράξη τα προβλήματα δεν μπορείς κατά τη γνώμη μου να έχεις γρήγορη ανταπόκριση στην επίλυσή τους.
- Μέσω θεωρίας.
- Και τα δύο πιστεύω ότι είναι εξίσου σημαντικά.
- Πιστεύω ότι βοηθούν και τα δύο εξίσου οπόταν καλό θα ήταν η εκπαίδευση να γίνει και θεωρητικά και πρακτικά.
- Θα προτιμούσα να εκπαιδευόμουν και στα θεωρητικά ζητήματα αλλά και μέσω πρακτικής για πλήρη κατανόηση και κατάρτιση.
- Θα προτιμούσα να εκπαιδευόμουν και για θεωρητικά ζητήματα αλλά και μέσω πρακτικής.



Ερώτηση 12 - Επειδή καθημερινά εργάζεστε συνέχεια με τα Π.Σ της εταιρείας και ανταλλάζετε δεδομένα μέσω email, η πρακτική θα είχε πιο πολύ ενδιαφέρον. Ο συνδυασμός όμως εκπαίδευσης μέσω θεωρίας και πρακτικής πιστεύετε θα είναι ιδανικότερος;

Απαντήσεις από το Τεχνικό Τμήμα:

- Ναι, γιατί έχοντας θεωρητικό υπόβαθρο υπάρχει και καλύτερη κατανόηση για το τι ακριβώς συμβαίνει. Με το κομμάτι της πρακτικής όμως μπορείς να δεις σε πραγματικό περιβάλλον, πραγματικά γεγονότα και πώς τα διαχειρίζεσαι για καλύτερα αποτελέσματα. Συνεπώς, το ένα συμπληρώνει το άλλο.
- Σίγουρα ο συνδυασμός θα ήταν πιο εποικοδομητικός, καθώς η επανάληψη μέσα από την θεωρία και την πρακτική θα επιφέρουν καλύτερα αποτελέσματα.
- Πιστεύω ότι ο συνδυασμός αυτός της εκπαίδευσης μέσω θεωρίας και πρακτικής είναι ο ιδανικότερος, γιατί μόνο τότε οι εκπαιδευόμενοι θα βιώσουν εμπειρικά περιστατικά malware και θα τα αντιμετωπίζουν μετά πιο εύκολα.
- Σίγουρα ο συνδυασμός θεωρίας και πρακτικής επιφέρει μια πιο ολοκληρωμένη εκπαίδευση σε αυτή την περίπτωση, αφού με τη θεωρία μαθαίνεις πληροφορίες σχετικά με το συγκεκριμένο αντικείμενο, ενώ με την πρακτική εξάσκηση χρησιμοποιώντας τα κατάλληλα εργαλεία πετυχαίνεις την αποφυγή τέτοιων περιπτώσεων, οπόταν ο συνδυασμός τους μπορεί να επιφέρει καλύτερα αποτελέσματα.
- Φυσικά, αφού εφαρμόζοντας την θεωρία στην πράξη είναι πολύ πιο εύκολο να γίνει μέρος της καθημερινότητάς μας μέσα και έξω στο χώρο εργασίας.
- Ναι, επειδή για να μπορεί να γίνει σωστή πρακτική πρέπει να υπάρχει αρχικά και η θεωρία αλλά όχι σε μεγάλο βαθμό.

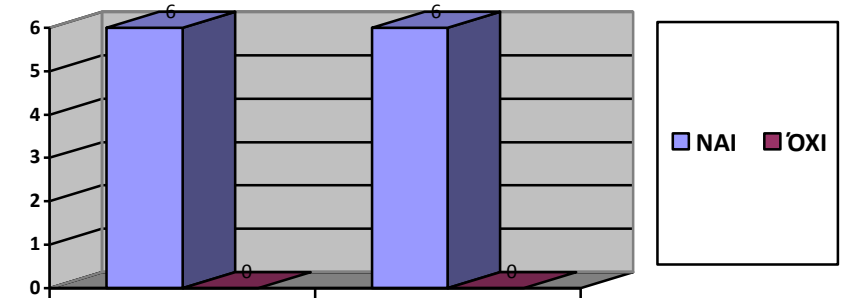
Απαντήσεις από το Τμήμα Λογιστηρίου και Πληροφοριών:

- Ναι πάντα χρειάζεται η θεωρία αλλά και η πρακτική εκπαίδευση για καλύτερη κατανόηση των προβλημάτων και συστημάτων
- Ναι όντως θα ήταν ιδανικότερος για να μπορούμε να μάθουμε κάποιες χρήσιμες πληροφορίες και πως να τις εφαρμόζουμε.
- Η θεωρία είναι καλή για την γενική ενημέρωση σχετικά με το θέμα. Επίσης, μέσω της πρακτικής ο μέσος άνθρωπος μπορεί να συγκρατήσει καλύτερα τις πληροφορίες που θα του δοθούν. Άρα ένας συνδυασμός των 2 θα ήταν το ιδανικότερο.
- Ναι γιατί πρέπει να γνωρίζεις και θεωρητικά κάποια γεγονότα και καταστάσεις γιατί στην πρακτική ίσως να μην έρθεις αντιμέτωπος με κάθε είδος απειλής

οπόταν καλό θα ήταν να γνωρίζεις έστω κάτι περισσότερο από εκείνο της πρακτικής εξάσκησης.

- Σίγουρα θα είναι ο ιδανικότερος γιατί με την θεωρία κατανοείς αυτά που εφαρμόζεις στην πρακτική.
- Σίγουρα θα ήταν η καλύτερη λύση και η πιο αποτελεσματική.

Πιστεύετε πως ο συνδιασμός εκπαίδευσης μέσω θεωρίας και πρακτικής είναι ιδανικότερος;



	Τεχνικό Τμήμα	Τμήμα Λογιστηρίου και Πληροφοριών
NAI	6	6
ΌΧΙ	0	0

3.2 Συμπεράσματα

Η ασφαλής διαχείριση των πληροφοριακών συστημάτων είναι ζωτικής σημασίας για τους οργανισμούς. Αν και οι περισσότεροι οργανισμοί έχουν εδώ και καιρό χρήση τεχνολογιών ασφαλείας, είναι γνωστό ότι η τεχνολογία από μόνη της δεν αρκεί. Η συμπεριφορά του ανθρώπινου δυναμικού ως τελικός χρήστης των συστημάτων έχει αποκτήσει αυξημένη προσοχή. Γίνεται ολοένα και πιο φανερό ότι ο ανθρώπινος παράγοντας είναι η Αχίλλειος πτέρνα της ασφάλειας των πληροφοριακών συστημάτων.

Όλοι οι συμμετέχοντες της έρευνας συμφωνούν απόλυτα ότι ο ανθρώπινος παράγοντας έχει το μεγαλύτερο μέρος ευθύνης για τη σωστή χρήση των συστημάτων της εταιρείας. Όταν τους ζητήθηκε να εξηγήσουν με λίγα λόγια τον όρο malware, στο Τεχνικό Τμήμα είχαν δώσει όλοι σωστά τον ορισμό, ενώ στο Τμήμα Λογιστηρίου και Πληροφοριών 4 από τους 6 τον έδωσαν σωστά (~66%) και 2 από τους 6 τον εξήγησα λανθασμένα (~33%). Αυτό δείχνει πως υπάρχουν άτομα στην εταιρεία που δεν γνωρίζουν τι μπορεί να είναι ένα κακόβουλο λογισμικό και τι επιπτώσεις μπορεί να προκαλέσει ένα τέτοιο

περιστατικό στην εταιρεία. Στην ερώτηση αν έχουν έρθει ποτέ αντιμέτωποι με κάποιο περιστατικό malware δόθηκαν διάφορες απαντήσεις. Μόνο 2 από τους 12 δεν είχαν έρθει αντιμέτωποι πρόσφατα με κάποιο περιστατικό malware (17%). Τα περιστατικά malware που έπληξαν τους εργαζομένους της εταιρείας προέρχονταν από: κατέβασμα αρχείων (8%), pop ups (8%), λογισμικό που άνοιγε από μόνο του την κάμερα του υπολογιστή (8%), Trojan (17%), email (17%) και μέσω phishing – πατώντας σε link (25%). Το Τμήμα των Τεχνικών της εταιρείας ήταν πιο συγκρατημένοι και πιο ψύχραιμοι στην αντιμετώπιση των περιστατικών αυτών, καθώς όλοι κατάφεραν από μόνοι τους να το επιλύσουν είτε μέσω antivirus είτε μέσω format τις πλείστες φορές. Το Τμήμα Λογιστηρίου και Πληροφοριών της εταιρείας μπροστά σε ένα περιστατικό malware είχαν χάσει την ψυχραιμία τους, πανικοβλήθηκαν, αγχώθηκαν και ζήτησαν οι περισσότεροι βοήθεια από ένα τεχνικό υπολογιστών ή από το αρμόδιο τμήμα της εταιρείας για να το επιλύσουν. Τα αποτελέσματα δείχνουν πως το 100% των τεχνικών κατάφεραν και επίλυσαν ένα τέτοιο περιστατικό, ενώ μόλις 2 από τους 6 (~33%) από το Τμήμα Λογιστηρίου και Πληροφοριών κατάφεραν μόνοι τους να το επιλύσουν και 4 στους 6 (~66%) ζήτησαν βοήθεια. Αυτό από μόνο του δείχνει την σημαντικότητα που έχει η εκπαίδευση του ανθρώπινου δυναμικού. Άτομα με γνώση μπόρεσαν από μόνοι τους να επιλύσουν το θέμα. Με συστηματική εκπαίδευση τα περιστατικά αυτά θα περιοριστούν ή και θα εξαλειφθούν, αφού πιο σημαντική από την αντιμετώπιση των περιστατικών αυτών είναι η πρόληψη.

Οι απειλές αλλάζουν συνεχώς και το ανθρώπινο δυναμικό πρέπει να το γνωρίζει και να είναι ενημερωμένο και ευαισθητοποιημένο. Το γιατί οι άνθρωποι συχνά επιδίδονται σε επικίνδυνες πρακτικές είναι ένα μεγάλο θέμα που θα πρέπει να συζητηθεί. Μέσω των πιο πάνω απαντήσεων βλέπουμε το γεγονός πως όταν είχαν έρθει αντιμέτωποι με περιστατικά malware, ανησύχησαν, πανικοβλήθηκαν και προσπάθησαν είτε μόνοι τους είτε μέσω τεχνικών υπολογιστών να λύσουν το θέμα. Βλέπουμε έτσι πως μέσω της άγνοιά τους, οδηγήθηκαν στη λήψη malware και όχι το ότι το ήθελα ή το έκαναν εσκεμμένα. Ρωτώντας τους ποιες μπορεί να είναι οι επιπτώσεις ενός περιστατικού malware για την εταιρεία που εργάζονται απάντησαν πως πιστεύουν ότι η μεγαλύτερη επίπτωση θα ήταν η κλοπή προσωπικών δεδομένων των εργαζομένων και των πελατών κατά 38%, η κλοπή δεδομένων της εταιρείας κατά 29%, η καταστροφή λογισμικών και αρχείων από τους υπολογιστές της εταιρείας κατά 21%, οι επιπτώσεις στην εικόνα της εταιρείας κατά 8% και η παρακολούθηση της εταιρείας κατά 4%. Ενώ

οι καθημερινές απειλές λήψης κακόβουλων λογισμικών στην εταιρεία είναι το email κατά 31%, οι ιστοσελίδες – διαφημίσεις και pop-ups κατά 30%, το κατέβασμα αρχείων κατά 23%, το phishing, οι διάφορες εφαρμογές, η λανθασμένη χρήση συστημάτων καθώς και οι συσκευές εισόδου/εξόδου (usb, σκληρός δίσκος κλπ.) κατά 4% ξεχωριστά.

Η αμέλεια των εργαζομένων ή η μη συμμόρφωση τους με τις πολιτικές ασφαλείας των πληροφοριακών συστημάτων του οργανισμού συχνά κοστίζουν εκατομμύρια στις επιχειρήσεις. Οι ελλείψεις για πρόληψη, αντιμετώπιση ή έστω ελαχιστοποίηση των περιστατικών malware που έχουν σχέση με τον τελικό χρήση, δηλαδή τον ανθρώπινο παράγοντα είναι δείκτες των αποτυχημένων πολιτικών ασφαλείας των πληροφοριακών συστημάτων. Μέσα από τα αποτελέσματα της έρευνας αυτής, βλέπουμε πως όλοι οι συμμετέχοντες συμφωνούν στο ότι τελικά οι χρήστες των υπολογιστών διαδραματίζουν το σημαντικότερο ρόλο για την εξασφάλιση ασφαλή συστημάτων. Και ότι η μία από τις μεγαλύτερες απειλές είναι ο ανθρώπινος παράγοντας.

Το ανθρώπινο δυναμικό πρέπει να συμμορφώνεται πλήρως με την πολιτική ασφαλείας των πληροφοριακών συστημάτων του οργανισμού. Από τα αποτελέσματα της έρευνας προκύπτει πως στην συγκεκριμένη εταιρεία και μπορεί και σε αρκετές άλλες εταιρείες στην Κύπρο ενώ η δουλειά τους έχουν να κάνουν με Διαδίκτυο και πληροφοριακά συστήματα, η Διοίκηση δεν έχει παρέχει στο ανθρώπινο δυναμικό κάποια μορφή εκπαίδευσης στην πολιτική ασφάλειας των πληροφοριακών συστημάτων. Το Τεχνικό Τμήμα όσο και το Τμήμα Λογιστηρίου και Πληροφοριών πιστεύουν πως ένα τέτοιο σεμινάριο ή εκπαίδευση θα βοηθήσει στην σωστή χρήση των συστημάτων και στην αποφυγή περιστατικών malware, καθώς επίσης είναι πολύ σημαντικό να εκπαιδευτούν για τα μέτρα πρόληψης και αντιμετώπισης των περιστατικών malware έτσι ώστε να είναι πιο ευαισθητοποιημένοι στα θέματα ασφαλείας πληροφοριακών συστημάτων του οργανισμού. Έτσι, προτείνεται ένα πρόγραμμα κατάρτισης που βασίζεται σε δύο προσεγγίσεις, την θεωρητική προσέγγιση και την πρακτική προσέγγιση στα θέματα ασφαλείας των πληροφοριακών συστημάτων και στην πολιτική ασφαλείας του οργανισμού.

Θετικά αποτελέσματα φαίνεται να έχει η θεωρητική προσέγγιση αφού τα άτομα από το Τεχνικό Τμήμα, δείχνουν να είναι πιο κατάλληλα καταρτισμένα και εν γνώση για το πώς

να προλάβουν ή να αντιμετωπίσουν κάποιο περιστατικό κακόβουλου λογισμικού. Η πρακτική προσέγγιση υποδηλώνει πως θα πρέπει να χρησιμοποιηθεί περιεχόμενο και μέθοδοι που να παρακινούν το ανθρώπινο δυναμικό στη συστηματική πληροφόρηση και εκπαίδευσή τους. Αποτελεσματικές μέθοδοι πρακτικής προσέγγισης μπορεί να είναι η εκπαίδευση μέσω βίντεο και η εκπαίδευση σε πραγματικό περιστατικό, σίγουρα από κάποιο αρμόδιο άτομο που κατέχει το συγκεκριμένο θέμα. Η συνεχής εκμάθηση σίγουρα βελτιώνει τη συμμόρφωση των χρηστών στις πολιτικές ασφαλείας των πληροφοριακών συστημάτων.

Το πρόγραμμα κατάρτισης μέσω πρακτικής προσέγγισης προτιμάται περισσότερο από τους τεχνικούς, ακολουθεί η θεωρητική προσέγγιση και μετά ο συνδυασμός των δύο. Πιο έντονο αίσθημα για μάθηση δείχνουν να έχουν τα άτομα από το Τμήμα Λογιστηρίου και Πληροφοριών, οι οποίοι ούτε μέσω των σπουδών τους έχουν ασχοληθεί με τον όρο malware, ή με θέματα ασφαλείας των πληροφοριακών συστημάτων. Το Τμήμα Λογιστηρίου και Πληροφοριών φαίνεται να χρειάζεται κατά 10% εκπαίδευση μόνο μέσω θεωρίας και κατά 90% εκπαίδευση αρχικά μέσω θεωρητικών σεμιναρίων και ακολούθως μία σειρά σεμιναρίων μέσω πρακτικής άσκησης για πιο επιθυμητά αποτελέσματα.

Και τα δύο όμως τμήματα συμφωνούν απόλυτα πως ο συνδυασμός των δύο αυτών προσεγγίσεων είναι ο ιδανικότερος, αφού καθημερινά έρχονται σε επαφή με τα πληροφοριακά συστήματα της εταιρείας, ανταλλάζουν δεδομένα μέσω email και γενικά χρησιμοποιούν το διαδίκτυο από τους υπολογιστές του οργανισμού.

Ένα σεμινάριο μπορεί να περιλαμβάνει την εκμάθηση των απειλών και των τρωτών σημείων των συστημάτων, έτσι ώστε να ευαισθητοποιηθούν οι εργαζόμενοι και να κατανοήσουν τις διάφορες απειλές, να συνειδητοποιήσουν ότι υπάρχουν διάφορα τεχνολογικά μέσα για τη μείωση του κινδύνου, όπως η χρήση λογισμικού προστασίας από ιούς, να μην μοιράζονται τους κωδικούς του κλπ. Επίσης, μέσω των σεμιναρίων να κατανοήσουν ακόμη περισσότερο τις πιθανές αρνητικές συνέπειες σε περίπτωση παραβίασης των πολιτικών ασφαλείας του οργανισμού, συμπεριλαμβανομένου της απώλειας δεδομένων της εταιρείας, καθώς και την απώλεια προσωπικών δεδομένων. Επιπρόσθετα, σημαντικό είναι να μάθουν για την ευκολία ανάκτησης των δεδομένων,

έτσι ώστε να χρησιμοποιούν την μέθοδο backup – δημιουργία αντιγράφων αρχείων και δεδομένων.

Κεφάλαιο 4

Επίλογος

Καθώς σχεδόν οποιαδήποτε υπηρεσία ή οργανισμός, ιδρύματα, εταιρείες και ιδιώτες χρησιμοποιούν υπολογιστές με πρόσβαση στο διαδίκτυο, η ανάγκη για την προστασία των δεδομένων είναι επιτακτική και ολοένα αυξανόμενη μιας που η μη εξουσιοδοτημένη πρόσβαση στις διακινούμενες πληροφορίες είναι σχετικά εύκολη και έχει ενδεχομένως καταστρεπτικές συνέπειες για την εύρυθμη λειτουργία των οργανισμών.

Το πρόβλημα της ασφάλειας στα πληροφοριακά συστήματα και στο Διαδίκτυο έχει απασχολήσει έντονα όλους όσων τα συμφέροντα διακυβεύονται με αυτά σε μεγάλο βαθμό και έχει κινητοποιήσει τόσο την επιστημονική κοινότητα όσο και εταιρείες ανάπτυξης λογισμικού και δικτυακών υποδομών προς την κατεύθυνση της πληρέστερης κατανόησης και επίλυσής του.

Το κακόβουλο λογισμικό είναι αναμφισβήτητα μία αναγνωρισμένη απειλή στο χώρο της Πληροφορικής εδώ και πολλά χρόνια, εξακολουθεί να είναι ένα από τα μεγαλύτερα προβλήματα του σήμερα που αντιμετωπίζουν πολλές επιχειρήσεις. Αυτό οφείλεται στο γεγονός ότι, παρά τις βελτιώσεις των προστατευτικών τεχνολογιών, πολλά συστήματα δεν χρησιμοποιούν αποτελεσματικά τις τεχνολογίες αυτές και οι χρήστες τους δεν είναι κατάλληλα ενημερωμένοι για τις πρακτικές πρόληψης και αντιμετώπισης που πρέπει να εφαρμόζει ένας οργανισμός.

Η μη συμμόρφωση των υπαλλήλων σε ένα οργανισμό αποτελεί ένα από τα βασικότερα προβλήματα για την ασφάλεια των πληροφοριακών συστημάτων. Γενικά, εάν το ανθρώπινο δυναμικό δεν συμμορφώνεται με τις πολιτικές ασφαλείας των πληροφοριακών συστημάτων του οργανισμού, η ασφάλεια του οργανισμού χάνει την αποτελεσματικότητά της.

Αναμφίβολο είναι το γεγονός ότι το κακόβουλο λογισμικό θα συνεχίσει να αναπτύσσεται, να εξαπλώνεται γρήγορα και αποδοτικά προκαλώντας μεγάλη λειτουργική και οικονομική δυσχέρεια στους οργανισμούς. Έτσι, χρειάζεται συνεχής προσπάθεια από τις επιχειρήσεις για την πρόληψη και αντιμετώπιση των περιστατικών malware ώστε να μπορούν πάντα να ανταποκρίνονται στις νέες προκλήσεις που προέρχονται από το κακόβουλο λογισμικό. Επίσης, χρειάζεται συνεχής ενημέρωση και εκπαίδευση του ανθρωπίνου δυναμικού, αφού είναι και οι κύριοι χρήστες των πληροφοριακών συστημάτων των εταιρειών.

Προτείνεται στις επιχειρήσεις να δίνουν έμφαση στα θέματα ασφαλείας πληροφοριακών συστημάτων και να κάνουν συχνά σεμινάρια στους εργαζομένους τους, έτσι ώστε να προλάβουν και να αποτρέψουν να πληγούν από περιστατικά malware. Οι εργαζόμενοι άθελα τους μπορεί να μολύνουν ολόκληρο το δίκτυο της εταιρείας με αποτέλεσμα η εταιρεία να χρειαστεί αρκετό κεφάλαιο για να διορθώσει το δίκτυό της. Σίγουρα μέσω συνεχής εκπαίδευσης ή δίνοντας κίνητρα στους εργαζομένους των εταιρειών, τέτοια θέματα μπορούν να ελαχιστοποιηθούν και οι εταιρείες να μην έρχονται τόσο συχνά σε κίνδυνο, ούτε να είναι σε θέση να εκθέσουν την εικόνα τους. Δίνοντας κίνητρα και γνώση στους εργαζομένους, χωρίς να τους ασκούνται κυρώσεις ή πιέσεις για την σωστή χρήση των συστημάτων ή για τη μη συμμόρφωση με τους κανονισμούς, οι επιχειρήσεις έχουν θετικά αποτελέσματα. Είναι στο χέρι των εταιρειών πως τελικά θα πράξει το ανθρώπινο δυναμικό.

Πρόκληση για τις επιχειρήσεις είναι το ποσό που χρειάζονται να διαθέσουν για να έχουν ασφαλή συστήματα, το οποίο ανέρχεται σε χιλιάδες ετησίως αν έχουν έστω και μια μέση παρουσία στο διαδίκτυο. Αν το ποσό αυτό είναι απαγορευτικό για να το διαθέσει μια επιχείρηση, τότε θα πρέπει να αποδεχτεί τον κίνδυνο. Για τις επιχειρήσεις με νομικές, ιατρικές ή κυβερνητικές πρακτικές, όπου η απώλεια δεδομένων μπορεί να οδηγήσει σε αστικές και ποινικές κυρώσεις, δεν υπάρχει άλλη επιλογή πέραν του να διαθέσουν το πόσο για να αυξήσουν την ασφάλεια στις επιχειρηματικές λειτουργίες τους. Επίσης, πρόκληση για μία επιχείρηση είναι το να βρουν πιο αποτελεσματικούς μηχανισμούς ανίχνευσης malware. Έτσι, οι επιχειρήσεις θα βοηθηθούν στο να αποτρέψουν πολλούς από τους κινδύνους που παρουσιάζουν τα σημερινά malware, τα οποία πλέον χρησιμοποιούν πολλαπλές μεθόδους για να αποκρύψουν την ύπαρξη τους μέσα στο σύστημα και καταστούν πολύ δύσκολο το να γίνουν αντιληπτά από τα μέσα

ανίχνευσης. Χρειάζεται επίσης, να υιοθετήσουν μια πολυεπίπεδη στρατηγική άμυνας Web που μπορεί να προστατεύσει τους χρήστες και τα δίκτυα της επιχείρησης από ολοένα και πιο εξελιγμένες μορφές malware.

Οι οργανισμοί από μόνοι τους δεν μπορούν να μετριάσουν τους κινδύνους malware, η ευθύνη εκτείνεται επίσης στις κυβερνήσεις, στους τελικούς χρήστες και στους διεθνείς φορείς. Η συλλογική προσπάθεια αυτών των οντοτήτων είναι αναγκαία, προκειμένου να αμβλυνθούν τα εγκλήματα που διαπράττονται μέσω του Διαδικτύου.

Παράρτημα Α
Ερωτήσεις Συνέντευξης

Δημογραφικά Στοιχεία:

Φύλο -

Ηλικία -

Τμήμα στην εταιρεία -

Χρόνια στην εταιρεία -

Σπουδές -

Όνομα - Ανώνυμο

Καλησπέρα σας, θα ήθελα να σας ευχαριστήσω για τον χρόνο που διαθέτετε για την διεξαγωγή της ερευνάς μου και επίσης για το ενδιαφέρον που δείχνετε. Ο στόχος της Διατριβής μου έχει να κάνει με το πόσο σημαντική είναι η εκπαίδευση και η ευαισθητοποίηση του Ανθρώπινου Δυναμικού στα μέτρα ασφαλείας των Πληροφοριακών Συστημάτων των εταιρειών.

1) Εσείς τι πιστεύετε για αυτό; Ο ανθρώπινος παράγοντας έχει μέρος ευθύνης για την σωστή χρήση των συστημάτων της εταιρείας;

2) Αν σας δινόταν η ευκαιρία να εξηγήσετε με λίγα λόγια τον όρο malware / κακόβουλο λογισμικό, πως θα τον ορίζατε; (Εδώ καταγράφετε η απάντηση αλλά αν δίνεται λανθασμένα ο ορισμός, εξηγώ με λίγα λόγια τον ορισμό για να γίνει πιο σωστά το υπόλοιπο μέρος της έρευνας)

3) Έχετε έρθει ποτέ αντιμέτωπος/η με κάποιο περιστατικό malware (πως/ποτε αν θυμάστε/τι έγινε/τι περιστατικό ήταν);

4) Ποια ήταν η πρώτη σας αντίδραση και πως προσπαθήσατε να το αντιμετωπίσετε;

5) Έχετε σκεφτεί ποτέ ποιες επιπτώσεις μπορεί να έχει ένα περιστατικό malware;

(Εδώ αν η απάντηση είναι ναι - Ποιες 2 επιπτώσεις είναι οι πιο σοβαρές κατά την γνώμη σας που πρέπει κάθε οργανισμός να αντιμετωπίσει;

Αν η απάντηση είναι όχι - Μπορείτε να σκεφτείτε 2 επιπτώσεις που είναι οι πιο σοβαρές κατά την γνώμη σας που κάθε οργανισμός πρέπει να αντιμετωπίσει;)

6) Ποιες πιστεύετε πως είναι οι καθημερινές απειλές λήψης κακόβουλου λογισμικού / malware;
7) Ο ανθρώπινος παράγοντας είναι απειλή; Τι γνώμη έχετε;
8) Σας έχει γίνει κάποιο σεμινάριο ή κάποια εκπαίδευση από την εταιρεία για τα μέτρα πρόληψης και αντιμετώπισης των περιστατικών malware;
9) Πιστεύετε πως ένα τέτοιο σεμινάριο ή εκπαίδευση θα βοηθούσε ή σας έχει βοηθήσει στην ορθή χρήση των συστημάτων και την αποφυγή τέτοιων περιστατικών;
Αν η απάντηση στην ερώτηση 8 είναι όχι ακολουθεί η ερώτηση:
10) Είναι σημαντικό κατά την γνώμη σας να εκπαιδευτείτε για τα μέτρα αυτά, έτσι ώστε να είστε πιο ευαισθητοποιημένοι στα θέματα ασφαλείας Π.Σ της εταιρείας όπου εργάζεστε;
Αν η απάντηση στην ερώτηση 8 είναι ναι ακολουθεί η ερώτηση:
10) Έχοντας εκπαιδευτεί για τα μέτρα πρόληψης και αντιμετώπισης των περιστατικών αυτών, νιώθετε πιο ευαισθητοποιημένοι στα θέματα ασφαλείας Π.Σ της εταιρείας όπου εργάζεστε;
Ακολουθούν:
11) Θα προτιμούσατε να εκπαιδευόσασταν ή να εκπαιδευτείτε μόνο από σεμινάρια μαθαίνοντας και για πιο θεωρητικά ζητήματα ή μόνο μέσω πρακτικής;
12) Επειδή καθημερινά εργάζεστε συνέχεια με τα Π.Σ της εταιρείας και ανταλλάζετε δεδομένα μέσω email, η πρακτική θα είχε πιο πολύ ενδιαφέρον. Ο συνδυασμός όμως εκπαίδευσης μέσω θεωρίας και πρακτικής πιστεύετε θα είναι ιδανικότερος;

Εδώ είναι το τέλος της συνέντευξης μας, σας ευχαριστώ πολύ και πάλι για τον χρόνο που διαθέσατε. Καλό απόγευμα.

Βιβλιογραφία

Allen, M. (2006) Social *Emgineering: A Means to Violate A Computer System.* SANS Information Security Reading Room. Available at: http://www.sans.org/reading_room/ whitepapers/ engineering/social-engineering-means-violate-computer-system_529

ALU, Motive Security Labs. (2014) Malware Report – H2 2014. Available at: https://www.alcatel-lucent.com/press/2015/alcatel-lucent-report-malware-2014-sees-rise-device-and-network-attacks-place-personal-and-workplace

Aycock, J. (2006) *Computers Viruses and Malware.* Advances in Information Security, University of Calgary Canada. Available at: http://www. scribed.com/dpc/19658063/computer-Viruses-and-Malware-2006

Blum, J. (2011) *How to Protect Your Business from Malware in Custom Apps.* September, 26, 2011. Available at: http://www.entrepreneur.com/article/220370

Cavusoglu, H., Raghunathan, S., Mishra, B. (2004) *A Model for Evaluating IT Security Investments*. Communications of the ACM 47(7): 87-92. Available at: http://dl.acm.org/citation.cfm?doid=1005817.1005828

Cisco. (2006) *Understanding remote worker security.* Available at: http://www.cisco.com/web/CA/pdf/Understanding_Remote_Worker_Security_A_survey_of_User_Awareness_vs_Behaviour.pdf

Edge, C., Barker, W., Hunter, B., Sullivan, G. (2010) *Malware Security: Combating Viruses, Worms, and Root Kits.* Enterprise Mac Security, 213-132. Available at: http://link.springer.com/chapter/10.1007%2F978-1-4302-2731-1_8

Furnell, S., Ward, J. (2004) *Malware comes of age: The arrival of the true computer parasite.* Available at: http://www.sciencedirect.com/science/article/pii/S1353485804001448

Gordon, L. A., Loeb, M.P. (2006) *Managing Cybersecurity Resources: A Cost-Benefit Analysis.* New York, McGraw-Hill.

Jakobbson, M., Myers, S. (2006) *Phishing and countermeasures: understanding the increasing problem of electronic identity theft.* Wiley-Interscience, 2006. Available at: http://www.google.gr/books?hl=el&lr=&id=xxAbEcNlIwwC&oi=fnd&pg=PR3&dq=Jakobbson,+M.,+Myers,+S.,+2006.+Phishing+and+countermeasures:+understanding+the+increasing+problem+of+electronic+identity+theft.+Wiley-Interscience,+2006&ots=JTlOrzBqsz&sig=qDHAeudpcgcex9dF6bfoJF_xaEQ&redir_esc=y#v=onepage&q&f=false

Kapersky Lab (2013) *Global Corporate IT Security Risks: 2013.* Available at: https://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

Kapersky Lab (2014) *Global IT Securty Risks Survey 2014 - Distributed Denial of Service (DDoS) Attacks.* Available at: https://media.kaspersky.com/en/B2B-International-2014-Survey-DDoS-Summary-Report.pdf

Kaspersky Lab (2015), *Financial Fraud: The Impact on Corporate Spend IT Security Risks Special Report Series.* Available at: http://press.kaspersky.com/files/2015/11/Kaspersky_Lab_IT_Risks_Survey_Report_Financial_Fraud.pdf

Kruegel, C. (2012) *Fighting Malicious Software.* Available at: http://link.springer.com/chapter/10.1007/978-3-642-35130-3_1#page-1

Mell, P., Kent, K., Nusbaum, J. (2005) *Guade to Malware Incident Prevention and Handling*. Information Technology Laboratory, National Institute of Stanfords and Technology,

Gaitherburg. November 2005. Available at: http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

Milosevic, N. (2013) History of malware. Inspiratron.org. Available at: http://arxiv.org/abs/1302.5392

Niccolai, J. (2000) *Analyst Puts Hacker Damage at $1.2B*. InfoWorld. Available at: http://www.computerworld.com.au/article/91948/analyst_puts_hacker_damage_us_1_2b_rising/

OECD, (2002). The OECD 2002 Security Guidelines - Q&A. Ogut, H., N. Menon and S. Raghunathan (2005). *Cyber insurance and IT security investment: Impact of interdependent risk.* Fourth Workshop on the Economics of Information Security. Harvard University

Puhakainen, P. (2006) *A design theory for information security awareness.* Unpublished dissertation, University of Oulu: Oulu, Finland, 2006. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95.6140

Rizwan, R., Dr. Hazarika, G.C., Gunadeep, C. (2011) *Malware threats and mitigation strategies: A survey*. July 2011. Available at: http://www.jatit.org/volumes/research-papers/Vol29No2/3Vol29No2.pdf

Rutwoska, J. (2006) *Introducting Stealth Malware Taxonomy.* COEINC Advanced Malware Labs, Version1.01. November 2006 Available at: https://invisiblethings.org/papers/malware-taxonomy.pdf

SANS Policy Team, 2014. *Password Construction Guidelines.* Consensus Policy Resource Community, June 2014. Available at: http://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines

SANS Policy Team, 2014. *Password Protection Policy.* Consensus Policy Resource Community, June 2014. Available at:

http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

SANS Policy Team, 2014. *Wireless Communication Standard.* Consensus Policy Resource Community, June 2014. Available at: http://www.sans.org/security-resources/policies/network-security/pdf/wireless-communication-standard

SANS Policy Team, 2014. *Software Installation Policy.* Consensus Policy Resource Community, June 2014. Available at: http://www.sans.org/security-resources/policies/server-security/pdf/software-installation-policy

Sherly, A., InduShobha, C.S. (2010) *An overview of of social engineering malware: Trends, tactics, and implications. Technology in Society 32 (2010), 183-196.* Available at: http://journals.ohiolink.edu/ejc/article.cgi?issn=0160791x&issue=v32i0003&article=183_aoosemttai

Siponen, M. (2000) *A conceptual foundation for organizational IS security awareness.* Information Management & Computer Security 2000, 8, 4-31. Available at: http://www.emeraldinsight.com/journals.htm?articleid=862758&show=abstract

Siponen, M., Oinas-Kukkonen, H. (2007) *A review of information security issues and respective research Contributions.* Database for Advances in Information Systems 2007, 60–81. Available at: http://dl.acm.org/citation.cfm?id=1216224

Slammer. (2009) FSecure Threat description, Internet. Available at: http://www.f-secure.com/v-descs/mssqlm.shtml

Souppaya, M., Scarfone, K. (2012) *Guide to Malware Incident Prevention and Handling for Desktops and Laptops (Draft).* July 2012. Available at: http://csrc.nist.gov/publications/drafts/800-83-rev1/draft_sp800-83-rev1.pdf

Stanton, J., Stam, K., Mastrangelo, P., Jolton, J. (2005) *Analysis of end user security behavior*. Computers & Security 2005, 24, 33-124. Available at: http://www.sciencedirect.com/science/article/pii/S0167404804001841

Weaver, N., Paxson, V., Staniford, S., Cunningham, R. (2003) *A Taxonomy of Computer Worms.* October 2003 Available at: http://dl.acm.org/citation.cfm?id=948190

Κρασανάκη Ζ. (2010) *Ανάλυση μετάδοσης κακόβουλου λογισμικού σε δυναμικά συστήματα δικτύων και υπολογιστών.* Σεπτέμβριος 2010. Διαθέσιμο: http://nemertes.lis.upatras.gr/jspui/bitstream/10889/4784/3/Nimertis_Krasanaki%28ele%29.pdf

Μπίρδα, Α. (2012) *Θέματα Ασφαλείας Δεδομένων Ευφυών Δικτύων Διανομής Ηλεκτρικής Ενέργειας.* Διπλωματική Εργασία, Θεσσαλονίκη. Διαθέσιμο: http://vivliothmmy.ee.auth.gr/1897/1/CyberSecurity_Athina_Mpirda.pdf

Παπαθανάση, Α. (2012) *Σύστημα μοντελοποίησης της εξάπλωσης κακόβουλου λογισμικού σε ευρείας κλίμακας δίκτυα.* Πτυχιακή εργασία, Λάρισα. Διαθέσιμο: http://ifestos.teilar.gr/index.php?option=com_docman&task=doc_view&gid=150

SANS Policy Team, 2014. *Password Construction Guidelines.* Consensus Policy Resource Community, June 2014. Available at: http://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines