ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ. «Ασφάλεια Ψηφιακών Συστημάτων»

Διπλωματική εργασία

Εκπαίδευση προσωπικού για ευαισθητοποίηση στην ασφάλεια πληροφοριών

Αλέξανδρος Μαυρόματος ΜΤΕ1726

Επιβλέπων καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2017-2018

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Λαμπρινουδάκη Κωνσταντίνο για την ανάθεση και την καθοδήγηση της παρούσας διπλωματικής εργασίας.

Μαυρόματος Αλέξανδρος

Περίληψη

Στα πλαίσια της παρούσας διπλωματικής εργασίας αναλύεται η σημαντικότητα της εκπαίδευσης του προσωπικού μιας εταιρείας/οργανισμού σε θέματα που αφορούν την ασφάλεια Πληροφοριακών Συστημάτων.

Στόχος της διπλωματικής είναι ο αναγνώστης να κατανοήσει τους σκοπούς της εκπαίδευσης ευαισθητοποίησης σε θέματα ασφαλείας καθώς και τους τρόπους με τους οποίους μπορεί αυτή να υλοποιηθεί.

Οι τύποι της εκπαίδευσης, οι ρόλοι κι οι ευθύνες κάθε εργαζομένου με βάση τη θέση του στον οργανισμό, καθώς και το περιεχόμενο της εκπαίδευσης ευαισθητοποίησης αποτελούν τον πυρήνα αυτής της διπλωματικής, η οποία μπορεί να χρησιμοποιηθεί ή να αποτελέσει πηγή έμπνευσης για ένα ρεαλιστικό πρόγραμμα εκπαίδευσης σχετική με θέματα ασφαλείας.

Επιπλέον, αναφέρονται τρόποι ανάπτυξης στρατηγικής και πλάνου ενώ δίνεται σημασία και στην ανάπτυξη του υλικού που θα μπορούσε να χρησιμοποιηθεί σε ένα πρόγραμμα εκπαίδευσης.

Η διπλωματική ολοκληρώνεται με κάποιες βέλτιστες πρακτικές, εμπόδια που μπορεί να χρειαστεί να αντιμετωπιστούν μέσα σε ένα τέτοιο πρόγραμμα, μεθόδους αξιολόγησης της εκπαίδευσης και ορισμένα τελικά συμπεράσματα.

Περιεχόμενα

1. Εισαγωγή

Η εκπαίδευση για την ευαισθητοποίηση σχετικά με την ασφάλεια είναι κάτι περισσότερο από εκπαίδευση συμπεριφοράς στην ασφάλεια: ο στόχος είναι να παρέχει πληροφορίες στους εργαζόμενους που θα τους βοηθήσουν να είναι πιο ενημερωμένοι για τις απειλές κατά της ασφάλειας, πιο σκεπτικοί σχετικά με το τι λαμβάνουν μέσω ηλεκτρονικού ταχυδρομείου ή μέσω άλλων καναλιών, και είναι λιγότερο πιθανό να διαπράξουν καταστροφικές συμπεριφορές όπως κάνοντας κλικ σε κακόβουλους συνδέσμους στο ηλεκτρονικό ταχυδρομείο, στην αναμετάδοση σε κοινωνικά μέσα ή πιστεύοντας σε αιτήματα που υποβάλλονται μέσω ηλεκτρονικών καναλιών χωρίς πρώτα να τα επαληθεύσουν.

Κάποια σημεία κλειδιά που κάνουν την εκπαίδευση ευαισθητοποίησης επιτακτική ανάγκη για τις εταιρείες είναι:

- *Οι επαγγελματίες ασφαλείας έχουν πολλές ανησυχίες*

Η έρευνα αποκάλυψε ότι υπάρχει ένα ευρύ φάσμα ζητημάτων σχετικά με τους επαγγελματίες ασφαλείας, αλλά οι πιο πιεστικές ανησυχίες επικεντρώνονται στις παραβιάσεις δεδομένων, στο ηλεκτρονικό ψάρεμα (phishing) και στο ransomware. Είναι ενδιαφέρον ότι αυτά είναι όλα τομείς στους οποίους η καλή εκπαίδευση για την ευαισθητοποίηση στον τομέα της ασφάλειας μπορεί να είναι ιδιαίτερα αποτελεσματική μειώνοντας τον κίνδυνο.

- *Οι περισσότερες οργανώσεις έχουν πέσει θύματα*

Η συντριπτική πλειοψηφία των οργανώσεων έχουν πέσει θύματα διαφόρων τύπων απειλών για την ασφάλεια, με κύριες το ηλεκτρονικό ψάρεμα, που ήταν επιτυχής στη μετάδοση κακόβουλου λογισμικού, στοχευμένες επιθέσεις ηλεκτρονικού ταχυδρομείου και παραβιάσεις δεδομένων.

- *Το ηλεκτρονικό ψάρεμα (phishing) και το spearphishing*

Περισσότερο από το 90% των οργανισμών αναφέρουν ότι οι προσπάθειες προσέγγισης των τελικών χρηστών τους τελευταίους 12 μήνες στο ηλεκτρονικό ψάρεμα και στο στοχευμένο ηλεκτρονικό ψάρεμα (spearphishing) αυξάνονται ή παραμένουν στα ίδια επίπεδα.

- *Η εμπιστοσύνη στην τρέχουσα εκπαίδευση στον τομέα της ασφάλειας είναι χαμηλή*

Όταν επαγγελματίες στον χώρο της ασφάλειας ερωτήθηκαν για την αντιληπτή αποτελεσματικότητα της τρέχουσας ασφάλειάς στο πρόγραμμα κατάρτισης ευαισθητοποίησης σχετικά με την ασφάλεια έναντι της τρέχουσας υποδομής ασφαλείας, εξέφρασαν μεγαλύτερη εμπιστοσύνη στην υποδομή σε ένα ευρύ φάσμα τύπων απειλών.

- *Η εκπαίδευση για την ευαισθητοποίηση σχετικά με την ασφάλεια δεν είναι επαρκής στις περισσότερες περιπτώσεις*

Το γεγονός ότι η υποδομή ασφάλειας θεωρείται ως καλύτερο μέσο πρόληψης στη διείσδυση των απειλών απ 'ό, τι η συνειδητοποίηση της ασφάλειας δεν προκαλεί έκπληξη δεδομένου του ότι η κατάρτιση είναι συχνά σε μεγάλο βαθμό ανεπαρκής. Έχει διαπιστωθεί ότι ορισμένες οργανώσεις δεν παρέχουν ποτέ την εκπαίδευση ευαισθητοποίησης για τους χρήστες τους και για εκείνους που το κάνουν πολλές φορές είναι σπάνιο και ανεπαρκής.

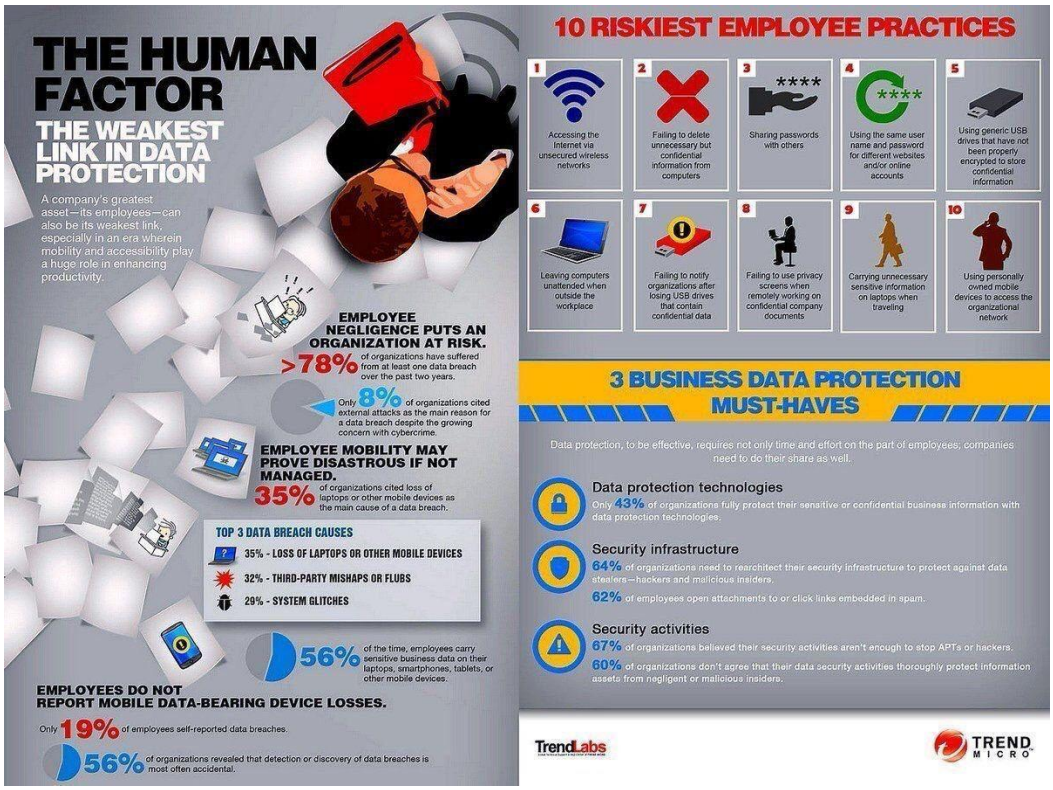
- *Οι ανώτεροι διευθυντές επιχειρήσεων, οι χρήστες δεν είναι ενθουσιασμένοι με τα προγράμματα εκπαίδευσης*

Ενώ η πλειοψηφία του προσωπικού πληροφορικής υποστηρίζει και ενθουσιάζεται με το πρόγραμμα κατάρτισης ευαισθητοποίησης σχετικά με την ασφάλεια, οι ανώτεροι διευθυντές επιχειρήσεων δεν δείχνουν αντίστοιχο ενδιαφέρον. [1]

2. Σκοποί και οφέλη της εκπαίδευσης

Η ασφάλεια σε κάθε πληροφοριακό σύστημα μιας εταιρείας καθορίζεται από το χαμηλότερο μέτρο προστασίας, όπου στις περισσότερες περιπτώσεις ο ανθρώπινος παράγοντας είναι ο πιο αδύναμος κρίκος. Αυτό καθιστά πολύ σημαντική την εκπαίδευση των χρηστών του πληροφοριακού συστήματος.

Ένας από τους καλύτερους τρόπους για να βεβαιωθείτε ότι οι υπάλληλοι της εταιρείας δεν θα κάνουν δαπανηρά λάθη όσον αφορά την ασφάλεια των πληροφοριών είναι να δημιουργηθούν εταιρικές πρωτοβουλίες κατάρτισης για την ευαισθητοποίηση σε θέματα ασφάλειας που περιλαμβάνουν εκτός των άλλων συνεδρίες εκπαίδευσης σε τάξη, ιστότοπους ευαισθητοποίησης σχετικά με την ασφάλεια, χρήσιμες συμβουλές μέσω ηλεκτρονικού ταχυδρομείου ή ακόμη και αφίσες. Αυτές οι μέθοδοι μπορούν να βοηθήσουν τους εργαζόμενους να έχουν μια σταθερή κατανόηση της πολιτικής ασφαλείας της εταιρείας, των διαδικασιών και των βέλτιστων πρακτικών. [2]



Εικόνα 1 – Ο ανθρώπινος παράγοντας στην προστασία δεδομένων

2.1 Συχνότητα εκπαίδευσης

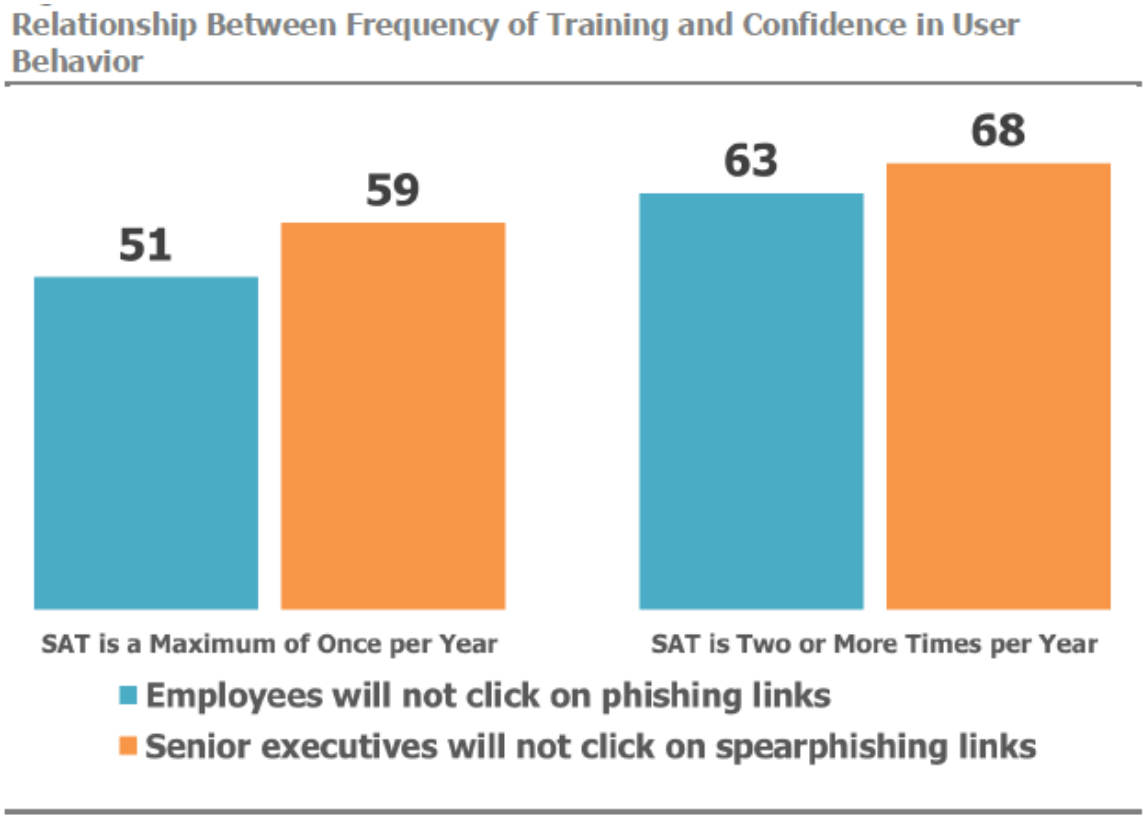
Συνιστάται όλοι οι υπάλληλοι να λαμβάνουν εκπαίδευση για την ενημέρωση σχετικά με την ασφάλεια και την διαχείριση έκτακτης ανάγκης κατά την πρόσληψή τους, όπως κρίνει σκόπιμο ο εκάστοτε οργανισμός/εταιρεία, προκειμένου να συμβάλουν σε ένα πιο ασφαλές πληροφοριακό σύστημα.

Επιπλέον, συνιστάται να ενημερώνονται όλοι οι υπάλληλοι σχετικά με τους στόχους επιμόρφωσης σχετικά με την ασφάλεια ετησίως, τουλάχιστον με συντομευμένη μέθοδο. Η ανανέωση της κατάρτισης θα πρέπει να επικαιροποιείται ώστε να αντικατοπτρίζει τις προόδους ή τις τροποποιήσεις κακόβουλων τεχνικών κι επιθέσεων και να ενισχύει την κατάρτιση ευαισθητοποίησης σχετικά με την ασφάλεια που έλαβαν αρχικά οι εργαζόμενοι. Οι στόχοι αυτής της επανακαθορισμένης κατάρτισης θα πρέπει να επαναπροσδιοριστούν και να αναθεωρηθούν χρησιμοποιώντας μια ποικιλία μέσων κατάρτισης.

Η συχνότητα εκπαίδευσης σχετικά με την ασφάλεια θα κρατήσει τους υπαλλήλους περισσότερο ικανούς να αναγνωρίζουν και να ανταποκρίνονται σε ζητήματα ασφάλειας ενώ παράλληλα θα τονίζεται ότι η συνειδητοποίηση της ασφάλειας αποτελεί προτεραιότητα για τον οργανισμό. [3]

Σύμφωνα με έρευνα που έγινε (Osterman Research Inc, 2018) η κατάρτιση σε ένα μεγάλο μέρος των οργανώσεων, εάν διεξάγεται, είναι σπάνια. Η εκπαίδευση χρηστών μία φορά το χρόνο ή μόνο όταν προσληφθούν στην εταιρεία δεν είναι επαρκής για να μεταφέρει τις πληροφορίες που χρειάζεται σχετικά με τα κρίσιμα ζητήματα ασφάλειας που έχουν σχεδιαστεί για να μεταβάλλουν τη συμπεριφορά των χρηστών. Επιπλέον, τα στοιχεία της έρευνας δείχνουν ότι υπάρχει μια σχέση μεταξύ της συχνότητας της κατάρτισης και της εμπιστοσύνης που δείχνουν οι επαγγελματίες στο χώρο της ασφάλειας στις ικανότητες των χρηστών τους. Όπως φαίνεται στην παρακάτω εικόνα, οι επαγγελματίες ασφαλείας σε οργανώσεις με σπάνια κατάρτιση ευαισθητοποίησης σχετικά με την ασφάλεια έχουν λιγότερη εμπιστοσύνη στις ικανότητες των χρηστών τους από ό, τι σε οργανισμούς με

συχνότερη κατάρτιση.



Εικόνα 2 – Σχέση συχνότητας εκπαίδευσης και εμπιστοσύνης στους χρήστες

3. Τύποι εκπαίδευσης

Η εκπαίδευση στην ευαισθητοποίηση σχετικά με την ασφάλεια μπορεί να πραγματοποιηθεί με διάφορους τρόπους, οι οποίοι μπορούν να χρησιμοποιηθούν μόνοι τους ή σε συνδυασμό μεταξύ τους. Αυτά τα μέσα μπορούν να συνίστανται σε μια τάξη, τη δημιουργία ενός ιστότοπου ευαισθητοποίησης σχετικά με την ασφάλεια, την προώθηση χρήσιμων συμβουλών στους υπολογιστές όταν ξεκινούν ή μέσω email σε εβδομαδιαία ή μηνιαία βάση καθώς κι η αξιοποίηση οπτικών βοηθημάτων όπως αφίσες.

3.1 Εκπαίδευση σε τάξη

Η χρήση αίθουσας διδασκαλίας για την εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας μπορεί να προσφέρει το πλεονέκτημα διαδραστικότητας μέσα στη μάθημα, καθώς και τη διαθεσιμότητα ερωταπαντήσεων σε πραγματικό χρόνο εγείροντας με αυτόν τον τρόπο το ενδιαφέρον των εργαζομένων,. Μπορεί επίσης να υπάρξει μια περίοδος ερωτηματολόγιου αξιολόγησης μετά την παρουσίαση καθώς και πληροφορίες επικοινωνίας που διανέμονται για ερωτήσεις που ενδέχεται να εμφανιστούν μετά.

Ορισμένες εταιρείες προσφέρουν κατάρτιση σε απευθείας σύνδεση και μέσω διαδικτύου και χρησιμοποιούν μια ποικιλία από μεθόδους όπως παιχνίδια ρόλων και προσομοίωσης, ώστε η αλληλεπίδραση να είναι πιο αμφίδρομη απ’ό,τι μονόδρομη. Άλλες εταιρείες προσφέρουν βίντεο, κατάρτιση μέσω διαδικτύου και ζωντανούς εκπαιδευτές.

Αυτός ο τύπος εκπαίδευσης μπορεί να διαφέρει ανάλογα με τον χρόνο που μπορεί να πάρει. Ο χρόνος εκπαίδευσης μπορεί να εξαρτάται από την αποτελεσματικότητα και την έκταση του υλικού που συζητήθηκε. Οι συνεδρίες κατάρτισης θα μπορούσαν ενδεχομένως να πάρουν μια ολόκληρη ημέρα εάν χρειαστεί.

3.2 Εκπαίδευση μέσω ιστοσελίδας

Ένας άλλος τρόπος υλοποίησης ενός προγράμματος ευαισθητοποίησης σχετικά με την ασφάλεια είναι η δημιουργία μιαw ιστοσελίδας ευαισθητοποίησης για την ασφάλεια Αυτός ο ιστότοπος μπορεί να αποτελείται από διαφορετικά τμήματα με διαφορετικές περιοχές ανάλογα με τα θέματα που πρέπει να καλύπτονται (π.χ. κακόβουλα προγράμματα, κοινή χρήση αρχείων, πνευματικά δικαιώματα, κ.λπ.).

Η εκπαίδευση αυτή είναι ένα πρόγραμμα κατάρτισης που οι μεμονωμένοι υπάλληλοι μπορούν να το ολοκληρώσουν με τον δικό τους ρυθμό και ανά πάσα στιγμή είναι

διαθέσιμη η πρόσβαση σε υπολογιστή συνδεδεμένο στο διαδίκτυο. Συνήθως παρέχει δραστηριότητες ή ολοκληρωμένες αξιολογήσεις μάθησης που προορίζονται για την ενίσχυση του περιεχομένου.

Μια άλλη εφαρμογή του δικτυακού τόπου ευαισθητοποίησης σχετικά με την ασφάλεια θα μπορούσε να είναι αυτοτροφοδοτούμενη, όπου οι χρήστες μπορούν να συνδεθούν και να ασχοληθούν με μίνι κουίζ στο τέλος του κάθε εκπαιδευτικού θέματος προκειμένου να βεβαιωθούν ότι το υλικό διαβάζεται κι απορροφάται. Η χρήση συνδέσεων μπορεί επίσης να είναι ένας τρόπος παρακολούθησης του ποιος έχει (και το σημαντικότερο ποιος δεν έχει) αφομοιώσει την εκπαίδευση. Θα μπορούσε επίσης να εφαρμοστεί ένα τμήμα Συχνών Ερωτήσεων καθώς και στοιχεία επικοινωνίας προκειμένου οι χρήστες να υποβάλλουν ερωτήσεις που δεν αναφέρονται στο τμήμα αυτό.

3.3 Βοηθητικές υποδείξεις

Η χρησιμοποίηση βοηθητικών υποδείξεων και χρήσιμων συμβουλών είναι περισσότερο συμπληρωματική στην εκπαίδευση, είτε μέσω αίθουσας διδασκαλίας ή μέσω ιστοσελίδας, και δεν πρέπει να χρησιμοποιείται ως μέσο ευαισθητοποίησης της ασφάλειας από μόνη της.

Οι βοηθητικές υποδείξεις μπορούν να αποτελούνται από συμβουλές και υπενθυμίσεις που ωθούνται στις οθόνες των χρηστών όταν αυτοί συνδέονται. Αυτές οι συμβουλές και υπενθυμίσεις μπορούν να συνίστανται σε βασικά σημεία που τονίζονται στην εκπαίδευση (π.χ. "Μην κρατάτε ποτέ τον κωδικό πρόσβασής σας σε μέρος που μπορεί να προσεγγιστεί ή να προβληθεί από οποιονδήποτε εκτός από τον εαυτό σας. "). Οι υπενθυμίσεις μπορούν να είναι τόσο απλές όσο το να υπενθυμίζουν σε κάποιον να αλλάξει τον κωδικό πρόσβασής του ή να εκτελέσει τη σάρωση ιών.

3.4 Οπτικά βοηθήματα

Τα οπτικά βοηθήματα είναι ένας άλλος τρόπος ευαισθητοποίησης που δεν πρέπει να χρησιμοποιείται ως μοναδική πηγή αλλά περισσότερο ως συμπλήρωμα. Το Πανεπιστήμιο του Michigan είχε δημιουργήσει στο παρελθόν μια σειρά πιασάρικων αφισών ασφάλειας κωδικών πρόσβασης που συγκρίνουν τους κωδικούς πρόσβασης με εσώρουχα. Κάποιος έλεγε ότι πρέπει να αλλάζουν συχνά, ένας άλλος έλεγε να μην αφήνουμε κωδικούς σε

μέρος που έχουν πρόσβαση μη εξουσιοδοτημένα άτομα, και ένας άλλος επισήμανε ότι δεν είναι σωστό να μοιράζονται με φίλους.

4. Εκπαιδευτικό κοινό

Όλοι οι υπάλληλοι θα πρέπει να εκπαιδεύονται και να ευαισθητοποιούνται σε θέματα που αφορούν την ασφάλεια πληροφοριακών συστημάτων. Οι οδηγίες προορίζονται να είναι χρήσιμες σε πολλά βασικά άτομα σε έναν οργανισμό, συμπεριλαμβανομένων, μεταξύ άλλων, του CIO, του διαχειριστή του προγράμματος ασφάλειας IT και του προσωπικού, των διαχειριστών (συμπεριλαμβανομένων των ιδιοκτητών συστημάτων και εφαρμογών) και των εξωτερικών συνεργατών τους, καθώς και των συντονιστών κατάρτισης. Η επιτυχία του προγράμματος ευαισθητοποίησης και κατάρτισης ενός οργανισμού, καθώς και του συνολικού προγράμματος ασφάλειας πληροφοριακών συστημάτων, εξαρτάται από την ικανότητα αυτών των ανθρώπων να εργαστούν για έναν κοινό στόχο προστασίας των πληροφοριών του οργανισμού και των πόρων που σχετίζονται με την τεχνολογία. Γενικότερα, σε ένα πρόγραμμα εκπαίδευσης όλοι οι συμβασιούχοι υπάλληλοι που εμπίπτουν σε οποιαδήποτε από τις ακόλουθες κατηγορίες θα πρέπει να εκπαιδεύονται:

- όσοι διατηρούν μια τακτική παρουσία στον οργανισμό, ενεργώντας σε μόνιμη θέση σε συνεχή χρονική περίοδο και πραγματοποιούν περισσότερες από παρεπόμενες δραστηριότητες

- εκείνους που το έργο και τα καθήκοντα απαιτεί πλήρη απασχόληση

- όσοι εργάζονται σε συνεργεία κατασκευών ή προσωπικό καθαρισμού

- όσοι εργάζονται με ευαίσθητες πληροφορίες ασφαλείας

- άλλες θέσεις που κρίνονται κατάλληλες να υποβληθούν σε εκπαίδευση για την ευαισθητοποίηση σχετικά με την ασφάλεια

4.1 Ρόλοι και ευθύνες

Ενώ είναι σημαντικό να κατανοήσουμε τις πολιτικές που απαιτούν οι οργανισμοί για να αναπτύξουν και να εφαρμόσουν την ευαισθητοποίηση και την εκπαίδευση, είναι εξίσου σημαντικό οι οργανισμοί να κατανοήσουν ποιος έχει την ευθύνη για την ενημέρωση και την εκπαίδευση στον τομέα της ασφάλειας. Παρακάτω γίνεται μια προσπάθεια εντοπισμού και περιγραφής αυτών.

Ορισμένες οργανώσεις διαθέτουν ένα ώριμο πρόγραμμα ασφάλειας, ενώ άλλες

οργανώσεις μπορεί να αγωνίζονται για την επίτευξη βασικού προσωπικού, χρηματοδότησης κι υποστήριξης. Η μορφή που λαμβάνει ένα πρόγραμμα ευαισθητοποίησης και κατάρτισης μπορεί να ποικίλλει σε μεγάλο βαθμό από εταιρεία σε εταιρεία. Αυτό οφείλεται, εν μέρει, στην ωριμότητα αυτού του προγράμματος. Ένας τρόπος για να εξασφαλιστεί η ωριμότητα κι η επιτυχία ενός προγράμματος είναι η ανάπτυξη και τεκμηρίωση των ευθυνών για την ευαισθητοποίηση και την κατάρτιση στον τομέα της ασφάλειας.

4.1.1 Επικεφαλής του οργανισμού

Οι επικεφαλής των οργανισμών πρέπει να διασφαλίζουν ότι δίδεται υψηλή προτεραιότητα στην αποτελεσματική ενημέρωση και κατάρτιση στον τομέα της ασφάλειας για το εργατικό δυναμικό. Αυτό περιλαμβάνει την εφαρμογή ενός βιώσιμου προγράμματος ασφάλειας με ισχυρό περιεχόμενο ευαισθητοποίησης και εκπαίδευσης. Οι επικεφαλής των οργανισμών πρέπει να:

- Ορίσουν έναν CIO.

- Αναθέσουν την ευθύνη όσον αφορά την ασφάλεια.

- Βεβαιωθούν ότι υλοποιείται ένα ευρύ πρόγραμμα ασφάλειας για υπηρεσίες πληροφορικής, ότι υποστηρίζεται καλά από πόρους και προϋπολογισμό κι ότι είναι αποτελεσματικό.

- Βεβαιωθούν ότι ο οργανισμός διαθέτει επαρκώς εκπαιδευμένο προσωπικό για να προστατεύσει τους πόρους του.

4.1.2 Διευθυντές Πληροφοριών

Οι Διευθυντές Πληροφοριών (CIO) θα πρέπει να διαχειρίζονται την εκπαίδευση και να επιβλέπουν το προσωπικό με σημαντικές ευθύνες για την ασφάλεια των πληροφοριών. Οι Διευθυντές Πληροφοριών θα πρέπει να συνεργαστούν με τον διαχειριστή του Προγράμματος Ασφαλείας Πληροφοριών για:

- Την καθιέρωση γενικής στρατηγικής για το πρόγραμμα πληροφόρησης και κατάρτισης στον τομέα της πληροφορικής.

- Να εξασφαλίζουν ότι ο επικεφαλής του γραφείου, τα ανώτερα διευθυντικά στελέχη, οι ιδιοκτήτες συστημάτων και δεδομένων κι άλλοι κατανοούν τις έννοιες και τη στρατηγική του προγράμματος ενημέρωσης και κατάρτισης στον τομέα της ασφάλειας και ενημερώνονται για την πρόοδο της εφαρμογής του προγράμματος.

- Να βεβαιωθούν ότι χρηματοδοτείται το πρόγραμμα ευαισθητοποίησης και κατάρτισης του οργανισμού στον τομέα της πληροφορικής.

- Να εξασφαλίσουν ότι η κατάρτιση του προσωπικού του γραφείου εφαρμόζεται με σημαντικές ευθύνες που αφορούν την ασφάλεια.

- Να εξασφαλίσουν ότι όλοι οι χρήστες είναι επαρκώς καταρτισμένοι για τις αρμοδιότητές τους στον τομέα της ασφάλειας.

- Να βεβαιωθούν ότι υπάρχουν αποτελεσματικοί μηχανισμοί παρακολούθησης κι αναφοράς.

4.1.3 Διαχειριστές Προγράμματος Ασφάλειας Πληροφοριών

Ο υπεύθυνος του προγράμματος ασφάλειας πληροφορικής έχει ευθύνη τακτικού επιπέδου για το πρόγραμμα ευαισθητοποίησης και κατάρτισης. Στον ρόλο αυτό, ο διαχειριστής του προγράμματος πρέπει να:

- Διασφαλίσει ότι το υλικό ευαισθητοποίησης και κατάρτισης που αναπτύσσεται είναι κατάλληλο και έγκαιρο για το συγκεκριμένο κοινό.

- Βεβαιωθεί ότι το υλικό ευαισθητοποίησης και κατάρτισης έχει αναπτυχθεί αποτελεσματικά για να φτάσει στο επιθυμητό κοινό.

- Διασφαλίσει ότι οι χρήστες και οι διαχειριστές έχουν έναν αποτελεσματικό τρόπο παροχής συμβουλών σχετικά με το υλικό ευαισθητοποίησης και κατάρτισης και την παρουσίασή του.

- Διασφαλίσει ότι τα ενημερωτικά κι εκπαιδευτικά υλικά επανεξετάζονται περιοδικά και ενημερώνονται όταν είναι απαραίτητο.

- Βοηθήσει στη δημιουργία στρατηγικής παρακολούθησης κι αναφοράς.

4.1.4 Επικεφαλής

Οι επικεφαλής (managers) είναι υπεύθυνοι για τη συμμόρφωση με τις απαιτήσεις πληροφόρησης και εκπαίδευσης, σχετικά με την ασφάλεια, που έχουν τεθεί για τους χρήστες τους. Οι επικεφαλής θα πρέπει να:

- Συνεργαστούν με τον διαχειριστή του CIO και του προγράμματος ασφάλειας για να καλύψουν τις κοινές ευθύνες.

- Υπηρετούν το ρόλο του ιδιοκτήτη του συστήματος και / ή του ιδιοκτήτη των δεδομένων, ανάλογα με την περίπτωση.

- Εξετάσουν την ανάπτυξη ατομικών αναπτυξιακών σχεδίων για τους χρήστες σε ρόλους με σημαντικές ευθύνες για την ασφάλεια.

- Προωθήσουν την επαγγελματική ανάπτυξη και πιστοποίηση του προσωπικού του προγράμματος ασφάλειας, των υπαλλήλων ασφαλείας πλήρους ή μερικής απασχόλησης και άλλων με σημαντικές αρμοδιότητες στον τομέα της ασφάλειας.

- Βεβαιωθούν ότι όλοι οι χρήστες (συμπεριλαμβανομένων των εξωτερικών συνεργατών) των συστημάτων τους (δηλ. Συστήματα γενικής υποστήριξης και σημαντικές εφαρμογές) έχουν καταρτιστεί κατάλληλα για να εκπληρώσουν τις ευθύνες τους όσον αφορά την ασφάλεια πριν τους επιτρέψουν την πρόσβαση.

- Βεβαιωθούν ότι οι χρήστες (συμπεριλαμβανομένων των εξωτερικών συνεργατών) κατανοούν συγκεκριμένους κανόνες για κάθε σύστημα και εφαρμογή που χρησιμοποιούν.

- Εργαστούν για να μειώσουν τα λάθη και τις παραλείψεις των χρηστών λόγω έλλειψης ενημέρωσης ή / και κατάρτισης.

4.1.5 Χρήστες

Οι χρήστες είναι το μεγαλύτερο ακροατήριο σε κάθε οργανισμό και είναι η πιο σημαντική ομάδα ανθρώπων που μπορούν να βοηθήσουν στη μείωση των σφαλμάτων και των ευπαθειών. Οι χρήστες μπορούν να είναι υπάλληλοι, ξένοι ή εγχώριοι ερευνητές, συνεργάτες, επισκέπτες κι άλλοι οι οποίοι χρειάζονται πρόσβαση. Οι χρήστες πρέπει να:

- Δείξουν κατανόηση και συμμόρφωση με τις πολιτικές και τις διαδικασίες ασφαλείας της υπηρεσίας.

- Εκπαιδεύονται κατάλληλα στους κανόνες συμπεριφοράς για τα συστήματα και τις εφαρμογές στις οποίες έχουν πρόσβαση.

- Δουλεύουν με τη διοίκηση για την κάλυψη των αναγκών κατάρτισης.

- Διατηρήσουν το λογισμικό / τις εφαρμογές ενημερωμένες.

- Είναι ενήμεροι για τις ενέργειες που μπορούν να αναλάβουν για την καλύτερη προστασία των πληροφοριών της υπηρεσίας τους. Αυτές οι ενέργειες περιλαμβάνουν (αλλά δεν περιορίζονται σε αυτές): σωστή χρήση κωδικού πρόσβασης, δημιουργία αντιγράφων ασφαλείας δεδομένων, κατάλληλη προστασία από ιούς, αναφορά τυχόν ύποπτων περιστατικών ή παραβιάσεων πολιτικής ασφαλείας και να ακολουθούν τους κανόνες που θεσπίστηκαν για την αποφυγή επιθέσεων κοινωνικής μηχανικής και κανόνων αποτροπής της εξάπλωσης spam ή ιών. [4]

5. Θέματα εκπαίδευσης

Τα θέματα που εξετάζονται για την ευαισθητοποίηση σχετικά με την ασφάλεια πρέπει να συνίστανται σε συνδυασμό με τις υπάρχουσες οργανωτικές πολιτικές και διαδικασίες (πώς συνδέονται με κάθε πτυχή, αν το κάνουν), την φυσική ασφάλεια, την ασφάλεια υπολογιστών, την ασφάλεια κωδικών πρόσβασης, το ηλεκτρονικό "ψάρεμα" (phishing), την κοινωνική μηχανική (social engineering), τις φάρσες, τα κακόβουλα προγράμματα (π.χ. ιούς, worms, trojans, spyware) καθώς και τα πνευματικά δικαιώματα όσον αφορά την κοινή χρήση αρχείων.

Αυτά τα θέματα θα βοηθήσουν τους υπαλλήλους να κατανοήσουν γιατί η συνειδητοποίηση της ασφάλειας είναι σημαντική και να τους οδηγήσουν να γνωρίζουν πώς να αποτρέπουν τυχόν συμβάντα και τι πρέπει να κάνουν αν συμβεί κάτι τέτοιο.

5.1 Φυσική προστασία

Όταν αντιμετωπίζει κανείς τη φυσική ασφάλεια, το κλείδωμα των πορτών και των συρταριών γραφείου / αρχειοθήκης θα πρέπει να είναι η κύρια εστίαση στην εκπαίδευση. Ένα άλλο στοιχείο που αγγίζει ελαφρά (αλλά για περισσότερες λεπτομέρειες ανατρέξτε στην Ασφάλεια υπολογιστών γραφείου) είναι το γεγονός ότι εάν ένας δυνητικός εισβολέας έχει πρόσβαση σε ένα υπολογιστή του χρήστη, θα μπορούσε να εγκαταστήσει έναν καταγραφέα κλειδιών ή να μπει σε ένα μηχάνημα που δεν έχει κλειδωθεί.

Συνοπτικά όσον αφορά τη φυσική ασφάλεια σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- το κλείδωμα των πορτών και των συρταριών γραφείου / αρχειοθήκης
- η συνοδεία επισκεπτών μέσα στον εργασιακό χώρο

5.2 Ασφάλεια υπολογιστών γραφείου

Η ενότητα ασφάλειας υπολογιστών γραφείου είναι ιδιαίτερα σημαντική και θα πρέπει να εξεταστεί λεπτομερώς. Η λήψη μέτρων για την ασφάλεια των υπολογιστών θα συμβεί αν οι χρήστες κατανοήσουν τη σημαντικότητα τους. Παρακάτω περιγράφονται τρόποι προστασίας των υπολογιστών γραφείου οι οποίοι θα πρέπει να περιλαμβάνονται σε ένα πρόγραμμα ευαισθητοποίησης εργαζομένων σε θέματα ασφάλειας.

Οι εργαζόμενοι επιβάλλεται να έχουν προστασία με κωδικό πρόσβασης στην προφύλαξη οθόνης ή, ακόμα καλύτερα, να έχουν τη συνήθεια κλειδώματος των υπολογιστών όταν απομακρύνονται από αυτές. Θα πρέπει να χρησιμοποιηθεί ένα χρονικό όριο προστασίας οθόνης, οπότε αν κάποιος χρήστης απομακρυνθεί από τον υπολογιστή του, η προφύλαξη οθόνης που προστατεύεται με κωδικό πρόσβασης να έρθει σε λειτουργία. Συνήθως 5 με 10 λεπτά είναι ένας αποδεκτό χρονικό όριο. Οι πληροφορίες για το πώς κανείς μπορεί να ρυθμίσει τα παραπάνω αλλάζουν ανάλογα με το εκάστοτε λειτουργικό σύστημα. Δεδομένου αυτού, ένα εγχειρίδιο που θα μοιράζεται σε κάθε εργαζόμενο με αναλυτικά τα βήματα εφαρμογής της ρύθμισης θα ήταν μια καλή λύση.

Οι τακτικές που θα μπορούσε να χρησιμοποιήσει κάποιος δυνητικός εισβολέας πρέπει επίσης να αντιμετωπιστούν. Για παράδειγμα μία μέθοδος που χρησιμοποιείται για την επίθεση σε επιτραπέζιους υπολογιστές είναι το shoulder surfing. Αυτό συμβαίνει όταν ένα απαρατήρητο άτομο παρακολουθεί πάνω από τον ώμο σας για να αποκτήσει ιδιωτικές πληροφορίες όπως το όνομα χρήστη και τον κωδικό πρόσβασής σας. Ο καλύτερος τρόπος για να το αποφύγετε είναι να τοποθετήσετε τον υπολογιστή σας έτσι ώστε να μπορείτε να δείτε όλα τα άτομα που θα μπορούσαν να δουν το πληκτρολόγιο ή την οθόνη του υπολογιστή σας. Αν δεν μπορείτε να μετακινήσετε τον υπολογιστή, τοποθετήστε μικρούς καθρέφτες στην οθόνη, ώστε να μπορείτε να δείτε οποιοδήποτε άτομο μπορεί να δει την οθόνη σας.

Μια άλλη μέθοδος hacking είναι η λήψη αρχείων που μεταφέρονται με τρόπο ανασφαλές. Τα αρχεία που μεταφέρονται μέσω FTP ή TELNET στέλνονται σε απλό κείμενο κι όχι κρυπτογραφημένα. Αυτό σημαίνει ότι όλη η επικοινωνία μπορεί να διαβαστεί σε καθαρά αγγλικά, συμπεριλαμβανομένου του αναγνωριστικού χρήστη, του κωδικού πρόσβασης και άλλων προσωπικών πληροφοριών. Η καλύτερη άμυνα εναντίον αυτής της μορφής hacking είναι η χρήση ασφαλών εφαρμογών μεταφοράς αρχείων, όπως το SSH και το PGP. Αυτές οι εφαρμογές παρέχουν κρυπτογράφηση για μεταφορά αρχείων και μηνύματα ηλεκτρονικού ταχυδρομείου.

Εξίσου σημαντικό στοιχείο που θα μπορούσε να αντιμετωπιστεί είναι να διασφαλίσει ότι οι χρήστες καταλαβαίνουν ότι είναι σημαντικό να κλείσουν τους υπολογιστές τους στο τέλος της ημέρας. Μερικές φορές αυτό επιτρέπει την εφαρμογή πολύτιμων ενημερώσεων, ενώ αν κάποιος δυνητικός εισβολέας αποκτήσει πρόσβαση σε έναν υπολογιστή που είναι

απενεργοποιημένος, θα είναι λιγότερο πιθανό να τον χρησιμοποιήσει από εκείνον που είναι ήδη ενεργοποιημένος κι ακλείδωτος. [5]

Συνοπτικά όσον αφορά την ασφάλεια υπολογιστών γραφείου σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- η προστασία στην προφύλαξη οθόνης με κωδικό πρόσβασης
- η συνήθεια κλειδώματος των υπολογιστών όταν απομακρύνονται από αυτές
- το χρονικό όριο προστασίας οθόνης, ώστε αν κάποιος χρήστης απομακρυνθεί από τον υπολογιστή του, η προφύλαξη οθόνης που προστατεύεται με κωδικό πρόσβασης να έρθει σε λειτουργία
- η θέση υπολογιστή, προκειμένου να μην μπορεί να παρακολουθηθεί εύκολα από τρίτους
- η χρήση ασφαλών εφαρμογών μεταφοράς αρχείων, όπως το SSH και το PGP
- το κλείσιμο υπολογιστή στο τέλος της ημέρας

5.3 Ασφάλεια ασύρματων δικτύων

Τα τμήματα ασύρματων δικτύων και ασφάλειας πρέπει να αντιμετωπίζουν τον μη ασφαλή χαρακτήρα των ασύρματων δικτύων, καθώς και να δίνουν συμβουλές και κόλπα στους εργαζομένους για να επιδείξουν προσοχή και να κάνουν τους φορητούς υπολογιστές ασφαλέστερους ενάντια στους κινδύνους που προκαλεί το «sniffing.» Θα πρέπει επίσης να δοθεί έμφαση στη μη αποθήκευση ευαίσθητων πληροφοριών σε φορητούς υπολογιστές που θα έχουν πρόσβαση σε ασύρματο δίκτυο.

Ένας άλλος τομέας που πρέπει να καλυφθεί είναι η σημασία των τειχών προστασίας, γνωστά κι ως Firewalls. Τις περισσότερες φορές οι εταιρείες θα παράσχουν ένα τείχος προστασίας που αγοράστηκε σε φορητούς υπολογιστές και υπολογιστές που παρέχονται από την εταιρεία (π.χ. Sophos, McAfee, Norton κ.λπ.), αλλά οι προσωπικοί φορητοί υπολογιστές που χρησιμοποιούν το ασύρματο δίκτυο της εταιρείας θα πρέπει να διαθέτουν κι αυτοί τείχος προστασίας. Για μικρά περιβάλλοντα γραφείου καθώς και για άτομα που έχουν πρόσβαση από το σπίτι, είναι πάντα χρήσιμο να παρέχονται πληροφορίες σχετικά με ελεύθερα τείχη προστασίας, καθώς και σχετικά φθηνές επιλογές τείχους προστασίας. Τα ελεύθερα τείχη προστασίας είναι περισσότερο για τον προσωπικό χρήστη και όχι για εμπορική χρήση. Μπορεί επίσης να είναι όφελος για την εκπαίδευση η σύγκριση της τιμής

ενός τείχου προστασίας με την τιμή μιας παραβίασης. Μια παραβίαση δεν θα κοστίσει μόνο στην εταιρεία τεράστια χρηματικά ποσά, θα μπορούσε επίσης να προκαλέσει την απόλυση του χρήστη. Συνεπώς, είναι επιτακτικής σημασίας οι εργαζόμενοι να διαθέτουν ενεργοποιημένο κι ενημερωμένο τείχος προστασίας στους υπολογιστές που χρησιμοποιούν.

Συνοπτικά όσον αφορά την ασφάλεια ασύρματων δικτύων σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- η μη αποθήκευση ή η κρυπτογράφηση ευαίσθητων πληροφοριών σε φορητούς υπολογιστές που θα έχουν πρόσβαση σε ασύρματο δίκτυο
- η σημασία των τειχών προστασίας, γνωστά κι ως Firewalls κι η σύγκριση της τιμής ενός τείχου προστασίας με την τιμή μιας παραβίασης

5.4 Ασφάλεια κωδικών πρόσβασης

Η εκπαίδευση που αφορά ασφάλεια κωδικών πρόσβασης πρέπει να περιλαμβάνει το τί μετατρέπει έναν κωδικό σε ισχυρό και ασφαλές. Κωδικοί άνω των 8 χαρακτήρων που περιλαμβάνουν αλφαριθμητικά, κεφαλαία και ειδικούς χαρακτήρες θεωρούνται συνήθως αρκετά δυνατοί και δύσκολα σπάνε. Οι ελάχιστες απαιτήσεις κωδικού πρόσβασης του οργανισμού θα πρέπει να περιλαμβάνουν τα παραπάνω και να γνωστοποιούνται στους εργαζομένους.

Η κοινή χρήση κωδικών πρόσβασης καθώς κι η εμφάνισή τους σε εμφανές σημείο προσβάσιμο από τον οποιονδήποτε, π.χ. σε χαρτάκι κολλημένο στην οθόνη του υπολογιστή, θα πρέπει να αποθαρρύνεται έντονα. Η πολιτική της οργάνωσης θα μπορούσε να είναι πολύ χρήσιμη σε αυτόν τον τομέα. Εάν αυτό ενσωματωθεί στην πολιτική, πρέπει να αντιμετωπιστεί και στην εκπαίδευση. Οι χρήστες πρέπει να γνωρίζουν ότι υπάρχει μια πολιτική και γενικά "Βασικοί κανόνες" οι οποίες ακολουθούνται από αυτή την πολιτική. Οι στατιστικές θα μπορούσαν επίσης να είναι ένα καλό συμπλήρωμα. Για παράδειγμα, ένα εξουσιοδοτημένο άτομο θα μπορούσε να μεταβεί σε όλα τα γραφεία και να δει αν μπορεί να αποκαλύψει τυχόν μη ασφαλείς κωδικούς πρόσβασης. Θα μπορούσαν ακόμη και να πάει αυτό το βήμα παραπέρα και να δει πόσοι υπολογιστές έχουν απομείνει χωρίς προστασία με κωδικό οθόνης. Η παρουσίαση του αριθμού των συμβάντων μη

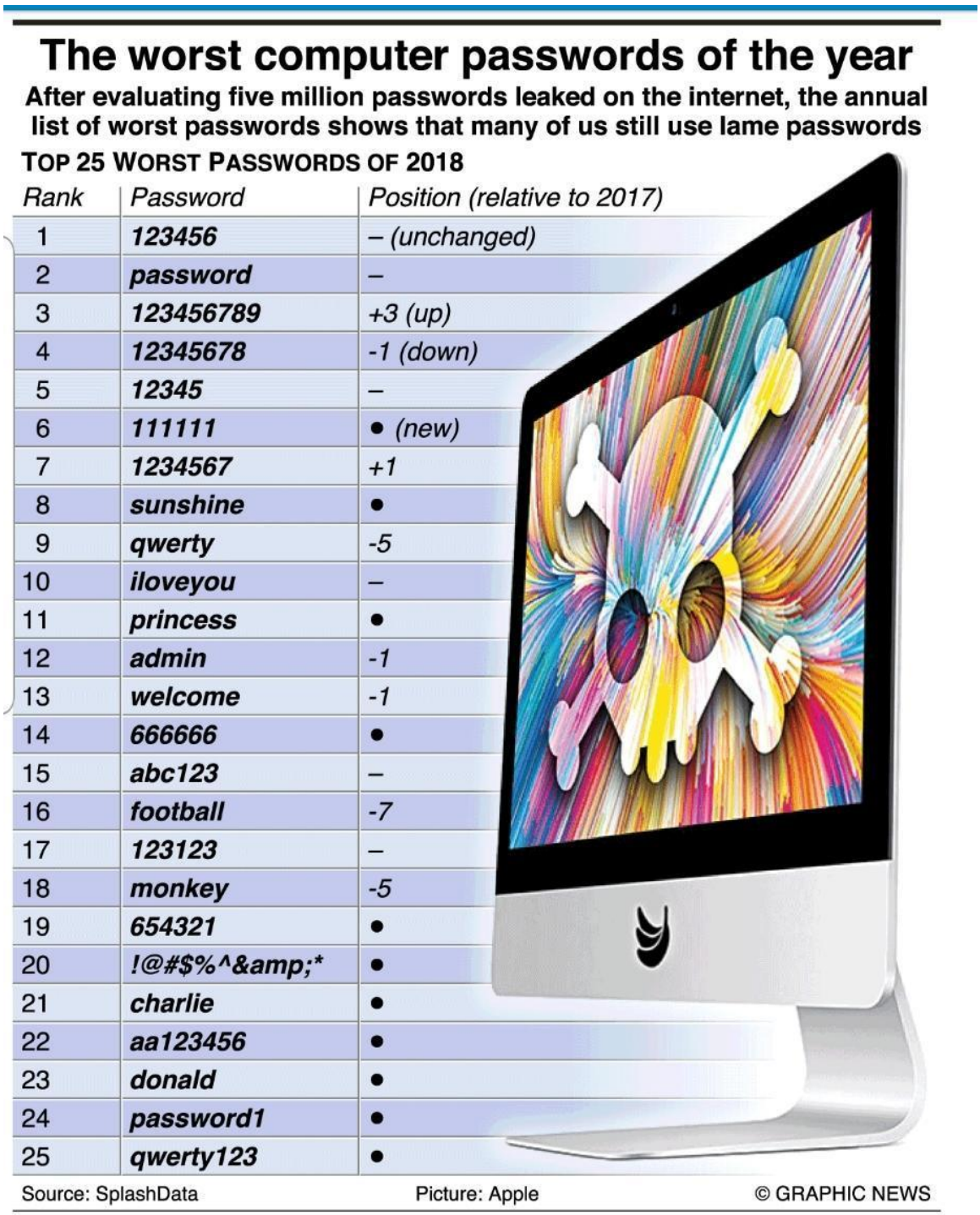
συμμόρφωσης σε σχέση με το σύνολο των υπολογιστών θα ήταν αρκετό.

Οι χρήσιμες συμβουλές και οι καλοί κανόνες θα πρέπει επίσης να αποτελούν μέρος αυτής της ενότητας. Για παράδειγμα, οι κωδικοί πρόσβασης δεν πρέπει να περιέχουν το όνομα χρήστη ή οποιοδήποτε τμήμα του πλήρους ονόματος του χρήστη. Οι κωδικοί πρόσβασης δεν πρέπει επίσης να βασίζονται σε προσωπικές πληροφορίες, όπως όνομα συζύγου, αγαπημένη ομάδα ή κατοικίδιο ζώο. Ένα άλλο σημαντικό σημείο είναι να τονίσουμε ότι ο προεπιλεγμένος κωδικός πρόσβασης που δίνεται στους χρήστες θα πρέπει να αλλάζει αμέσως. Θα πρέπει επίσης να συμπεριληφθούν οδηγίες σχετικά με τον τρόπο αλλαγής κωδικών πρόσβασης.

Για την ολοκλήρωση της ενότητας ασφάλειας κωδικών πρόσβασης, μπορεί να είναι πολύ ωφέλιμο να καθορίσετε τι αποτελεί μια κακή επιλογή του κωδικού πρόσβασης καθώς και μια λίστα των πιο συνηθισμένων κωδικών που χρησιμοποιούνται κι άρα θα πρέπει να αποφεύγονται.

Συνοπτικά όσον αφορά την ασφάλεια κωδικών πρόσβασης σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- οι χρήσιμες συμβουλές και οι καλοί κανόνες για το τί μετατρέπει έναν κωδικό σε ισχυρό και ασφαλές
- η αποφυγή της κοινής χρήσης κωδικών πρόσβασης καθώς κι η εμφάνισή τους σε εμφανές σημείο προσβάσιμο από τον οποιονδήποτε
- η λίστα των πιο συνηθισμένων κωδικών που χρησιμοποιούνται κι άρα θα πρέπει να αποφεύγονται



The worst computer passwords of the year

After evaluating five million passwords leaked on the internet, the annual list of worst passwords shows that many of us still use lame passwords

TOP 25 WORST PASSWORDS OF 2018

Rank	Password	Position (relative to 2017)
1	123456	– (unchanged)
2	password	–
3	123456789	+3 (up)
4	12345678	-1 (down)
5	12345	–
6	111111	• (new)
7	1234567	+1
8	sunshine	•
9	qwerty	-5
10	iloveyou	–
11	princess	•
12	admin	-1
13	welcome	-1
14	666666	•
15	abc123	–
16	football	-7
17	123123	–
18	monkey	-5
19	654321	•
20	!@#$%^&*	•
21	charlie	•
22	aa123456	•
23	donald	•
24	password1	•
25	qwerty123	•

Source: SplashData Picture: Apple © GRAPHIC NEWS

Εικόνα 3 - Λίστα από τους πιο συνηθισμένους κωδικούς το 2018

5.5 Κοινωνική μηχανική (Social engineering)

Για να καταλάβουμε πως μπορούμε να προστατευτούμε από μια επίθεση κοινωνικής μηχανικής θα πρέπει πρώτα να καταλάβουμε το πως δρα η κοινωνική μηχανική. Μια

επιτυχημένη επίθεση από κοινωνικό μηχανικό βασίζεται στους υπαλλήλους μίας επιχείρησης. Οπότε για να περιοριστεί μια τέτοιου είδους επίθεση, οι εργαζόμενοι θα πρέπει να εκπαιδευτούνε και να ενημερωθούνε για τις πιο συχνές τεχνικές κοινωνικής μηχανικής. Επίσης είναι σημαντικό για έναν οργανισμό να καθιερωθεί μια σαφής και ισχυρή πολιτική ασφαλείας, συμπεριλαμβανομένων των προτύπων ασφαλείας και των διαφόρων μεθόδων και διαδικασιών τα οποία θα βοηθήσουν στην εξάλειψη της απειλής της κοινωνικής μηχανικής. [6]

Ένα πετυχημένο πρόγραμμα εκπαίδευσης ενάντια στην κοινωνική μηχανική μπορεί να περιλαμβάνει τα εξής στοιχεία:

- *Δώστε ένα καλό όνομα εκπαίδευσης:*

Αυτό μπορεί να ακούγεται ασήμαντο, αλλά ένα "πιασάρικο" όνομα κρατά τα προγράμματα κατάρτισης και τα μαθήματά τους στο μυαλό των χρηστών.

- *Βάλτε τους χρήστες στην άλλη πλευρά της επίθεσης*

Διδάξτε τους την βασική κοινωνική μηχανική. Δεν υπάρχει καλύτερος τρόπος κατανόησης του τρόπου με τον οποίο λειτουργεί η κοινωνική μηχανική παρά να διδάσκει πώς να το κάνει. Με την τοποθέτηση των υπαλλήλων στο ρόλο του επιτιθέμενου, μπορούν να κατανοήσουν πώς να εντοπίσουν μια επίθεση καθώς και ότι όλα τα δεδομένα είναι πολύτιμα για έναν κοινωνικό μηχανικό κι όχι μόνο αυτά που κανονικά θα θεωρούνταν «ευαίσθητα».

- *Μην ξεχνάτε την αξία του "όχι".*

Μια πολύ αποτελεσματική τακτική που χρησιμοποιούν οι κοινωνικοί μηχανικοί είναι οι απειλές που αποκαλύπτουν ότι αν ο στόχος δεν κάνει αυτό που τους ζητείται, το αφεντικό τους θα ακούσει γι 'αυτό και θα είναι θυμωμένος. Αυτό μπορεί να αντιμετωπιστεί με το να γνωρίζουν οι εργαζόμενοι (και οι διευθυντές) ότι δεν θα υπάρξει ποτέ ποινή στο να λένε "όχι" και να επαληθεύσουν όποιον είναι υπεύθυνος. Οι τηλεφωνικές κλήσεις / επιστροφές αλληλογραφίας (μέσω των πληροφοριών στα βιβλία διευθύνσεων της εταιρείας) πρέπει να αποτελούν μέρος της διαδικασίας της εταιρείας.

Μέρος ενός καλού προγράμματος κατάρτισης στον τομέα της κοινωνικής μηχανικής είναι η «κοινωνική» δοκιμή διείσδυσης, δηλαδή αν κάποιος διαδραματίσει το ρόλο ενός εισβολέα και προσπαθήσει να εφαρμόσει κοινωνική μηχανική. Ωστόσο, ορισμένες

οργανώσεις προσπαθούν να μειώσουν το κόστος και να βασίζονται αποκλειστικά σε αυτοματοποιημένες δοκιμές. Αυτό μπορεί να είναι πρόβλημα επειδή προφανώς οι "ψεύτικες" δοκιμές θα ενοχλήσουν τους υπαλλήλους και θα τους κάνουν πιο ευάλωτους σε πραγματικές επιθέσεις. Οι οργανισμοί πρέπει να διασφαλίζουν ότι οι δοκιμές που πραγματοποιούνται είναι όσο το δυνατόν πιο ρεαλιστικές, ώστε να μετρήσουν ρεαλιστικά και με ακρίβεια την ικανότητα των υπαλλήλων να αντιστέκονται στην κοινωνική μηχανική.

Τόσο η δοκιμή όσο και η κατάρτιση πρέπει να είναι μια συνεχής και ατέρμονη διαδικασία. Οι επιθέσεις κοινωνικής μηχανικής, όπως και με όλες τις επιθέσεις, γίνονται ισχυρότερες με την πάροδο του χρόνου. Οι εργαζόμενοι συμμετέχουν και εγκαταλείπουν την εταιρεία ή αλλάζουν τους ρόλους τους. Ένα πραγματικά αποτελεσματικό εκπαιδευτικό πρόγραμμα πρέπει να τα έχει όλα αυτά υπόψη, προκειμένου να προστατεύσει έναν οργανισμό. [7]

Συνοπτικά όσον αφορά την κοινωνική μηχανική σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- η ενημέρωση για τις πιο συχνές τεχνικές κοινωνικής μηχανικής
- η σημαντικότητα συμμόρφωσης με πολιτική ασφαλείας, στην οποία προτείνονται πρότυπα ασφαλείας και διάφοροι μέθοδοι και διαδικασίες οι οποίες θα βοηθήσουν στην εξάλειψη της απειλής της κοινωνικής μηχανικής

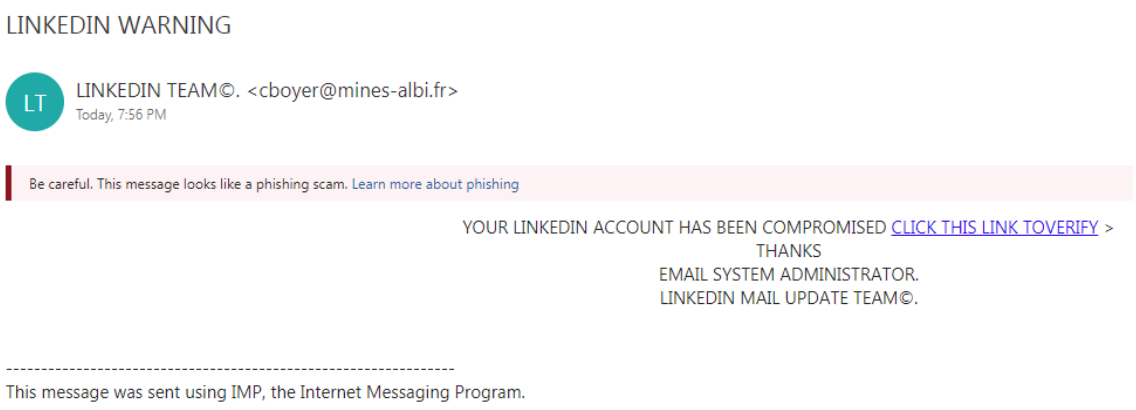
5.6 Ηλεκτρονικό ψάρεμα (Phishing)

Το phishing είναι μια πολυεπίπεδη πράξη εξαπάτησης με χρήση ηλεκτρονικού ταχυδρομείου, όπου μέσω πλαστοπροσωπίας αποσπώνται πληροφορίες από ένα συγκεκριμένο στόχο. Ιδιαίτερη προσοχή πρέπει να δοθεί στο spear phishing το οποίο αποτελεί ιδιαίτερο τύπο phishing, κατά τον οποίο ο στόχος και το περιεχόμενο διερευνώνται, έτσι ώστε το email να είναι προσαρμοσμένο στον δέκτη.

Όταν συζητάμε για το ηλεκτρονικό "ψάρεμα" (phishing), ο όρος και ο σκοπός θα πρέπει να καθορίζονται πάντα. Τα παραδείγματα αποτελούν το κλειδί για αυτή την εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια. Πράγματα που πρέπει να αποφευχθούν (π.χ. κάνοντας κλικ σε συνδέσμους που παρέχονται μέσω ηλεκτρονικού ταχυδρομείου, υποβάλλοντας τραπεζικές πληροφορίες και πληροφορίες κωδικού πρόσβασης μέσω email, κ.λπ.) θα πρέπει να επισημανθούν έτσι ώστε οι άνθρωποι να γνωρίζουν τι πρέπει να

αναζητήσουν. Επιπλέον, σύμφωνα με μελέτες η επιτυχία του phishing επηρεάζεται από παράγοντες λήψης αποφάσεων όπως είναι η πείνα, το άγχος, η έλλειψη ύπνου καθώς και εξωτερικοί παράγοντες όπως η θερμοκρασία και το φως. [8]

Ένα άλλο στοιχείο που πρέπει να αντιμετωπιστεί είναι πώς να αντιμετωπίσετε πραγματικά τις επιθέσεις ηλεκτρονικού "ψαρέματος". Μερικές ιστοσελίδες ενθαρρύνουν την αναφορά και την παρακολούθηση ιστοτόπων και μηνυμάτων ηλεκτρονικού ταχυδρομείου όπου γίνεται προσπάθεια για ηλεκτρονικό ψάρεμα. Θα μπορούσε επίσης να είναι χρήσιμο οι χρήστες να δοκιμάσουν κάποιο IQ Phishing test από αυτά που υπάρχουν διαθέσιμα στο διαδίκτυο.



Εικόνα 4 - Στιγμιότυπο προσπάθεας ηλεκτρονικού ψαρέματος

Συνοπτικά όσον αφορά το ηλεκτρονικό ψάρεμα σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- παραδείγματα ηλεκτρονικού ψαρέματος, τα οποία αποτελούν το κλειδί για αυτή την εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια
- τα πράγματα που πρέπει να αποφευχθούν (π.χ. κάνοντας κλικ σε συνδέσμους που παρέχονται μέσω ηλεκτρονικού ταχυδρομείου, υποβάλλοντας τραπεζικές πληροφορίες και πληροφορίες κωδικού πρόσβασης μέσω email, κ.λπ.)
- ο έλεγχος της ηλεκτρονικής διεύθυνσης του αποστολέα

5.7 Φάρσες

Οι φάρσες θα πρέπει να αντιμετωπιστούν στην εκπαίδευση, διότι μπορεί να χρειαστεί πολύς χρόνος και πόροι στην ανάγνωση και τη προώθηση μηνυμάτων ηλεκτρονικού ταχυδρομείου. Οι τύποι των φαρσών καθώς και παραδείγματά τους θα πρέπει να είναι το κύριο περιεχόμενο στην εκπαίδευση. Η συζήτηση γνωστών φαρσών είναι η καλύτερη επιλογή ώστε να γίνεται αποδοτικότερη η ευαισθητοποίηση των εργαζομένων. Θα μπορούσε επίσης να είναι χρήσιμο να συγκριθούν οι φάρσες με τους ιούς, διότι μεταδίδονται με συνεχή προώθηση τους.

Πολλές φορές οι φάρσες προειδοποιούν για έναν ιό και ενθαρρύνουν τους χρήστες να διαγράψουν έγκυρα και μερικές φορές σημαντικά αρχεία συστήματος, κάτι το οποίο μπορεί να προκαλέσει σημαντική ζημιά στην εταιρεία. Άλλες φορές οι φάρσες έρχονται με τη μορφή προειδοποίησης σχετικά με έναν ιό που μπορεί να "διαγράψει τον σκληρό σας δίσκο" ή κάτι παρόμοιο και στο μήνυμα θα αναφέρεται να το προωθήσετε σε όλες σας τις επαφές για να τους προειδοποιήσετε. Μια από τις πιο διαδεδομένες απάτες ηλεκτρονικού ταχυδρομείου που εξαπλώνονται είναι αυτή που δηλώνει "Μπορείτε να είστε εκατομμυριούχος" διαβιβάζοντας το μήνυμα ηλεκτρονικού ταχυδρομείου σε άλλους και να πληρώνεστε ένα συγκεκριμένο χρηματικό ποσό για κάθε αποστολή ηλεκτρονικού ταχυδρομείου. Εκατομμύρια άνθρωποι πέφτουν θύματα αυτών των απατών.

Ένας εύκολος τρόπος να εντοπίσετε μια φάρσα ή απάτη είναι η συμπερίληψη ενός συνημμένου. Όπως αξιόπιστοι ιστότοποι δεν θα ζητήσουν προσωπικές πληροφορίες σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου, αξιόπιστοι άνθρωποι ή εταιρείες δεν θα σας στείλουν ένα συνημμένο με οδηγίες για να το χρησιμοποιήσετε προκειμένου να "αφαιρέσει ένα μολυσμένο αρχείο από τον υπολογιστή σας". Δεν θα πρέπει ποτέ να ανοίγετε ένα συνημμένο από κάποιον που δεν γνωρίζετε. [9]

Η πρόληψη της εξάπλωσης των φαρσών μπορεί να αποφευχθεί ελέγχοντας μια σειρά από ιστοσελίδες στο διαδίκτυο που ασχολούνται με την καταγραφή φαρσών και ακολουθώντας κάποιους κανόνες όπως αυτοί που προαναφέρθηκαν. Είναι σημαντικό να επισημανθεί ότι αν κάτι ακούγεται πολύ καλό για να είναι αληθινό, είναι πιθανότατα φάρσα, ενώ αν κάτι φαίνεται ύποπτο μπορεί να ελεγχθεί σε μία από τις ιστοσελίδες αυτές.

Συνοπτικά όσον αφορά τις φάρσες σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- οι τύποι των φαρσών καθώς και παραδείγματά τους
- η επικινδυνότητα του να ανοίγει κανείς ένα συνημμένο από κάποιον που δεν γνωρίζει

5.8 Κακόβουλα προγράμματα

Κατά την αντιμετώπιση κακόβουλου λογισμικού, θα πρέπει αυτό πάντα να αναγνωρίζεται και στη συνέχεια να κατατάσσεται σε κατηγορίες: ιούς, σκουλήκια, δούρειους ίππους, spyware και adware. Στη συνέχεια θα πρέπει να αναλύεται πώς κατάληξε στα συστήματα.

5.8.1 Ιοί (Viruses)

Ξεκινήστε περιγράφοντας τι κάνει έναν ιό έναν ιό. Είναι σημαντικό για τους χρήστες να μπορούν να εντοπίσουν έναν πιθανό ιό όταν βλέπουν κάποιον ή να αναγνωρίσουν χαρακτηριστικά ενός ιού που έχει ήδη διεισδύσει στο σύστημα του χρήστη. Τι είναι ο ιός ικανός να προκαλέσει είναι επίσης κάτι που πρέπει να συμπληρώνει τον ορισμό του τι κάνει έναν ιό αυτό που είναι.

Ο καθορισμός του τι είναι ένας ιός και ο τρόπος αναγνώρισης ενός πρέπει να ολοκληρωθεί με κάποιο λογισμικό προστασίας από ιούς (antivirus). Οι περισσότεροι οργανισμοί θα το έχουν εγκαταστήσει σε όλους τους εταιρικούς υπολογιστές, αλλά πιθανότατα να μην έχει εγκατασταθεί σε προσωπικούς φορητούς υπολογιστές που χρησιμοποιούν οι υπάλληλοι. Οι χρήστες πρέπει επίσης να μάθουν τη σημασία όχι μόνο της εκτέλεσης τακτικών σαρώσεων στους υπολογιστές τους, αλλά και σε οποιοδήποτε αρχείο που κατεβάζουν από μια ιστοσελίδα, από το ηλεκτρονικό ταχυδρομείο ή από κάποια μονάδα δίσκου.

Μια άλλη σημαντική συμβουλή που πρέπει να συμπεριλάβουμε είναι πόσο ζωτικής σημασίας είναι να διατηρηθούν τα συστήματα και οι εφαρμογές ενημερωμένες. Ποτέ μην υποθέσετε ότι ένα σύστημα ή μια εφαρμογή πάντα πρόκειται να ενημερωθεί από μόνη της. Οι χρήστες θα πρέπει να δουν από μόνοι τους εάν τα συστήματα κι οι εφαρμογές που χρησιμοποιούν χρειάζονται ενημέρωση.

Τέλος, είναι σημαντικό να επιτρέπεται στους χρήστες να γνωρίζουν τι πρέπει να κάνουν αν το σύστημά τους μολυνθεί από κάποιο ιό. Βεβαιωθείτε ότι δεν υποκινήσατε μια αίσθηση πανικού η οποία θα κατευθύνει τους εργαζόμενους προς την απόκρυψη της μόλυνσης μέχρι αυτή να ξεφύγει από τον έλεγχο ή το μηχάνημά τους να μην μπορεί να

διορθωθεί. Η κύρια διαδικασία αντιμετώπισης είναι τι πρέπει να κάνετε εάν και όταν ένας ιός μολύνει έναν υπολογιστή.

Όταν το μηχάνημα εργασίας σας μολυνθεί, μην κάνετε τίποτα στον υπολογιστή πέρα από την εκτέλεση σάρωσης με το λογισμικό προστασίας από ιούς που είναι εγκατεστημένο στο μηχάνημα. Έπειτα επικοινωνήστε με το Τμήμα Πληροφορικής της επιχείρησής σας προκειμένου αυτή να έρθει και να αξιολογήσει την κατάσταση.

Εάν το μηχάνημά σας στο σπίτι (ειδικά αν εργάζεστε από το σπίτι) μολυνθεί, είναι σημαντικό να ακολουθήσετε τα παρακάτω βήματα:

1. Μην πανικοβληθείτε.

2. Αποσυνδεθείτε από το Ίντερνετ ή οποιοδήποτε τοπικό δίκτυο μπορεί να είναι συνδεδεμένος ο υπολογιστής.

3. Εάν ο υπολογιστής δεν μπορεί να εκκινήσει, δοκιμάστε να ξεκινήσετε σε ασφαλή λειτουργία (safe mode) ή από τη δισκέτα εκκίνησης των Windows.

4. Δημιουργήστε αντίγραφα ασφαλείας όλων των σημαντικών δεδομένων που δεν μπορείτε να αντέξετε οικονομικά να χάσετε σε ένα εξωτερικό δίσκο, αφού δοκιμάσετε πρώτα το αρχείο με το λογισμικό προστασίας από ιούς.

5. Εάν δεν έχετε εγκαταστήσει λογισμικό προστασίας από ιούς (που δεν θα έπρεπε να συμβάινει σε καμία περίπτωση), εγκαταστήστε το και στη συνέχεια ενημερώστε το.

6. Εκτελέστε μια πλήρη σάρωση του συστήματός σας.

Εικόνα 5 - Στιγμιότυπο σάρωσης συστήματος για ιούς

Συνοπτικά όσον αφορά τους ιούς σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- η σημασία της εκτέλεσης τακτικών σαρώσεων στους υπολογιστές, αλλά και σε οποιοδήποτε αρχείο που κατεβάζουν από μια ιστοσελίδα, από το ηλεκτρονικό ταχυδρομείο ή από κάποια μονάδα δίσκου
- η σημαντικότητα της διατήρησης των συστημάτων και των εφαρμογών με ενημερωμένες εκδόσεις
- τι πρέπει να κάνουν οι χρήστες αν το σύστημά τους μολυνθεί από κάποιο ιό

5.8.2 Σκουλήκι υπολογιστή (Computer worm)

Ένα σκουλήκι υπολογιστή (computer worm) είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας του υπολογιστή προορισμού.

Πολλές φορές συγχέεται το σκουλήκι υπολογιστή (worm) με τον ιό υπολογιστή (virus), επειδή παρουσιάζουν πολλές ομοιότητες στην λειτουργία τους. Παρόλα αυτά όμως υπάρχουν κάποιες σημαντικές διαφορές ως προς τον τρόπο μετάδοσης τους και ως προς την περιοχή του συστήματος που θα προσβάλουν, που τους κάνει να ξεχωρίζουν. Αντίθετα από ότι θα έκανε ένας ιός υπολογιστή, το σκουλήκι δεν χρειάζεται να συνδεθεί με ένα υπάρχον πρόγραμμα. Τα σκουλήκια, σχεδόν πάντα, προκαλούν τουλάχιστον κάποια βλάβη στο δίκτυο, έστω και με την κατανάλωση εύρους ζώνης, ενώ οι ιοί σχεδόν πάντα διαφθείρουν ή τροποποιούν αρχεία σε έναν υπολογιστή προορισμού, αφήνοντας το δίκτυο αβλαβές.

Συνοπτικά όσον αφορά τα σκουλήκια υπολογιστών σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- ο ορισμός του τί ακριβώς είναι το σκουλήκι υπολογιστών
- πώς να εντοπιστεί, τί είναι ικανό να προκαλέσει και πώς να αποτραπεί
- τί να κάνει κάποιος αν ένα σκουλήκι υπολογιστών εισβάλει στο σύστημα

5.8.3 Δούρειος Ίππος (Trojan horse)

Ο δούρειος ίππος (trojan horse ή απλά trojan) είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Συγκεκριμένα, κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν χρήσιμες λειτουργίες, είναι ενδιαφέροντα και δίνουν την εντύπωση στον χρήστη ότι είναι ακίνδυνα. Όταν όμως ο χρήστης εκτελέσει αυτό το πρόγραμμα, τότε ενεργοποιείται ο κακόβουλος κώδικας με αποτέλεσμα ο υπολογιστής να μολυνθεί. Συνήθως αποτέλεσμα της μόλυνσης από δούρειο ίππο είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή και να τον χρησιμοποιούν για να ξεκινήσουν άλλες επιθέσεις προς άλλους υπολογιστές του διαδικτύου. Σε αντίθεση με τους ιούς, οι δούρειοι ίπποι δε μεταδίδονται μολύνοντας αρχεία.

Η πλειοψηφία των μολύνσεων υπολογιστών από δούρειους ίππους συμβαίνει επειδή ο χρήστης προσπάθησε να εκτελέσει ένα μολυσμένο πρόγραμμα. Για τον λόγο αυτό οι

χρήστες θα πρέπει πάντα να προτρέπονται από το άνοιγμα ύποπτων αρχείων επισυναπτόμενα σε e-mail. Συνήθως το επισυναπτόμενο αρχείο περιλαμβάνει όμορφα γραφικά ή κινούμενη εικόνα, αλλά περιέχει επίσης ύποπτο κώδικα που μολύνει τον υπολογιστή του χρήστη. Παρόλα αυτά, το πρόγραμμα δεν είναι απαραίτητο να έχει φτάσει στον χρήστη με e-mail. Μπορεί να το έχει κατεβάσει από έναν ιστοχώρο, μέσω προγραμμάτων Instant Messaging, σε CD ή DVD.
Οι τύποι δούρειων ίππων μπορούν να διαχωριστούν περαιτέρω στις εξής κατηγορίες ανάλογα με τις συνέπειες που έχουν στον μολυσμένο υπολογιστή:

- Απομακρυσμένη πρόσβαση.

- Αποστολή e-mail.

- Καταστροφή αρχείων.

- Κατέβασμα αρχείων.

- Proxy Trojan.

- FTP Trojan (προσθήκη, διαγραφή ή μεταφορά αρχείων από τον μολυσμένο υπολογιστή).

- Απενεργοποίηση λογισμικού ασφαλείας (firewall, αντιϊκά κλπ).

- Επιθέσεις άρνησης υπηρεσιών (Denial of Service, DoS).

- URL Trojan (επιτρέπει στον υπολογιστή να συνδεθεί στο διαδίκτυο μόνο μέσω μίας πολύ ακριβής σύνδεσης).

Μερικές από τις επιπτώσεις εκτέλεσης ενός δούρειου ίππου είναι για παράδειγμα η διαγραφή αρχείων στον μολυσμένο υπολογιστή, η χρησιμοποίησή του για επίθεση σε άλλους υπολογιστές, το ανοιγόκλεισμα του οδηγού CD-ROM, η παρακολούθηση των κινήσεων του χρήστη για την απόκτηση των κωδικών του σε τράπεζες, απόκτηση διευθύνσεων e-mail για να χρησιμοποιηθούν για spamming, επανεκκίνηση του υπολογιστή, απενεργοποίηση προγραμμάτων firewall ή αντιϊκών και πολλά άλλα. [10]
Όλα τα παραπάνω κάνουν το τμήμα που αφορά τους δούρειους ίππους σημαντικό κομμάτι στην εκπαίδευση προσωπικού γι’αυτό θα πρέπει να οριστεί σε αυτή το τι είναι, τι μπορούν να κάνουν, τι μπορεί να γίνει για να αποτραπούν, και τι πρέπει να κάνουμε στην περίπτωση

που κάποιος εισβάλει στο σύστημα. Ένα στοιχείο που πρέπει να τονιστεί επίσης κατά την εκπαίδευση είναι ότι οι δούρειοι ίπποι διαφέρουν από τους ιούς και γιατί είναι δύο διαφορετικά πράγματα.
Συνοπτικά όσον αφορά τους δούρειους ίππους σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- να οριστεί το τί είναι ένα δούρειος ίππος, τί μπορεί να κάνει σε ένα σύστημα και πώς μπορεί να αποτραπεί μια ενδεχόμενη εισβολή
- πώς πρέπει να αντιδράσει κανείς σε περίπτωση που εισβάλει ένας δούρειος ίππος στο σύστημα
- η αποτροπή των χρηστών από το άνοιγμα ύποπτων αρχείων επισυναπτόμενα σε e-mail

5.8.4 Spyware

Τα προγράμματα κατασκοπείας ή αλλιώς spyware είναι γραμμένα με κακόβουλη πρόθεση. Μπορούν να είναι απλά όσο τα ενοχλητικά αναδυόμενα παράθυρα που αποσκοπούν να σας αποσπάσουν την προσοχή ή να σας προσελκύσουν σε κακόβουλα sites. Μπορούν να είναι και λογισμικό που παρακολουθεί τις συνήθειες περιήγησης ιστού ή καταγράφει όλες τις πληκτρολογήσεις που κάνετε με σκοπό να βρεθούν κωδικοί πρόσβασης, τραπεζικοί λογαριασμοί κτλ.
Οι παρακάτω κανόνες αν ακολουθηθούν από το προσωπικό θα προστατεύσουν το σύστημά σας από το spyware:

- Προσπαθήστε να παραμείνετε σε γνωστούς ή αξιόπιστους ιστότοπους στο Internet. Αυτές οι τοποθεσίες παρακολουθούνται γενικά από τους διαχειριστές τους και σπανίως θα έχουν ενσωματωμένο λογισμικό υποκλοπής spyware στον ιστότοπο.

- Πριν πλοηγηθείτε στο διαδίκτυο, συνδεθείτε στο λογαριασμό σας ως κάποιος απλός χρήστης με περιορισμένα δικαιώματα κι όχι ως διαχειριστής. Αυτό θα μειώσει τη δυνατότητα ενός χάκερ να αποκτήσει τον έλεγχο του υπολογιστή σας και να αποκτήσει πρόσβαση σε προσωπικές πληροφορίες.

- Ενεργοποιήστε την ασφάλεια του προγράμματος περιήγησης. Τα προγράμματα περιήγησης όπως ο Internet Explorer, το Mozilla, το Netscape και το Safari έχουν όλα ενσωματωμένα χαρακτηριστικά ασφαλείας στο Διαδίκτυο.

- Απενεργοποιήστε το πρόγραμμα περιήγησης από την αυτόματη λήψη cookies (τα οποία μπορούν να χρησιμοποιηθούν για κακόβουλη πρόθεση).

- Λήψη προγραμμάτων ή λογισμικού μόνο από αξιόπιστους ιστότοπους.

- Ποτέ μην κάνετε κλικ σε ανεπιθύμητα αναδυόμενα παράθυρα. Αντ 'αυτού, κλείστε τις κάνοντας κλικ στο κόκκινο "X" στην επάνω δεξιά γωνία του αναδυόμενου παραθύρου.

- Εγκαταστήστε λογισμικό anti-spyware, κρατάτε το ενημερωμένο και αφήστε το να τρέχει τακτικά. Αρκετά πακέτα όπως το SpyBot και το AdAware είναι δωρεάν και κάνουν μεγάλη δουλειά στην προστασία του συστήματός σας από το ανεπιθύμητο και ενοχλητικό λογισμικό υποκλοπής spyware.

- Εγκαταστήστε ένα πρόγραμμα που να μην επιτρέπει τη λειτουργία αναδυόμενων παράθυρα.

Στο πρόγραμμα ευαισθητοποίησης θα πρέπει να οριστεί τι είναι το spyware, τι μπορεί να κάνει, συμβουλές και κόλπα πρόληψης και στη συνέχεια τι πρέπει να κάνετε αν βρεθεί στο σύστημα. Καλό θα ήταν να προταθούν και κάποια προγράμματα εντοπισμού και αφαίρεσης προγραμμάτων υποκλοπής spyware, όπως το SpyBot και το AdAware που είναι δωρεάν και κάνουν μεγάλη δουλειά στην προστασία του συστήματός σας από το ανεπιθύμητο και ενοχλητικό λογισμικό υποκλοπής spyware.[11]
Συνοπτικά όσον αφορά τα spyware σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- να οριστεί τι είναι το spyware, τι είναι ικανό να κάνει και συμβουλές και κόλπα πρόληψής του
- τι πρέπει να κάνει ο χρήστης αν αυτό βρεθεί στο σύστημα
- η σημαντικότητα του να παραμένουν οι χρήστες σε γνωστούς ή αξιόπιστους ιστότοπους στο Internet και λήψη προγραμμάτων ή λογισμικού μόνο από αυτούς

- η σύνδεση λογαριασμών ως κάποιος απλός χρήστης με περιορισμένα δικαιώματα κι όχι ως διαχειριστής
- η ενεργοποίηση της ασφάλειας του προγράμματος περιήγησης και απενεργοποίηση από την αυτόματη λήψη cookies
- η εγκατάσταση κάποιου προγράμματος που να μην επιτρέπει τη λειτουργία αναδυόμενων παραθύρων
- η εγκατάσταση λογισμικού anti-spyware, το οποίο θα πρέπει να κρατάει ο χρήστης ενημερωμένο και να το τρέχει τακτικά

5.9 Διαμοιρασμός αρχείων και πνευματικά δικαιώματα

Κατά την επίλυση των δικαιωμάτων πνευματικής ιδιοκτησίας όσον αφορά την κοινή χρήση αρχείων, οι τύποι των πνευματικών δικαιωμάτων (π.χ. εγγραφές, βίντεο και λογισμικό) θα πρέπει να περιλαμβάνονται στην εισαγωγή. Οι προτάσεις σχετικά με τον τρόπο ψηφιακής απόκτησης νόμιμων έργων που προστατεύονται από πνευματικά δικαιώματα θα πρέπει να ολοκληρώνουν την εισαγωγή.

Οι περισσότερες εγγραφές και τα βίντεο που είναι διαθέσιμα σήμερα προστατεύονται από νόμους περί πνευματικών δικαιωμάτων. Για να αποκτήσετε ένα έργο που δεν είναι δημόσιο, είναι απαραίτητο να λάβετε άδεια από τον κάτοχο των πνευματικών δικαιωμάτων. Αυτό μπορεί να επιτευχθεί με την καταβολή του κατάλληλου τέλους σε ένα νόμιμο site λήψης. Υπηρεσίες όπως η Napster, η Apple iTunes και η Musicmatch παρέχουν άδεια λήψης με βάση μια υπογεγραμμένη συμφωνία ή μια χρέωση υπηρεσιών. Μερικές φορές οι ιστότοποι έχουν μια ρητή δήλωση λέγοντας ότι είναι αποδεκτό να κατεβάζετε και να αναπαράγετε το έργο τους χωρίς άδεια, αλλά αυτό είναι ένα σπάνιο περιστατικό.

Τα προγράμματα και οι μέθοδοι κοινής χρήσης αρχείων πρέπει να είναι το επόμενο στοιχείο που πρέπει να καλυφθεί (π.χ. προγράμματα peer to peer και bittorrenting). Πρέπει επίσης να τονιστεί ότι, παρά το γεγονός ότι είναι παράνομα, αυτά τα προγράμματα και οι χώροι που προσφέρουν τους πόρους γι 'αυτούς αποτελούν λόγους αναπαραγωγής για ιούς. Πρέπει επίσης να δηλωθεί ότι η παράνομη διανομή και λήψη αρχείων είναι σπατάλη πόρων και αν το αντιμετωπίζει η πολιτική του οργανισμού, μπορεί να αποτελέσει αξιόποινη πράξη.

Σε αυτό το κεφάλαιο πρέπει επίσης να αναφερθούν οι νομικές συνέπειες της κοινής χρήσης και της λήψης των παράνομων αρχείων, καθώς και παραδείγματα περιπτώσεων που έχουν ασκηθεί εναντίον ατόμων που έχουν πιαστεί να κάνουν κάτι τέτοιο.
Συνοπτικά όσον αφορά το διαμοιρασμό αρχείων και τα πνευματικά δικαιώματα σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- οι τύποι των πνευματικών δικαιωμάτων
- προτάσεις σχετικά με τον τρόπο ψηφιακής απόκτησης νόμιμων έργων που προστατεύονται από πνευματικά δικαιώματα
- προγράμματα και μέθοδοι κοινής χρήσης αρχείων
- η αναφορά των νομικών συνεπειών της κοινής χρήσης και της λήψης των παράνομων αρχείων, καθώς και παραδείγματα περιπτώσεων που έχουν ασκηθεί εναντίον ατόμων που έχουν κάνει κάτι τέτοιο

5.10 Αναφορά περιστατικού ασφαλείας

Το πρόγραμμα εκπαίδευσης θα μπορούσε να περιλαμβάνει κι οδηγίες στην περίπτωση που συμβεί κάποιο περιστατικό ασφαλείας. Συγκεκριμένα το προσωπικό θα πρέπει να γνωρίζει πώς να αναγνωρίζει ένα περιστατικό, τί ενέργειες πρέπει να κάνει και ποιο τμήμα να ενημερώσει για την αντιμετώπιση του περιστατικού.
Ένα περιστατικό ασφάλειας που αφορά ηλεκτρονικές πληροφορίες ή τεχνολογία πληροφοριών περιλαμβάνει τα ακόλουθα:

- Μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, τροποποίηση ή καταστροφή ηλεκτρονικών πληροφοριών

- Παραβίαση αποδεκτών πολιτικών χρήσης

- Παρεμβολή στη λειτουργία των πόρων του πληροφοριακού συστήματος, όπως η επίθεση άρνησης εξυπηρέτησης (dos attack)

- Ανακάλυψη αδυναμιών στα μέτρα προστασίας των ηλεκτρονικών πληροφοριών ή συστημάτων πληροφοριών

Για την ευκολότερη κατανόηση από το προσωπικό, σχετικά με περιστατικά ασφαλείας, θα μπορούσαν να αναφερθούν κάποια από τα παρακάτω παραδείγματα:

- Απώλεια ή κλοπή φορητών υπολογιστών, επιτραπέζιων υπολογιστών ή άλλου εξοπλισμού που χρησιμοποιείται για την πρόσβαση ή την αποθήκευση δεδομένων, συμπεριλαμβανομένων των κινητών τηλεφώνων και των εξωτερικών σκληρών δίσκων

- Εισβολή σε υπολογιστικό σύστημα

- Μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες, είτε σκόπιμα είτε τυχαία

- Μη εξουσιοδοτημένη χρήση των διαπιστευτηρίων άλλου χρήστη ή πλαστοπροσωπία άλλου χρήστη

- Μια επίθεση άρνησης εξυπηρέτησης

- Ένας εκτεθειμένος λογαριασμός χρήστη

Η χρήση ενός υπολογιστή ή συσκευής που έχει εκτεθεί θα μπορούσε να επιδεινώσει το περιστατικό ασφάλειας και να επηρεάσει αρνητικά το πληροφοριακό σύστημα. Οι πρώτες κινήσεις του προσωπικού ενδέχεται να ειδοποιήσουν τους εισβολείς και να προβούν σε ενέργειες για την κατάργηση αποδεικτικών στοιχείων ή τη διαγραφή αρχείων. Το πρόγραμμα εκπαίδευσης πρέπει να ενημερώνει τους εκπαιδευόμενους με το που αντιληφθούν ένα περιστατικό ασφαλείας να:

- Απενεργοποιήσουν τον υπολογιστή ή όποια άλλη ηλεκτρονική συσκευή έχουν συνδέσει στο δίκτυο

- Εάν είναι δυνατό μετά την απενεργοποίηση, να αποσυνδέσουν το καλώδιο δικτύου Ethernet

- Στη συνέχεια, να απομακρυνθούν από τον υπολογιστή χωρίς να κάνουν οποιαδήποτε άλλη ενέργεια, μέχρι να αναλάβει το τμήμα αντιμετώπισης περιστατικών ασφαλείας. [12]

Ακόμα κι αν το προσωπικό δεν είναι σίγουρο για το αν ένα συμβάν αφορά την ασφάλεια, καλό θα ήταν να το αναφέρει προκειμένου να επιβεβαιωθεί αν όντως πρόκειται για περιστατικό. Η αναφορά ενός περιστατικού ασφαλείας μπορεί να είναι εύκολη υπόθεση

αν υπάρχει έτοιμο έντυπο υπόδειγμα. Σε κάθε περίπτωση στην αναφορά το προσωπικό θα πρέπει να γνωστοποιήσει, εφόσον είναι δυνατόν, τις παρακάτω πληροφορίες:

- Ημερομηνία κι ώρα του περιστατικού

- Ποιες υπηρεσίες ή συσκευές έχουν επηρεαστεί

- Αιτία περιστατικού (π.χ. ανθρώπινο λάθος, κακόβουλη επίθεση, φυσική καταστροφή κτλ)

- Ενέργειες που έγιναν μετά το περιστατικό

- Άλλες πληροφορίες και παρατηρήσεις που μπορεί να βοηθήσουν στην αντιμετώπιση του περιστατικού

Θα πρέπει να τονιστεί ότι η σωστή αντιμετώπιση περιλαμβάνει και την ψυχραιμία του προσωπικού, καθώς υπάρχει (ή θα πρέπει να υπάρχει) ένα καθιερωμένο πρωτόκολλο για το χειρισμό περιστατικών και το αντίστοιχο τμήμα θα είναι εξοπλισμένο για να καθοδηγήσει την όλη διαδικασία. Επίσης, το περιστατικό δεν θα πρέπει να συζητηθεί με άτομα που δεν είναι εξουσιοδοτημένα, ενώ είναι σημαντικό οι πληροφορίες να είναι ακριβείς χωρίς υποθέσεις ή εικασίες οι οποίες μπορεί να μπερδέψουν ή να καθυστερήσουν την έρευνα.

Συνοπτικά όσον αφορά την αναφορά περιστατικού ασφαλείας σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- οι οδηγίες στην περίπτωση που συμβεί κάποιο περιστατικό ασφαλείας
- πώς να αναγνωρίζει κανείς ένα περιστατικό, τί ενέργειες πρέπει να κάνει και ποιο τμήμα να ενημερώσει για την αντιμετώπιση του περιστατικού
- η σημασία της διατήρησης ψυχραιμίας του προσωπικού, καθώς υπάρχει (ή θα πρέπει να υπάρχει) ένα καθιερωμένο πρωτόκολλο για το χειρισμό περιστατικών και το αντίστοιχο τμήμα θα είναι εξοπλισμένο για να καθοδηγήσει την όλη διαδικασία
- η αποτροπή συζήτησης του περιστατικού με άτομα που δεν είναι εξουσιοδοτημένα καθώς και αποφυγή εικασιών

SANS CRITICAL LOG REVIEW CHECKLIST FOR SECURITY INCIDENTS

This cheat sheet presents a checklist for reviewing critical logs when responding to a security incident. It can also be used for routine log review.

GENERAL APPROACH

1. Identify which log sources and automated tools you can use during the analysis.
2. Copy log records to a single location where you will be able to review them.
3. Minimize "noise" by removing routine, repetitive log entries from view after confirming that they are benign.
4. Determine whether you can rely on logs' time stamps; consider time zone differences.
5. Focus on recent changes, failures, errors, status changes, access and administration events, and other events unusual for your environment.
6. Go backwards in time from now to reconstruct actions after and before the incident.
7. Correlate activities across different logs to get a comprehensive picture.
8. Develop theories about what occurred; explore logs to confirm or disprove them.

POTENTIAL SECURITY LOG SOURCES

- Server and workstation operating system logs
- Application logs (e.g., web server, database server)
- Security tool logs (e.g., anti-virus, change detection, intrusion detection/prevention system)
- Outbound proxy logs and end-user application logs
- Remember to consider other, non-log sources for security events.

TYPICAL LOG LOCATIONS

- Linux OS and core applications: /var/log
- Windows OS and core applications: Windows Event Log (Security, System, Application)
- Network devices: usually logged via Syslog; some use proprietary locations and formats

WHAT TO LOOK FOR ON LINUX

Successful user login	**"Accepted password", "Accepted publickey", "session opened"**
Failed user login	**"authentication failure", "failed password"**
User log-off	**"session closed"**
User account change or deletion	**"password changed", "new user", "delete user"**
Sudo actions	**"sudo: … COMMAND=…" "FAILED su"**
Service failure	**"failed" or "failure"**

WHAT TO LOOK FOR ON WINDOWS

- Event IDs are listed below for Windows 2000/XP. For Vista/7 security event ID, add 4096 to the event ID.
- Most of the events below are in the Security log; many are only logged on the domain controller.

User logon/logoff events	**Successful logon 528, 540; failed logon 529-537, 539; logoff 538, 551, etc**
User account changes	**Created 624; enabled 626; changed 642; disabled 629; deleted 630**
Password changes	**To self: 628; to others: 627**
Service started or stopped	**7035, 7036, etc.**
Object access denied (if auditing enabled)	**560, 567, etc**

WHAT TO LOOK FOR ON NETWORK DEVICES

- Look at both inbound and outbound activities.
- Examples below show log excerpts from Cisco ASA logs; other devices have similar functionality.

Traffic allowed on firewall	**"Built … connection", "access-list … permitted"**
Traffic blocked on firewall	**"access-list … denied", "deny inbound"; "Deny … by"**
Bytes transferred (large files?)	**"Teardown TCP connection … duration … bytes …"**
Bandwidth and protocol usage	**"limit … exceeded", "CPU utilization"**
Detected attack activity	**"attack from"**
User account changes	**"user added", "user deleted", "User priv level changed"**
Administrator access	**"AAA user …", "User … locked out", "login failed"**

WHAT TO LOOK FOR ON WEB SERVERS

- Excessive access attempts to non-existent files
- Code (SQL, HTML) seen as part of the URL
- Access to extensions you have not implemented
- Web service stopped/started/failed messages
- Access to "risky" pages that accept user input
- Look at logs on all servers in the load balancer pool
- Error code 200 on files that are not yours

Failed user authentication	**Error code 401, 403**
Invalid request	**Error code 400**
Internal server error	**Error code 500**

OTHER RESOURCES

- **Windows event ID lookup:** www.eventid.net
- **A listing of many Windows Security Log events:** ultimatewindowssecurity.com/.../Default.aspx
- **Log analysis references:** www.loganalysis.org
- **A list of open-source log analysis tools:** securitywarriorconsulting.com/logtools
- **Anton Chuvakin's log management blog:** securitywarriorconsulting.com/logmanagementblog
- **Other security incident response-related cheat sheets:** zeltser.com/cheat-sheets

Authored by Anton Chuvakin (chuvakin.org) and Lenny Zeltser (zeltser.com).

Reviewed by Anand Sastry.

Cheat sheet version 1.0.

Εικόνα 6 – Οδηγίες για περιστατικό ασφαλείας

5.11 Πολιτικές Ασφαλείας

Είναι ιδιαίτερα σημαντικό το εκπαιδευόμενο προσωπικό να γνωρίζει την Πολιτική

Ασφάλειας Πληροφοριακών Συστημάτων της εταιρείας ή του οργανισμού στο οποίο εργάζεται διότι αυτή ορίζει ένα σύνολο αρχών, κανόνων και διαδικασιών που έχουν ως κύριο στόχο την προστασία των Π.Σ. και των δεδομένων που χρησιμοποιούνται και διαχειρίζονται από τον οργανισμό στα πλαίσια της επιχειρησιακής του λειτουργίας. Βασίζεται στις βέλτιστες πρακτικές ασφάλειας πληροφοριών και χρησιμεύει ως ένας ενιαίος οδηγός Ασφάλειας για την ορθή χρήση των Π.Σ. και δεδομένων.

Ο σκοπός της Πολιτικής είναι να παρέχει την βούληση της ανώτατης διοίκησης ως απόφαση του Δ.Σ και τις απαραίτητες κατευθύνσεις ακολουθώντας τις αρχές εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας για τα δεδομένα που ο οργανισμός χρησιμοποιεί, διατηρεί και μεταφέρει μέσω των Πληροφοριακών Συστημάτων για την υλοποίηση των επιχειρηματικών στόχων του.

Οι στόχοι μιας Πολιτικής Ασφαλείας μπορεί να είναι:

- Η ασφάλεια Πληροφοριών και Δεδομένων.

- Η καθοδήγηση στην επιλογή και υλοποίηση των μέτρων και αντιμέτρων ασφάλειας.

- Η ενίσχυση των καναλιαών επικοινωνίας μεταξύ των εμπλεκομένων μερών (IT Security officers and Managers).

- Η εξασφάλιση και διαχείριση των απαιτούμενων πόρων για την υλοποίηση της.

- Η εδραίωση της σημασίας της Ασφάλειας των Π.Σ.

- Η βοήθεια στην ανάπτυξη νοοτροπίας και φιλοσοφίας ασφάλειας στον ανθρώπινο παράγοντα.

- Η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των εμπορικά ευαίσθητων πληροφοριών Χρηστών και φορέων της αγοράς και των Προσωπικών Δεδομένων σύμφωνα με τον Κανονισμό Προστασίας των Δεδομένων(General Data Protection Regulation - GDPR) της Ευρωπαϊκής Ένωσης.

Η εκπαίδευση του προσωπικού για ευαισθητοποίηση σε θέματα ασφαλείας θα πρέπει να προσαρμόζεται κάθε φορά στην υπάρχουσα Πολιτική Ασφαλείας του οργανισμού και γι’αυτό θα πρέπει να μελετηθεί προσεχτικά και από τους εκπαιδευτές. Παρακάτω αναλύονται κάποιες από τις περιοχές της Πολιτικής στις οποίες θα πρέπει να δώσει

προσοχή και να συμπεριλάβει το πρόγραμμα εκπαίδευσης, εφόσον αυτές ταιριάζουν με τις Πολιτικές του εκάστοτε οργανισμού:

- *Διαβάθμιση Πληροφοριών*

Οι πληροφορίες που διαχειρίζεται ο οργανισμός θα πρέπει να διαβαθμίζονται σύμφωνα με την Πολιτική Διαβάθμισης Πληροφοριών, η οποία αποσκοπεί στον καθορισμό των αρχών και κανόνων και στην αποτύπωση του μηχανισμού διασφάλισης της ορθής διαχείρισης και προστασίας της εμπιστευτικότητας των πληροφοριών που διαχειρίζεται ο οργανισμός.

- *Αποδεκτή Χρήση Συστημάτων Και Πληροφοριών*

Προσδιορίζεται η αποδεκτή χρήση του διαδικτύου, της ηλεκτρονικής αλληλογραφίας, των συστημάτων τηλεομοιοτυπίας (φαξ) & φωτοτυπίας, για τις άδειες χρήσης λογισμικού και η χρήση μη εγκεκριμένου λογισμικού. Επίσης, μπορεί να διανέμεται στους χρήστες εγχειρίδιο στο οποίο θα αναφέρονται όλες οι υποχρεώσεις τους και οι βασικοί κανόνες ασφάλειας που αφορούν τη χρήση των Πληροφοριακών Συστημάτων.

- *Ασφάλεια Συστημάτων*

Η Διεύθυνση Πληροφορικής & Τηλεπικοινωνιών θα πρέπει να συντηρεί επίσημο αρχείο (λίστα) στο οποίο θα περιγράφονται οι εφαρμογές του οργανισμού, η επιχειρησιακή λειτουργία τους, τα τεχνικά χαρακτηριστικά τους (λειτουργικό σύστημα, βάσεις δεδομένων, δίκτυο, γέφυρες επικοινωνίας), οι επιχειρησιακοί υπεύθυνοι, οι υπεύθυνοι διαχειριστές από πλευράς πληροφορικής και η φυσική τοποθεσία της πληροφοριακής υποδομής. Επιπλέον, θα πρέπει να υφίστανται και να διατηρούνται επίσημα έγγραφα ανά είδος τεχνολογίας, στα οποία να περιγράφονται οι βασικές παράμετροι ασφάλειας που είναι ενεργοποιημένες.

- *Ασφάλεια Δικτύου και Επικοινωνιών*

Ο σχεδιασμός και η λειτουργία της δικτυακής υποδομής με ταυτόχρονη διασφάλιση της υψηλής απόδοσης, αξιοπιστίας και ελέγχου πρόσβασης των χρηστών στα απαραίτητα μόνο συστήματα και εφαρμογές, πρέπει να αποτελεί προτεραιότητα για τον οργανισμό. Ενημερωμένα διαγράμματα δικτύου και πληροφοριακό υλικό θα πρέπει να διατηρούνται με σκοπό την υποστήριξη λειτουργίας του δικτύου, σύμφωνα με τις απαιτήσεις ασφαλείας. Πρότυπα ασφάλειας και οργανωτικές ρυθμίσεις πρέπει να ακολουθούνται εφόσον

σχετίζονται με το εταιρικό δίκτυο του οργανισμού, το σχεδιασμό, τη διαμόρφωση και την τεκμηρίωση του.

- *Προστασία από Κακόβουλο Λογισμικό*

Κατευθυντήριες γραμμές πρέπει να δοθούν με σκοπό να προστατευτούν οι υποδομές του οργανισμού από ιούς υπολογιστών ή οποιοδήποτε άλλο κακόβουλο λογισμικό. Το λογισμικό αντιμετώπισης ιών πρέπει υποχρεωτικά να είναι εγκατεστημένο σε όλα τα συστήματα του οργανισμού, συμπεριλαμβανομένων δοκιμαστικών συστημάτων και συστημάτων της παραγωγής, σταθμών εργασίας, φορητών υπολογιστών και αυτόνομων προσωπικών υπολογιστών που αποκτούν απομακρυσμένα πρόσβαση στις υποδομές του οργανισμού. Το λογισμικό αντιμετώπισης ιών θα πρέπει να είναι πάντα ενεργοποιημένο και να ενημερώνεται συχνά. Για οποιαδήποτε αλλαγή στις ρυθμίσεις του λογισμικού αντιμετώπισης ιών θα πρέπει προηγουμένως να υπάρχει έγκριση από τον Υπεύθυνο Ασφάλειας.

- *Έλεγχος Προσβάσεων*

Η σύνδεση και η πρόσβαση στα σύστημα του οργανισμού, θα καταγράφεται και θα περιορίζεται χωρίς να να παρεμποδίζεται η καλή λειτουργία του οργανισμού. Ειδική διαδικασία θα πρέπει να ακολουθείται για την κατανομή των δικαιωμάτων πρόσβασης στους χρήστες των Πληροφοριακών Συστημάτων του οργανισμού. Τα δικαιώματα πρόσβασης των χρηστών στα πληροφοριακά συστήματα του οργανισμού θα πρέπει να βασίζονται στην αρχή της «ελάχιστης αναγκαίας γνώσης».

- *Ασφάλεια Διαχείρισης Τρίτων Μερών*

Ο οργανισμός θα πρέπει να ακολουθεί καθορισμένους κανόνες που θα επιτρέπουν σε τρίτους (πελάτες, προμηθευτές, ή οποιουσδήποτε άλλους συνεργάτες του οργανισμού) να παρέχουν υπηρεσίες ή να έχουν πρόσβαση στα πληροφοριακά συστήματα ή στο δίκτυο του οργανισμού, με ασφαλή τρόπο.

- *Διαχείριση Κωδικών Πρόσβασης*

Προδιαγραφές για την ασφαλή διαχείριση των κωδικών πρόσβασης και κανόνες για την ασφαλή διαχείριση των εταιρικών κωδικών πρόσβασης πρέπει να καθοριστούν, δίνοντας παράλληλα ιδιαίτερη προσοχή στους λογαριασμούς της βάσης δεδομένων και στους χρήστες με δικαιώματα διαχειριστή. Όλοι οι λογαριασμοί των χρηστών θα πρέπει να

ρυθμίζονται κεντρικά από το Τμήμα Πληροφορικής για την εφαρμογή των ακόλουθων βασικών κανόνων διαμόρφωσης κωδικών : ο κωδικός πρόσβασης πρέπει να αποτελείται τουλάχιστον από 6 χαρακτήρες, θα πρέπει να περιέχει κεφαλαία και μικρά γράμματα / ειδικούς χαρακτήρες και αριθμούς και δεν μπορεί να είναι ταυτόσημος με το όνομα χρήστη. Επίσης ο κωδικός πρόσβασης πρέπει να αλλάζεται κάθε 3 μήνες και δεν μπορεί να είναι ταυτόσημος με τους τελευταίους 5 κωδικούς πρόσβασης. Μετά από ορισμένο αριθμό αποτυχημένων προσπαθειών ο λογαριασμός του χρήστη θα πρέπει να κλειδώνεται.

- *Λειτουργικός Έλεγχος & Έλεγχοι Ασφάλειας*

Θα πρέπει να διεξάγονται σε τακτά χρονικά διαστήματα εσωτερικοί έλεγχοι ασφάλειας, ώστε να εξασφαλίζεται κατά το μέγιστο δυνατό η έγκαιρη εξακρίβωση των τεχνολογικών και διαδικαστικών αδυναμιών ασφάλειας. Σημαντικά συμβάντα ασφάλειας και ενέργειες σχετικά με κρίσιμα λειτουργικά συστήματα, βάσεις δεδομένων, εφαρμογές και συσκευές δικτύου πρέπει να καταγράφονται και να παρακολουθούνται.

- *Φυσική Ασφάλεια*

Οι κανόνες που αφορούν στην φυσική ασφάλεια των εγκαταστάσεων του οργανισμού όπου κρατείται ηλεκτρονική και μη πληροφορία, καθώς και ο εξοπλισμός και οι υποδομές Πληροφορικής, πρέπει να εφαρμόζονται. Εξειδικευμένοι έλεγχοι φυσικής ασφαλείας θα πρέπει να εφαρμόζονται στους τομείς της ασφάλειας των κτιρίων, της ασφάλειας των τηλεπικοινωνιών, της ασφάλειας των Data Centers και των ασφαλών χώρων εργασίας.

- Διαχείριση Συμβάντων Ασφάλειας

Ένα πλαίσιο θα πρέπει να θεσπιστεί για την έγκαιρη και αποτελεσματική αντιμετώπιση των περιστατικών που ανιχνεύονται και αναφέρονται από τους εργαζομένους του οργανισμού, από εξωτερικούς συνεργάτες ή από το σύστημα παρακολούθησης συμβάντων ασφαλείας. Όλα τα συμβάντα θα πρέπει να καταγράφονται προσεκτικά για ανάλυση, με απώτερο σκοπό την εφαρμογή μέτρων που θα αποτρέψουν την εκδήλωση παρομοίων συμβάντων στο μέλλον.

- Διαχείριση Συνέχειας Εργασιών

Η διαδικασία Ανάκαμψης από Καταστροφή υλοποιείται προκειμένου να επανέλθει βέλτιστα και άμεσα ο οργανισμός σε λειτουργία ύστερα από διακοπές που οφείλονται σε καταστροφές ή αστοχίες σε θέματα ασφάλειας (τα οποία ενδέχεται να είναι, για

παράδειγμα, αποτέλεσμα φυσικών φαινομένων, ατυχημάτων, βλάβες εξοπλισμού ή ακόμη και ενσυνείδητων πράξεων), σε ένα αποδεκτό – για την επιχείρηση – επίπεδο, μέσω ενός συνδυασμού προληπτικών και επανορθωτικών ενεργειών. Βασικό συστατικό για το σχεδιασμό και την υλοποίηση των σχεδίων ανάκαμψης από καταστροφή και επιχειρηματικής συνέχειας είναι ο προσδιορισμός μιας αναλυτικής και τεκμηριωμένης διαδικασίας για την διαχείριση των αντιγράφων ασφάλειας, το αποδεκτό επίπεδο από την εταιρεία του χρόνου επανάκαμψης και το αποδεκτό όριο απώλειας δεδομένων.

- Ιδιαιτερότητες Ασφάλειας Κρίσιμων Εγκαταστάσεων

Λόγω του σημαντικού επιχειρησιακού σκοπού του οργανισμού οι κρίσιμες εγκαταστάσεις πρέπει να είναι εναρμονισμένες με τα ευρωπαϊκά και διεθνή κανονιστικά πλαίσια ασφάλειας που ισχύουν.

- Προμήθεια, Ανάπτυξη & Συντήρηση Π.Σ

Η εισαγωγή των μηχανισμών ελέγχου και ασφάλειας κατά τον σχεδιασμό και ανάπτυξη νέων συστημάτων και εφαρμογών θα πρέπει να θεωρείται απαραίτητη και επιβεβλημένη, ώστε να καλύπτονται οι απαιτήσεις ασφάλειας με τέτοιο τρόπο που να εξασφαλίζονται η συμμόρφωση με το υπάρχον νομοθετικό πλαίσιο και το Ευρωπαϊκό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων. Ο οργανισμός θα πρέπει να έχει σχεδιάσει και υλοποιήσει συγκεκριμένους μηχανισμούς και διαδικασίες παρακολούθησης, καταγραφής και διαχείρισης κάθε είδους αλλαγής που δύναται να θέσει σε κίνδυνο την ομαλή λειτουργία των επιχειρηματικών λειτουργιών και την ασφάλεια των συστημάτων και των πληροφοριών.

- Ασφάλεια Ανθρώπινου Δυναμικού

Ένα γενικό πλαίσιο των μέτρων προστασίας που πρέπει να λάβει ο οργανισμός έτσι ώστε να περιοριστεί στο ελάχιστο η πιθανότητα να πλήξει την ασφάλεια των πληροφοριακών συστημάτων και των πληροφοριών ο ανθρώπινος παράγοντας. Η διοίκηση του οργανισμού πρέπει να εξασφαλίσει ότι όλοι οι υπάλληλοι και τα τρίτα μέρη ή συνεργάτες ενημερώνονται και εκπαιδεύονται στα καθήκοντα και στις αρμοδιότητές τους, όσον αφορά στην Πολιτική Ασφάλειας και στην εφαρμογή της, με σκοπό να είναι σε θέση να αναγνωρίζουν και να αντιμετωπίζουν κατάλληλα πιθανά συμβάντα ασφάλειας.

- Απόκλιση από την Πολιτική Ασφάλειας

Περιπτώσεις μη συμμόρφωσης με την Πολιτική Ασφάλειας Π.Σ. θα πρέπει να καταγράφονται και να αναφέρονται στον Υπεύθυνο Ασφάλειας και στην Επιτροπή Ασφάλειας Πληροφοριακών Συστημάτων. Εφόσον υφίσταται σημαντική αιτία, οι υπεύθυνοι θα μπορούν να προτείνουν για συγκεκριμένες δικαιολογημένες περιπτώσεις εξαιρέσεις από τους κανόνες που περιγράφονται στην Πολιτική Ασφάλειας. [13]

Συνοπτικά όσον αφορά την πολιτική ασφαλείας σε ένα πρόγραμμα εκπαίδευσης θα πρέπει να τονιστούν τα παρακάτω θέματα:

- η αναγκαιότητα ύπαρξης Πολιτικής Ασφαλείας
- η σπουδαιότητα επίγνωσης της Πολιτικής Ασφαλείας
- τί περιλαμβάνει γενικά μια Πολιτική Ασφαλείας

6. Ανάπτυξη στρατηγικής και πλάνου για ευαισθητοποίηση κι εκπαίδευση

Ο οργανισμός θα πρέπει να αναπτύξει μια στρατηγική για την εφαρμογή και διατήρηση του προγράμματος ευαισθητοποίησης στον τομέα της ασφάλειας. Το πλάνο είναι το έγγραφο εργασίας που περιέχει τα στοιχεία που αποτελούν τη στρατηγική. Στο πλάνο πρέπει να συζητηθούν τα ακόλουθα στοιχεία:

- Υπάρχουσα εθνική και τοπική πολιτική που απαιτεί την πραγματοποίηση της ευαισθητοποίησης και εκπαίδευσης.

- Πεδίο εφαρμογής του προγράμματος ευαισθητοποίησης κι εκπαίδευσης.

- Ρόλοι και ευθύνες του προσωπικού που θα πρέπει να σχεδιάζει, να αναπτύσσει, να εφαρμόζει και να διατηρεί το υλικό ευαισθητοποίησης και εκπαίδευσης καθώς και ποιος πρέπει να διασφαλίζει ότι οι κατάλληλοι χρήστες παρευρίσκονται ή έχουν πρόσβαση στο κατάλληλο υλικό.

- Στόχοι που πρέπει να επιτευχθούν για κάθε πτυχή του προγράμματος (π.χ. ευαισθητοποίηση, κατάρτιση, εκπαίδευση, επαγγελματική ανάπτυξη [πιστοποίηση]).

- Στοχευόμενα ακροατήρια για κάθε πτυχή του προγράμματος ·

- Υποχρεωτικά (και κατά περίπτωση προαιρετικά) μαθήματα ή υλικό για κάθε στοχευόμενο ακροατήριο.

- Εκμάθηση στόχων για κάθε πτυχή του προγράμματος.

- Θέματα που πρέπει να εξεταστούν σε κάθε συνεδρία ή σεμινάριο.

- Μέθοδοι ανάπτυξης που πρέπει να χρησιμοποιούνται για κάθε πτυχή του προγράμματος.

- Τεκμηρίωση, ανατροφοδότηση και απόδειξη εκμάθησης για κάθε πτυχή του προγράμματος.

- Αξιολόγηση και ενημέρωση υλικού για κάθε πτυχή του προγράμματος.

- Συχνότητα που κάθε στοχευμένο ακροατήριο πρέπει να εκτεθεί στο υλικό.

6.1 Διεξαγωγή αξιολόγησης αναγκών

Η αξιολόγηση των αναγκών είναι μια διαδικασία που μπορεί να χρησιμοποιηθεί για τον προσδιορισμό των αναγκών ευαισθητοποίησης και κατάρτισης ενός οργανισμού. Τα αποτελέσματα της εκτίμησης των αναγκών μπορούν να αποτελέσουν αιτιολόγηση για να πείσουν τη διοίκηση να διαθέσει επαρκείς πόρους για να ανταποκριθεί στις αναγνωρισμένες ανάγκες ευαισθητοποίησης και κατάρτισης.

Κατά τη διενέργεια αξιολόγησης των αναγκών, είναι σημαντικό να εμπλέκεται το βασικό προσωπικό. Ως ελάχιστο, οι ακόλουθοι ρόλοι πρέπει να αντιμετωπιστούν όσον αφορά τις ειδικές ανάγκες κατάρτισης:

- *Εκτελεστική Διοίκηση*

Οι ηγέτες των οργανώσεων πρέπει να κατανοούν πλήρως τις οδηγίες και τους νόμους που αποτελούν τη βάση του προγράμματος ασφαλείας. Πρέπει επίσης να κατανοήσουν τους ηγετικούς τους ρόλους για την εξασφάλιση της πλήρους συμμόρφωσης των χρηστών εντός των μονάδων τους.

- *Προσωπικό Ασφαλείας (διαχειριστές προγραμμάτων ασφαλείας και αξιωματικοί ασφαλείας)*

Αυτά τα άτομα ενεργούν ως ειδικοί σύμβουλοι για την οργάνωσή τους και ως εκ τούτου πρέπει να είναι καλά εκπαιδευμένοι σχετικά με την πολιτική ασφαλείας και τις αποδεκτές βέλτιστες πρακτικές.

- *Ιδιοκτήτες συστημάτων*

Οι ιδιοκτήτες πρέπει να έχουν ευρεία κατανόηση της πολιτικής ασφαλείας και υψηλό βαθμό κατανόησης όσον αφορά τους ελέγχους ασφαλείας και τις απαιτήσεις που ισχύουν για τα συστήματα που διαχειρίζονται.

- *Διαχειριστές Συστημάτων και Προσωπικό Υποστήριξης Πληροφορικής*

Έχουν υψηλό βαθμό εξουσίας για τις λειτουργίες υποστήριξης που είναι κρίσιμες για ένα επιτυχημένο πρόγραμμα ασφάλειας, τα άτομα αυτά χρειάζονται υψηλότερο βαθμό τεχνικών γνώσεων για αποτελεσματικές πρακτικές και εφαρμογές ασφαλείας.

- *Λειτουργικοί Διαχειριστές και Χρήστες Συστήματος*

Αυτά τα άτομα χρειάζονται υψηλό βαθμό συνειδητοποίησης και εκπαίδευσης σχετικά με

την ασφάλεια σχετικά με τους ελέγχους ασφαλείας και τους κανόνες συμπεριφοράς για τα συστήματα που χρησιμοποιούν για τη διεξαγωγή επιχειρηματικών δραστηριοτήτων.

Μια ποικιλία πηγών πληροφοριών σε έναν οργανισμό μπορεί να χρησιμοποιηθεί για τον προσδιορισμό των αναγκών πληροφόρησης και κατάρτισης στον τομέα της πληροφορικής. Υπάρχουν διάφοροι τρόποι συλλογής αυτών των πληροφοριών. Παρακάτω προτείνονται τεχνικές συλλογής πληροφοριών ως ένα μέρος της αξιολόγησης των αναγκών (σύμφωνα με το NIST).

- Συνεντεύξεις με όλες τις βασικές ομάδες και οργανισμούς που εντοπίστηκαν

- Οργανωτικές έρευνες

- Επανεξέταση και αξιολόγηση του διαθέσιμου υλικού πόρων, όπως το τρέχον υλικό ενημέρωσης και κατάρτισης, τα προγράμματα κατάρτισης και οι κατάλογοι των συμμετεχόντων

- Ανάλυση των μετρήσεων που σχετίζονται με την ευαισθητοποίηση και την κατάρτιση (π.χ. το ποσοστό των χρηστών που ολοκληρώνουν την απαιτούμενη ενημερωτική συνεδρία, το ποσοστό των χρηστών με σημαντικές αρμοδιότητες στον τομέα της ασφάλειας που έχουν εκπαιδευτεί σε υλικό που αφορά συγκεκριμένο ρόλο)

- Επανεξέταση των σχεδίων ασφαλείας για συστήματα γενικής υποστήριξης και σημαντικές εφαρμογές για τον εντοπισμό των ιδιοκτητών συστημάτων και εφαρμογών και των διορισμένων αντιπροσώπων ασφαλείας

- Επανεξέταση των απογραφών συστημάτων και των βάσεων δεδομένων που περιέχουν τα αναγνωριστικά των χρηστών για τον προσδιορισμό όλων όσων έχουν πρόσβαση

- Επανεξέταση τυχόν συμπερασμάτων ή / και συστάσεων των φορέων εποπτείας (π.χ. έρευνα του Κογκρέσου, γενικός επιθεωρητής, εσωτερικός έλεγχος και πρόγραμμα εσωτερικού ελέγχου) ή ανασκοπήσεις προγράμματος σχετικά με το πρόγραμμα ασφάλειας του τμήματος πληροφορικής

- Συζητήσεις και συνεντεύξεις με τη διοίκηση, με ιδιοκτήτες συστημάτων γενικής υποστήριξης και σημαντικών εφαρμογών, καθώς και άλλου προσωπικού οργάνωσης των οποίων οι επιχειρησιακές λειτουργίες βασίζονται στην πληροφορική

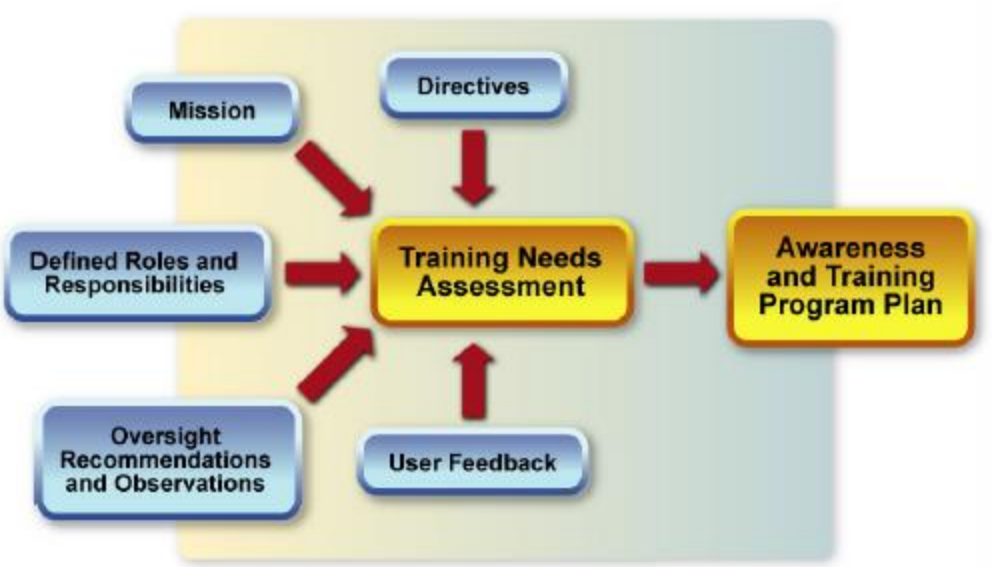
- Η ανάλυση των γεγονότων (όπως οι επιθέσεις άρνησης εξυπηρέτησης, οι παραβιάσεις ιστότοπων, η εποπτεία των συστημάτων που χρησιμοποιούνται σε επακόλουθες επιθέσεις, οι επιτυχείς επιθέσεις από ιούς) ενδέχεται να υποδηλώνουν την ανάγκη κατάρτισης (ή πρόσθετης κατάρτισης)

- Επανεξέταση κατά την πραγματοποίηση τεχνικών αλλαγών ή αλλαγών υποδομής

- Η μελέτη των τάσεων που εντοπίστηκαν για πρώτη φορά σε βιομηχανικές, ακαδημαϊκές ή κυβερνητικές εκδόσεις ή σε εκπαιδευτικούς οργανισμούς. Η χρήση αυτών των "συστημάτων έγκαιρης προειδοποίησης" μπορεί να δώσει μια εικόνα για ένα ζήτημα εντός του οργανισμού που δεν έχει ακόμη θεωρηθεί πρόβλημα.

Οι μετρήσεις είναι ένα σημαντικό και αποτελεσματικό εργαλείο που μπορεί να χρησιμοποιηθεί για να βοηθήσει στον προσδιορισμό των αναγκών πληροφόρησης και κατάρτισης ενός οργανισμού στον τομέα της πληροφορικής. Οι μετρήσεις παρακολουθούν την επίτευξη των στόχων και στόχων του προγράμματος ευαισθητοποίησης και κατάρτισης, ποσοτικοποιώντας το επίπεδο εφαρμογής της ευαισθητοποίησης και της κατάρτισης, την αποτελεσματικότητα και αποτελεσματικότητα της ευαισθητοποίησης και της κατάρτισης, αναλύοντας την επάρκεια των προσπαθειών ευαισθητοποίησης και κατάρτισης και προσδιορίζοντας πιθανές βελτιώσεις.

Το παρακάτω σχήμα απεικονίζει γενικά θέματα που αφορούν συγκεκριμένους οργανισμούς, τα οποία πρέπει να γίνουν κατανοητά κατά την έναρξη της αξιολόγησης των αναγκών. Οι τεχνικές που αναφέρθηκαν παραπάνω θα πρέπει να βοηθάνε στην κατανόηση αυτών των θεμάτων. Τα ζητήματα αυτά πρέπει να τροφοδοτούν τις απαραίτητες πληροφορίες στη διαδικασία αξιολόγησης των αναγκών. Η κατανόησή τους θα συμβάλει στη διαμόρφωση της στρατηγικής και του σχεδιασμού του προγράμματος ενημέρωσης και κατάρτισης στον τομέα της πληροφορικής.



Εικόνα 7 – Κατανόηση των γενικότερων θεμάτων του οργανισμού (πηγή: NIST)

Η ανάλυση των πληροφοριών που συλλέγονται θα πρέπει να παρέχουν απαντήσεις σε βασικές ερωτήσεις, όπως:

- Τι είδους ευαισθητοποίηση και εκπαίδευση χρειάζονται (δηλαδή, τι απαιτείται);

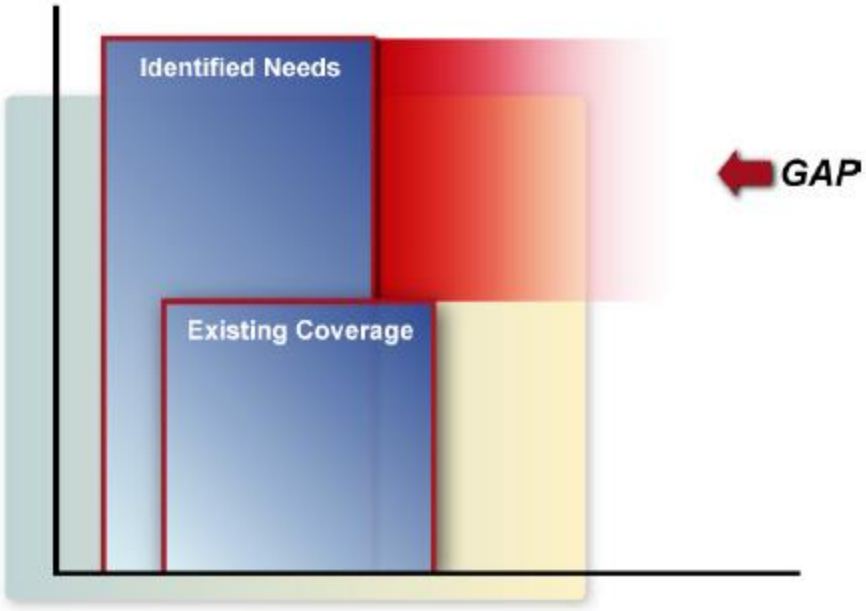
- Τι γίνεται αυτή τη στιγμή για την κάλυψη αυτών των αναγκών;

- Ποια είναι η τρέχουσα κατάσταση σχετικά με τον τρόπο αντιμετώπισης αυτών των αναγκών (δηλαδή πόσο καλά λειτουργούν οι τρέχουσες προσπάθειες);

- Πού είναι τα κενά μεταξύ των αναγκών και τι γίνεται (δηλαδή τι χρειάζεται να γίνει);

- Ποιες είναι οι πιο κρίσιμες ανάγκες;

Το παρακάτω σχήμα δείχνει τη σχέση μεταξύ των απαιτήσεων ευαισθητοποίησης και κατάρτισης και τις τρέχουσες προσπάθειες ενός οργανισμού. Η σκιασμένη περιοχή αντιπροσωπεύει τις επιπρόσθετες προσπάθειες ευαισθητοποίησης για την ασφάλεια των πληροφοριών και / ή τις προσπάθειες κατάρτισης που πρέπει να γίνουν. Η εκτίμηση των αναγκών μπορεί να συμβάλει στον εντοπισμό αυτών των πρόσθετων αναγκών - στο χάσμα μεταξύ του τι γίνεται και του τι χρειάζεται.



Εικόνα 8 – Απαιτούμενη ευαισθητοποίηση και κατάρτιση έναντι της τρέχουσας προσπάθειας

Μια άλλη σημαντική πτυχή της εκτίμησης των αναγκών είναι οι σχετικές απαιτήσεις σχετικά με την ευαισθητοποίηση και την κατάρτιση στον τομέα της πληροφορικής. Για παράδειγμα, εάν παρουσιαστεί υλικό πληροφόρησης και κατάρτισης με χρήση τεχνολογίας ηλεκτρονικής κατάρτισης (CBT), θα πρέπει να πραγματοποιηθεί τεχνική αξιολόγηση στην πλατφόρμα επεξεργασίας του οργανισμού (π.χ. τοπικό δίκτυο, σταθμοί εργασίας, κάρτες γραφικών, ομιλητές) για να αποφασιστεί αν το υπάρχον περιβάλλον θα υποστηρίξει το νέο ή διευρυμένο πρόγραμμα ευαισθητοποίησης και κατάρτισης. Ομοίως, εάν ο οργανισμός σχεδιάζει να παρέχει εκπαίδευση στην τάξη, η αξιολόγηση των αναγκών θα πρέπει να προσδιορίζει εάν υπάρχει επαρκής χώρος για ένα αποτελεσματικό μαθησιακό περιβάλλον. Μπορεί επίσης να υπάρχουν θέματα Ανθρώπινου Δυναμικού, συμπεριλαμβανομένων των εργαζομένων με αναπηρίες και ειδικών αναγκών.

Μόλις ολοκληρωθεί η αξιολόγηση των αναγκών, διατίθενται οι απαραίτητες πληροφορίες για την ανάπτυξη ενός προγράμματος ευαισθητοποίησης και κατάρτισης. Το σχέδιο πρέπει να καλύπτει ολόκληρο τον οργανισμό και να ενσωματώνει τις προτεραιότητες που προσδιορίζονται από την αξιολόγηση των αναγκών.

6.2 Καθορισμός προτεραιοτήτων

Μόλις ολοκληρωθεί η στρατηγική και το πλάνο για την ευαισθητοποίηση και την

εκπαίδευση στον τομέα της ασφάλειας, πρέπει να καθοριστεί ένα χρονοδιάγραμμα υλοποίησης. Εάν αυτό πρέπει να συμβεί σε φάσεις (π.χ. λόγω περιορισμών του προϋπολογισμού και διαθεσιμότητας πόρων), είναι σημαντικό να αποφασιστούν οι παράγοντες που θα χρησιμοποιηθούν για να αποφασιστεί τί θα προγραμματιστεί πρώτα και σε ποια σειρά. Βασικοί παράγοντες που πρέπει να λάβουμε υπόψη είναι:

- *Διαθεσιμότητα υλικού / πόρων*

Εάν είναι άμεσα διαθέσιμα το υλικό ευαισθητοποίησης και κατάρτισης και οι απαραίτητοι πόροι, οι βασικές πρωτοβουλίες στο σχέδιο μπορούν να προγραμματιστούν νωρίς. Ωστόσο, αν πρέπει να αναπτυχθεί υλικό μαθήματος ή / και οι εκπαιδευτές πρέπει να αποφασιστούν και να προγραμματιστούν, οι απαιτήσεις αυτές πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό προτεραιοτήτων.

- *Ρόλος και οργανωτικός αντίκτυπος*

Είναι πολύ συνηθισμένο να διευθετούμε την προτεραιότητα από πλευράς οργανωτικού ρόλου και κινδύνου. Οι πρωτοβουλίες ευαισθητοποίησης που απευθύνονται σε εντολές της επιχείρησης μπορούν να λάβουν υψηλή προτεραιότητα, διότι οι κανόνες καλών πρακτικών ασφαλείας μπορούν να παραδοθούν γρήγορα στο εργατικό δυναμικό. Επίσης, είναι συχνό να προσέξουμε τις θέσεις υψηλού επιπέδου εμπιστοσύνης / υψηλού αντικτύπου (π.χ. διαχειριστές προγραμμάτων ασφάλειας ΠΣ, αξιωματικοί ασφαλείας, διαχειριστές συστημάτων και διαχειριστές ασφαλείας των οποίων οι θέσεις στην οργάνωση έχουν καθοριστεί ότι έχουν μεγαλύτερη ευαισθησία) και να διασφαλίσουμε ότι λαμβάνουν υψηλή προτεραιότητα στη στρατηγική ανάπτυξης. Αυτοί οι τύποι θέσεων είναι συνήθως ανάλογοι με τον τύπο πρόσβασης (και σε ποιο σύστημα) που αυτοί οι χρήστες διαθέτουν.

- *Κατάσταση τρέχουσας συμμόρφωσης*

Περιλαμβάνει την εξέταση σημαντικών κενών στο πρόγραμμα ευαισθητοποίησης και κατάρτισης (π.χ. ανάλυσης κενών) και τη στόχευση ανεπαρκών περιοχών για έγκαιρη ανάπτυξη.

- *Κρίσιμες εξαρτήσεις έργου*

Εάν υπάρχουν σχέδια που εξαρτώνται από ένα τμήμα εκπαίδευσης για την ασφάλεια, προκειμένου να προετοιμαστούν οι απαραίτητες απαιτήσεις για το σχετικό σύστημα (π.χ.

νέο λειτουργικό σύστημα, τείχη προστασίας, εικονικά ιδιωτικά δίκτυα [VPNs]), το πρόγραμμα κατάρτισης πρέπει να διασφαλίσει ότι η εκπαίδευση πραγματοποιείται εντός του προβλεπόμενου χρονικού πλαισίου που απαιτείται για την αντιμετώπιση αυτών των εξαρτήσεων.

6.3 Χρηματοδότηση του προγράμματος ευαισθητοποίησης

Μόλις συμφωνηθεί μια στρατηγική ευαισθητοποίησης και κατάρτισης και καθοριστούν οι προτεραιότητες, πρέπει να προστεθούν στο σχέδιο και οι απαιτήσεις χρηματοδότησης. Πρέπει να προσδιοριστεί η έκταση της χρηματοδοτικής στήριξης που πρέπει να διατεθεί βάσει των όσων έχουν σχεδιαστεί. Ο CIO πρέπει να στείλει ένα σαφές μήνυμα σχετικά με τις προσδοκίες συμμόρφωσης σε αυτόν τον τομέα. Οι προσεγγίσεις που χρησιμοποιούνται για τον προσδιορισμό των πηγών χρηματοδότησης πρέπει να αντιμετωπίζονται από τους οργανισμούς βάσει του υφιστάμενου ή αναμενόμενου προϋπολογισμού και των άλλων προτεραιοτήτων του οργανισμού. Το σχέδιο ευαισθητοποίησης και κατάρτισης στον τομέα της ασφάλειας πρέπει να θεωρείται ως ένα σύνολο ελάχιστων απαιτήσεων που πρέπει να πληρούνται και οι απαιτήσεις αυτές πρέπει να μπορούν να υποστηριχθούν από έναν προϋπολογισμό ή από μια συμβατική προοπτική. Οι απαιτήσεις συμβατικής κατάρτισης θα πρέπει να καθορίζονται σε μια δεσμευτική τεκμηρίωση (π.χ. υπομνήματα κατανόησης, συμβάσεις). Οι προσεγγίσεις που χρησιμοποιούνται για να εκφράσουν την απαίτηση χρηματοδότησης μπορεί να περιλαμβάνουν:

- Ποσοστό συνολικού προϋπολογισμού κατάρτισης.

- Κατανομή ανά χρήστη ανά ρόλο (π.χ. η εκπαίδευση για το βασικό προσωπικό ασφαλείας και τους διαχειριστές συστημάτων θα είναι πιο δαπανηρή από την εκπαίδευση γενικής ασφάλειας για όσους δεν εκτελούν συγκεκριμένες λειτουργίες ασφαλείας).

- Ποσοστό συνολικού προϋπολογισμού του τμήματος πληροφορικής.

- Αναλυτικές κατανομές σε ευρώ ανά συνιστώσα με βάση το συνολικό κόστος εφαρμογής.

Προβλήματα στην εφαρμογή του σχεδίου ευαισθητοποίησης και κατάρτισης στον τομέα της ασφάλειας μπορεί να προκύψουν όταν οι πρωτοβουλίες για την ευαισθητοποίηση και την κατάρτιση στον τομέα της ασφάλειας θεωρούνται ότι έχουν χαμηλότερη προτεραιότητα από ό, τι άλλες πρωτοβουλίες οργανισμών. Είναι ευθύνη του CIO να

αξιολογεί τις ανταγωνιστικές προτεραιότητες και να αναπτύσσει μια στρατηγική για την αντιμετώπιση κάθε έλλειψης χρηματοδότησης που μπορεί να επηρεάσει την ικανότητα του οργανισμού να συμμορφώνεται με τις υφιστάμενες απαιτήσεις εκπαίδευσης στον τομέα της ασφάλειας. Αυτό μπορεί να σημαίνει προσαρμογή της στρατηγικής ευαισθητοποίησης και κατάρτισης ώστε να συμβαδίζει περισσότερο με τον διαθέσιμο προϋπολογισμό, να ασκεί πιέσεις για πρόσθετη χρηματοδότηση ή να κατευθύνει την ανακατανομή των τρεχόντων πόρων. Μπορεί επίσης να σημαίνει ότι το σχέδιο υλοποίησης μπορεί να εφαρμοστεί σταδιακά σε κάποια προκαθορισμένη χρονική περίοδο μέχρι η απαιτούμενη χρηματοδότηση να είναι διαθέσιμη.

7. Ανάπτυξη υλικού ευαισθητοποίησης και κατάρτισης

Μόλις σχεδιαστεί το πρόγραμμα ευαισθητοποίησης και κατάρτισης, μπορεί να αναπτυχθεί το υλικό υποστήριξης. Το υλικό πρέπει να αναπτυχθεί λαμβάνοντας υπόψη τα ακόλουθα:

- "Ποια συμπεριφορά θέλουμε να ενισχύσουμε;" (ευαισθητοποίηση)

- "Ποιες δεξιότητες θέλουμε να μάθει και να εφαρμόσει το κοινό;" (εκπαίδευση)

Και στις δύο περιπτώσεις, πρέπει να δοθεί έμφαση σε συγκεκριμένο υλικό το οποίο οι συμμετέχοντες πρέπει να ενσωματώσουν στις δουλειές τους. Οι συμμετέχοντες θα δώσουν προσοχή και θα ενσωματώσουν αυτό που βλέπουν ή ακούνε σε μια συνεδρία εάν αισθάνονται ότι το υλικό αναπτύχθηκε ειδικά για αυτούς. Οποιαδήποτε παρουσίαση είναι απρόσωπη και τόσο γενική ώστε να μπορεί να προσαρμοστεί για οποιοδήποτε κοινό θα αντιμετωπιστεί ως μια συνεδρία «Είμαστε εδώ επειδή πρέπει να είμαστε εδώ». Ωστόσο, ένα πρόγραμμα ενημέρωσης και κατάρτισης μπορεί να είναι αποτελεσματικό εάν το υλικό είναι ενδιαφέρον και σύγχρονο.

Σε κάποιο σημείο θα τεθεί το ερώτημα: "Αναπτύσσω υλικό ευαισθητοποίησης ή κατάρτισης;". Γενικά, δεδομένου ότι ο στόχος του υλικού ευαισθητοποίησης είναι απλώς να εστιάσει την προσοχή στις ορθές πρακτικές ασφαλείας, το μήνυμα που στέλνει η προσπάθεια ευαισθητοποίησης πρέπει να είναι σύντομο και απλό. Το μήνυμα μπορεί να απευθύνεται σε ένα θέμα ή μπορεί να απευθύνεται σε διάφορα θέματα για τα οποία θα πρέπει να γνωρίζει το κοινό.

Το κοινό ευαισθητοποίησης πρέπει να περιλαμβάνει όλους τους χρήστες ενός οργανισμού. Το μήνυμα που θα διανεμηθεί μέσω ενός προγράμματος ή καμπάνια ευαισθητοποίησης θα πρέπει να γνωστοποιήσει σε όλα τα άτομα τις κοινές τους ευθύνες σχετικά με την ασφάλεια. Από την άλλη πλευρά, το μήνυμα της εκπαίδευσης μέσα σε μια τάξη απευθύνεται σε ένα συγκεκριμένο κοινό. Το μήνυμα στο εκπαιδευτικό υλικό πρέπει να περιλαμβάνει όλα όσα σχετίζονται με την ασφάλεια που πρέπει να γνωρίζουν οι συμμετέχοντες για να κάνουν τις δουλειές τους. Το εκπαιδευτικό υλικό έχει συνήθως περισσότερο βάθος σε σχέση με το υλικό που χρησιμοποιείται σε μια συνεδρία ευαισθητοποίησης.

7.1 Ανάπτυξη υλικού ευαισθητοποίησης

Το ερώτημα που πρέπει να απαντηθεί όσον αφορά την ανάπτυξη ενός υλικού για ένα ευρύ πρόγραμμα ευαισθητοποίησης ή εκστρατείας ενός οργανισμού είναι: "Τι θέλουμε να γνωρίζει το προσωπικό του οργανισμού όσον αφορά την ασφάλεια των πληροφοριακών συστημάτων;". Το σχέδιο ευαισθητοποίησης και κατάρτισης πρέπει να περιλαμβάνει κατάλογο θεμάτων. Οι πολιτικές του οργανισμού, οι αναθεωρήσεις προγραμμάτων, οι εσωτερικοί έλεγχοι, οι αξιολογήσεις του εσωτερικού ελέγχου, οι αυτοαξιολογήσεις και οι επιτόπου έλεγχοι μπορούν επίσης να εντοπίσουν πρόσθετα θέματα προς αντιμετώπιση.
Υπάρχουν διάφορες πηγές υλικού για την ευαισθητοποίηση σχετικά με την ασφάλεια που μπορούν να ενσωματωθούν σε ένα πρόγραμμα ευαισθητοποίησης. Το υλικό μπορεί να αντιμετωπίσει ένα συγκεκριμένο ζήτημα ή, σε ορισμένες περιπτώσεις, μπορεί να περιγράψει πώς να αρχίσει να αναπτύσσεται ένα ολόκληρο πρόγραμμα ευαισθητοποίησης, μια συνεδρία ή μια καμπάνια. Πηγές έγκαιρου υλικού μπορεί να περιλαμβάνουν:

- Συμβουλές ηλεκτρονικού ταχυδρομείου που εκδίδονται από ομάδες ειδήσεων που προέρχονται από τη βιομηχανία, από ακαδημαϊκά ιδρύματα ή από το γραφείο ασφαλείας του οργανισμού.

- Επαγγελματικές οργανώσεις και πωλητές

- Ηλεκτρονικές ιστοσελίδες ειδήσεων στον τομέα της ασφάλειας ηλεκτρονικών υπολογιστών

- Περιοδικά

- Συνέδρια, σεμινάρια και μαθήματα.

Το υλικό ευαισθητοποίησης μπορεί να αναπτυχθεί χρησιμοποιώντας ένα θέμα κάθε φορά ή να δημιουργηθεί συνδυάζοντας διάφορα θέματα ή μηνύματα σε μια παρουσίαση. Για παράδειγμα, μια αφίσα ή ένα σύνθημα σε ένα εργαλείο ευαισθητοποίησης θα πρέπει να περιέχει ένα θέμα, ενώ μια καθοδηγούμενη από εκπαιδευτικό ή μια παρουσίαση μέσω διαδικτύου μπορεί να περιέχει πολλά θέματα. Ανεξάρτητα από την προσέγγιση που ακολουθήθηκε, το ποσό των πληροφοριών δεν θα πρέπει να κατακλύζει το κοινό. Σύντομη αναφορά των απαιτήσεων (πολιτικών), των προβλημάτων για των οποίων σχεδιάστηκαν απαιτήσεις για την αντιμετώπιση τους και των δράσεων που πρέπει να αναληφθούν είναι

τα κύρια θέματα που πρέπει να καλυφθούν σε μια τυπική παρουσίαση για ευαισθητοποίηση.

7.2 Ανάπτυξη εκπαιδευτικού υλικού

Όπως προαναφέρθηκε, το ερώτημα που πρέπει να απαντηθεί όταν αρχίζει να αναπτύσσεται υλικό για ένα συγκεκριμένο εκπαιδευτικό μάθημα είναι: " Ποιες δεξιότητες θέλουμε να μάθει και να εφαρμόσει το κοινό;" Το σχέδιο ευαισθητοποίησης και κατάρτισης θα πρέπει να αναγνωρίσει το ακροατήριό του προκειμένου να αντιμετωπίσει τις υποχρεώσεις του στον τομέα της ασφάλειας των πληροφοριών.

Το πρώτο βήμα για τον προσδιορισμό των πηγών εκπαιδευτικού υλικού για την κατασκευή ενός κύκλου μαθημάτων είναι να αποφασιστεί εάν το υλικό θα αναπτυχθεί εσωτερικά ή θα ανατεθεί σε εξωτερικούς συνεργάτες. Στην πρώτη περίπτωση, ο οργανισμός θα πρέπει να έχει εξειδικευμένη τεχνογνωσία και να μπορεί να διαθέσει τους απαραίτητους πόρους για την ανάπτυξη εκπαιδευτικού υλικού και μαθημάτων. Τα παρακάτω ερωτήματα μπορούν να βοηθήσουν τον οργανισμό να αποφασίσει (σύμφωνα με το NIST):

- Έχουμε τους εσωτερικούς πόρους για να κάνουμε τη δουλειά; Αυτό περιλαμβάνει ανθρώπους με τις κατάλληλες δεξιότητες και αρκετούς ανθρώπους για να κάνουν τη δουλειά.

- Είναι πιο αποδοτικό από πλευράς κόστους η ανάπτυξη του υλικού μέσα από την εξωτερική ανάθεση;

- Υπάρχει μηχανισμός χρηματοδότησης (προϋπολογισμός);

- Έχουμε κάποιον στο προσωπικό που μπορεί να λειτουργήσει ως τεχνικός εκπρόσωπος του εξωτερικού συνεργάτη και να παρακολουθεί αποτελεσματικά τη δραστηριότητα του;

- Διαθέτει ο οργανισμός τους αναγκαίους πόρους (π.χ. χρηματοδότηση και προσωπικό με την απαιτούμενη τεχνογνωσία) για τη διατήρηση του υλικού, εάν αναπτύσσεται από έναν εξωτερικό συνεργάτη;

- Η ευαισθησία του περιεχομένου του μαθήματος αποκλείει τη χρήση ενός εξωτερικού συνεργάτη;

- Μπορεί η εξωτερική ανάθεση να καλύψει τα κρίσιμα προγράμματα κατάρτισης;

Αν ο οργανισμός αποφασίσει να αναθέσει σε τρίτους την ανάπτυξη του εκπαιδευτικού του προγράμματος, υπάρχουν διάφοροι πωλητές που προσφέρουν μαθήματα κατάλληλα για συγκεκριμένο κοινό ή που μπορούν να αναπτυχθούν για συγκεκριμένο κοινό. Πριν από την επιλογή ενός συγκεκριμένου πωλητή, οι οργανισμοί θα πρέπει να έχουν πλήρη γνώση των εκπαιδευτικών αναγκών τους και να είναι σε θέση να προσδιορίσουν αν το υλικό του υποψήφιου πωλητή ανταποκρίνεται στις ανάγκες τους.

Μεγιστοποίηση των συνεργασιών: Οι οργανισμοί έχουν περισσότερες επιλογές από τις οποίες μπορούν να επιλέξουν από το να αποφασίσουν απλώς εάν θα αναπτύξουν υλικό μαθημάτων κατάρτισης με υπάρχοντες πόρους ή θα το αναθέσουν σε τρίτους. Οι οργανισμοί μπορούν να δημιουργήσουν (ή να μεγιστοποιήσουν τις υπάρχουσες) εταιρικές σχέσεις με άλλους οργανισμούς για να αναπτύξουν υλικό ή να συντονίσουν εκπαιδευτικά γεγονότα που ανταποκρίνονται στις ανάγκες τους σε κατάρτιση σε θέματα ασφάλειας. Για παράδειγμα, διάφοροι οργανισμοί μπορούν να συνδυάζουν πόρους και εμπειρογνωμοσύνη και να αναπτύσσουν ένα εκπαιδευτικό μάθημα για ένα συγκεκριμένο κοινό. Εάν το συγκεκριμένο υλικό του οργανισμού περιλαμβάνεται και περιορίζεται σε μία μόνο ενότητα στο μάθημα, όλες οι εμπλεκόμενες υπηρεσίες μπορούν να χρησιμοποιήσουν το μεγαλύτερο μέρος του υλικού που αναπτύχθηκε. Οι οργανισμοί θα πρέπει στη συνέχεια να τροποποιήσουν ή να προσαρμόσουν μόνο την ενότητα που περιέχει το συγκεκριμένο υλικό της υπηρεσίας.

Ομοίως, ένας οργανισμός μπορεί να διοργανώσει μια ημέρα ασφάλειας ή μια ετήσια ή περιφερειακή διάσκεψη και να ανακοινώσει ότι θα είναι ανοιχτή στο προσωπικό άλλων οργανισμών. Ενώ το υλικό που παρουσιάζεται ενδέχεται να μην ταιριάζει ακριβώς με αυτό που απαιτείται και από τις δύο υπηρεσίες, μπορεί να είναι ένας αρκετά φθηνός τρόπος για να ικανοποιήσει κάποιες από τις εκπαιδευτικές ανάγκες συγκεκριμένου ακροατηρίου. Εάν γίνει μια τέτοια συμφωνία, πρέπει να δημιουργηθεί μια διαδικασία που θα επιτρέπει σε κάθε συμμετέχοντα οργανισμό να παρακολουθεί τη συμμετοχή, να διασφαλίζει την εφαρμογή του εκπαιδευτικού υλικού, να καθορίζει την ευθύνη και να αντιμετωπίζει άλλα διοικητικά και διαχειριστικά ζητήματα.

Οι οργανισμοί μπορούν να διερευνήσουν τη χρήση εκπαιδευτικού υλικού που έχει

αναπτυχθεί από άλλους οργανισμούς και το οποίο μπορεί να εκδοθεί χωρίς κόστος προκειμένου να μην χρειαστεί η ανάπτυξη ενός εντελώς καινούργιου μαθήματος. Θα πρέπει να ληφθεί μέριμνα ώστε το διαθέσιμο υλικό να ενδιαφέρει το κοινό που στοχεύει και να διδάσκει στους υποψήφιους το τι θα πρέπει να γνωρίζουν για να ικανοποιήσουν τις ευθύνες τους στον τομέα της ασφάλειας.

Μέσα σε έναν οργανισμό, οι διαχειριστές του προγράμματος ασφάλειας μπορούν να δημιουργήσουν νέες εταιρικές σχέσεις ή να ενισχύσουν υπάρχουσες συνεργασίες με την εκπαιδευτική λειτουργία του οργανισμού ή με λειτουργικούς διαχειριστές που συντονίζουν ή διεξάγουν τη δική τους εκπαίδευση. Η λειτουργική κατάρτιση που αναπτύσσεται στο εσωτερικό της επιχείρησης (π.χ. χρηματοοικονομικές εφαρμογές, διαχείριση προσωπικού) συχνά στερείται επαρκούς συζήτησης σχετικά με θέματα ασφάλειας της πληροφορικής. Μέσω μιας εταιρικής σχέσης, ο διαχειριστής του προγράμματος ασφάλειας μπορεί να προτείνει την αναθεώρηση των υφιστάμενων αναφορών σχετικά με την ασφάλεια στο εκπαιδευτικό υλικό, ελέγχοντας την πληρότητα και την ακρίβεια. Ο διαχειριστής του προγράμματος ασφάλειας μπορεί επίσης να βοηθήσει τον εκπαιδευτή ή τον λειτουργικό διαχειριστή να αναπτύξει μια ενότητα ασφαλείας για το λειτουργικό υλικό εκείνο που δεν διαθέτει ήδη περιεχόμενο σχετικό με την ασφάλεια. Ο διαχειριστής του προγράμματος ασφάλειας μπορεί επίσης να αναθεωρήσει τις προδιαγραφές της σύμβασης για την ανάπτυξη της λειτουργικής κατάρτισης που θα ανατεθεί σε εξωτερικούς συνεργάτες, διασφαλίζοντας ότι τα κατάλληλα ζητήματα ασφάλειας αντιμετωπίζονται με επαρκή λεπτομέρεια και πολυπλοκότητα για το συγκεκριμένο κοινό.

8. Βέλτιστες πρακτικές

Στο παρόν κεφάλαιο αναλύονται κάποιες βέλτιστες πρακτικές που πρέπει να λάβει κανείς υπόψη για την ανάπτυξη ενός προγράμματος ευαισθητοποίησης σχετικό με την ασφάλεια που θα αλλάξει πραγματικά τη συμπεριφορά των εργαζομένων και θα κάνει λιγότερο πιθανό ο οργανισμός να πέσει θύμα επίθεσης.

- *Η ασφάλεια πρέπει να αποτελεί διοικητικό θέμα*

Η εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια πρέπει να είναι σε επίπεδο διοικητικού συμβουλίου για να λάβει την προσοχή που της αξίζει. Σε έναν αυξανόμενο αριθμό οργανώσεων, η ασφάλεια παίρνει πολύ περισσότερη προσοχή από τα διοικητικά συμβούλια. Οι CISOs και παρόμοιες θέσεις σε επίπεδο διευθυντών προσχωρούν σε διοικητικά συμβούλια προκειμένου τα μέλη να έχουν επίγνωση των ζητημάτων ασφάλειας και των εταιρικών κινδύνων στη μη συμμόρφωση. Διευθυντές που παίρνουν σοβαρά την ασφάλεια και της δίνουν την προτεραιότητα που της αξίζει θα προχωρήσουν σε μεγάλο βαθμό προς την ενίσχυση του προγράμματος εκπαίδευσης σε θέματα ασφάλειας σε έναν οργανισμό.

- *Κατανόηση του εταιρικού πολιτισμού*

Είναι σημαντικό να καταλάβουμε ότι δεν είναι εξίσου ευνοϊκές για όλους τους εταιρικούς πολιτισμούς η έννοια της κατάρτισης ευαισθητοποίησης σχετικά με την ασφάλεια. Η διαχείριση ορισμένων οργανισμών, ιδίως εκείνων που δεν ασχολούνται με την πληροφορική, δεν είναι ανοικτή στην ιδέα της κατάρτισης για την ευαισθητοποίηση σχετικά με την ασφάλεια κι έτσι δεν θα την υποστηρίξουν ούτε θα την χρηματοδοτήσουν στο βαθμό που θα έπρεπε. Ως επακόλουθο της ιδέας ότι τα διοικητικά συμβούλια θα πρέπει να επικεντρωθούν στην ασφάλεια, έτσι θα πρέπει και τα διευθυντικά στελέχη προκειμένου η κατάρτιση να υποστηριχθεί και να της δοθεί η ευκαιρία να αναπτυχθεί. Εν συντομία, κερδίζοντας την εμπιστοσύνη της διοίκησης για τη χρηματοδότηση και την ενθάρρυνση της κατάρτισης ευαισθητοποίησης ασφαλείας θα έχει ουσιαστική σημασία για την προώθηση όχι μόνο καλών προγραμμάτων κατάρτισης στον τομέα της ασφάλειας, αλλά και για τη δημιουργία μιας εταιρικής κουλτούρας στην οποία αποτιμάται η ασφάλεια.

Ένα ουσιαστικό στοιχείο για να διασφαλιστεί ότι η εταιρική κουλτούρα θα στηρίξει την κατάρτιση ευαισθητοποίησης ασφάλειας και τις βέλτιστες πρακτικές ασφαλείας

καθορίζουν εάν οι διαχειριστές εταιρειών είναι ανοικτοί στην ιδέα να αμφισβητηθούν. Για παράδειγμα, εάν ένας CEO απαιτεί ότι οι εντολές του γίνονται χωρίς αμφιβολία, τότε ο CFO ο οποίος λαμβάνει ένα spearphishing στο ηλεκτρονικό του ταχυδρομείο, κατά πάσα πιθανότητα από τον Διευθύνοντα Σύμβουλο, απαιτώντας να γίνει μεταφορά μέσω τραπεζικού λογαριασμού σε ένα προμηθευτή της εταιρείας, πιθανότατα θα φοβάται να αμφισβητήσει την εγκυρότητα αυτού του email. Μια υγιής εταιρική κουλτούρα που υποστηρίζει μια υγιής κουλτούρα ασφάλειας δεν θα επιτρέψει αυτό το είδος του "φόβου".

- *Βεβαιωθείτε ότι η εκπαίδευση καλύπτει όλες τις βάσεις*

Φυσικά, η κατάρτιση για την ευαισθητοποίηση σχετικά με την ασφάλεια πρέπει να ξεκινήσει με την εστίαση σχετικά με τις πιο κοινές απειλές, όπως οι προσπάθειες ηλεκτρονικού ψαρέματος από ηλεκτρονικές διευθύνσεις που υποτίθεται προέρχονται από τις τράπεζες των εργαζομένων ή από τον διαχειριστή ηλεκτρονικού ταχυδρομείου. Ωστόσο, η εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια πρέπει επίσης να επικεντρώνεται σε λιγότερο κοινούς φορείς απειλής, όπως π.χ. το spearphishing που απευθύνεται σε ανώτερα στελέχη και την κοινοποίηση σε κοινωνικά μέσα δικτύωσης που μπορούν να αποκαλύψουν ευαίσθητες εταιρικές πληροφορίες. Όσον αφορά το τελευταίο, η υπερβολική κοινοποίηση πληροφοριών στα κοινωνικά μέσα δικτύωσης σχετικά με μέλη της οικογένειας, προσωπικές ιστορίες, αγαπημένα εστιατόρια, επαγγελματικά ταξίδια κτλ μπορούν να διευκολύνουν τους κυβερνοεγκληματίες να μαντέψουν κωδικούς πρόσβασης ή να σκαρφιστούν μηνύματα που θα τους επιτρέψουν να εισέλθουν σε εταιρικά emails και άλλους λογαριασμούς.

- *Βεβαιωθείτε ότι οι δοκιμές ηλεκτρονικού εγκλήματος είναι τυχαίες*

Είναι απαραίτητο να βεβαιωθείτε ότι το phishing και άλλες δοκιμές σχετικές με την εκπαίδευση είναι πραγματικά τυχαίες. Ένα πρόγραμμα ελέγχου των εργαζομένων που διεξάγει τακτικά έλεγχο στο καθορισμένο χρονοδιάγραμμα θα αναγνωρίζεται ευκολότερα από τους υπαλλήλους ως δοκιμή ηλεκτρονικού ψαρέματος και θα προκαλέσει συμπεριφορές που δεν είναι αντιπροσωπευτικές των πραγματικών απειλών που αντιμετωπίζουν οι εργαζόμενοι.

- *Η εκπαιδευση πρέπει να γίνεται με επαρκή συχνότητα*

Όπως προαναφέρθηκε και σε προηγούμενο κεφάλαιο η συχνότητα εκπαίδευσης πρέπει να

γίνεται όσες φορές χρειαστεί μέσα στο έτος προκειμένου να βεβαιωθεί ότι οι εργαζόμενοι είναι ευαισθητοποιημένοι με ότι αφορά την ασφάλεια. Η συχνότητα εκπαίδευσης μπορεί να καθοριστεί από την εταιρεία, από τους υπεύθυνους ασφαλείας ή ακόμα κι από τους ίδιους τους εργαζομένους σε περίπτωση που δεν νιώθουν σιγουριά.

- *Διαχωρισμός εκπαίδευσης σε ειδικές ομάδες*

Ενώ όλοι οι εργαζόμενοι είναι πιθανά θύματα εγκληματικότητας στον κυβερνοχώρο και μπορούν να χρησιμεύσουν ως αγωγός των εγκληματιών να διεισδύσουν σε έναν οργανισμό, ορισμένοι χρήστες είναι στόχοι υψηλότερης αξίας από ό, τι οι υπόλοιποι. Για παράδειγμα, ο CFO μιας εταιρείας είναι πιο πιθανό να είναι ο στόχος μιας συντονισμένης και εστιασμένης εκστρατείας πειρατείας σε σχέση με κάποιον που δεν έχει πρόσβαση σε εταιρικούς χρηματοοικονομικούς λογαριασμούς. Κατά συνέπεια, είναι λογικό να εξεταστεί η παροχή πρόσθετης εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια για ορισμένα άτομα. Σύμφωνα με έρευνα που διεξήχθη (Osterman Research Inc, 2018) διαπιστώθηκε ότι τα τμήματα πληροφορικής, τα ανώτερα στελέχη και τα χρηματοοικονομικά ήταν οι τρεις πιο πιθανές ομάδες να λάβουν ενισχυμένη εκπαίδευση.

- *Δημιουργία καλής «πριν και μετά» εικόνας*

Πριν από την εφαρμογή ενός προγράμματος εκπαίδευσης για την ευαισθητοποίηση σχετικά με την ασφάλεια, είναι χρήσιμο να καταστεί γνωστό το επίπεδο συνειδητοποίησης. Η δημιουργία αυτής της εικόνας "πριν" αποτελεί βασικό στοιχείο κατανοώντας πόσο αποτελεσματική είναι η κατάρτιση με την πάροδο του χρόνου.

- *Συνδιασμός εκπαίδευσης και δοκιμών*

Είναι σημαντικό να συνδεθεί η κατάρτιση ευαισθητοποίησης σχετικά με την ασφάλεια με δοκιμές σε βασικά θέματα, όπως η ανίχνευση ηλεκτρονικού ψαρέματος Για παράδειγμα, ένας εργαζόμενος που αποτυγχάνει σε μια δοκιμή phishing θα πρέπει να δεχτεί πρόσθετη κι ευαίσθητη από πλευράς περιβάλλοντος εκπαίδευσης, με στόχο την αντιμετώπιση των ελλείψεων που αποκαλύφθηκαν στη δοκιμή.

- *Δημιουργία εναλλακτικών διαβιβάσεων*

Είναι σημαντικό για όλους τους υπαλλήλους να έχουν μια κατάλληλη εναλλακτική επικοινωνία για τον έλεγχο των αμφισβητήσιμων αιτημάτων που λαμβάνονται μέσω ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, ένας CFO ο οποίος λαμβάνει ένα αίτημα

του Διευθύνοντος Συμβούλου να πραγματοποιήσει τραπεζική μεταφορά, υπό ασυνήθιστες περιστάσεις, πρέπει να διαθέτει μια μέθοδο επαλήθευσης αυτού του αιτήματος ανεξάρτητα από το κανάλι που χρησιμοποιήθηκε για την υποβολή του αιτήματος.

- *Εστίαση σε εναλλαγή συμπεριφοράς*

Η κατάρτιση για την ευαισθητοποίηση σχετικά με την ασφάλεια αφορά την εναλλαγή συμπεριφοράς. Βοηθώντας τους χρήστες να είναι πιο επιφυλακτικοί και λιγότερο ευάλωτοι στις προσπάθειες των εγκληματιών του κυβερνοχώρου να τους ξεγελάσουν, καθίσταται λιγότερο πιθανό να μοιραστούν πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν από τους κυβερνοεγκληματίες στην δημιουργία προσαρμοσμένων μηνυμάτων, υπάρχει μεγαλύτερη προσοχή σχετικά με το άνοιγμα συνημμένων, πραγματοποιείται συχνότερη επαλήθευση των αποστολέων μηνυμάτων ηλεκτρονικού ταχυδρομείου κ.ο.κ. Ο στόχος της εκπαίδευσης πρέπει τελικά να βελτιώσει τη συμπεριφορά των υπαλλήλων που έχουν πιθανότητα υπονόμευσης της ασφάλειας που παρέχει η ασφάλεια του οργανισμού υποδομή.

- *Ευχάριστο κλίμα εκπαίδευσης*

Η εκπαίδευση ευαισθητοποίησης για την ασφάλεια που δεν είναι διασκεδαστική ή τουλάχιστον ευχάριστη για τους υπαλλήλους θα είναι πιθανότατα αναποτελεσματική. Ενώ η διαπαιδαγώγηση της διαδικασίας κατάρτισης δεν είναι και απόλυτη απαίτηση για ένα πρόγραμμα εκπαίδευσης, θα πρέπει να είναι ενδιαφέρουσα και αρκετά ελκυστική για να κρατήσει το ενδιαφέρον των χρηστών και να τους κάνει πρόθυμους να συμμετάσχουν στους στόχους του προγράμματος.

- *Ελαστικότητα στα λάθη*

Μια από τις βασικές βέλτιστες πρακτικές που θα πρέπει να ακολουθήσει οποιοσδήποτε οργανισμός ως μέρος οποιουδήποτε εκπαιδευτικού προγράμματος ευαισθητοποίησης σχετικά με την ασφάλεια δεν είναι να τιμωρεί τα λάθη που κάνουν οι χρήστες, είτε πρόκειται για λάθη που έγιναν κατά τη διάρκεια δοκιμών, είτε για λήψη πραγματικού κακόβουλου περιεχομένου. Αν οι εργαζόμενοι δεν είναι ελεύθεροι να κάνουν λάθη και να μοιράζονται ανοιχτά την εμπειρία τους με τις ομάδες ασφαλείας και τους συνομηλίκους τους, δεν θα συμμετάσχουν στη διαδικασία. Φυσικά, ένας εργαζόμενος που συνεχίζει να κάνει κλικ σε κακόβουλους ιστότοπους και ποτέ δεν βελτιώνει τη συμπεριφορά του μπορεί

να χρειαστεί περισσότερη προσοχή, αλλά η τιμωρία, αν τελικά εφαρμοστεί, πρέπει να είναι η τελευταία λύση. [14]

9. Εμπόδια στην εκπαίδευση προσωπικού

Η ανάπτυξη κι η εφαρμογή ενός προγράμματος ευαισθητοποίησης του προσωπικού σχετικό με την ασφάλεια πληροφοριακών συστημάτων μπορεί να ελλοχεύει κάποια εμπόδια. Οι δημοσιονομικοί περιορισμοί, ο κακός σχεδιασμός, η έλλειψη στήριξης σε εκτελεστικό επίπεδο κι η θεμελιώδους σημασίας παρεξήγηση των σημαντικών ζητημάτων μπορεί μεμονωμένα και συλλογικά να καταστρέψουν κάθε καμπάνια που δεν καταφέρνει να αντιμετωπίσει αυτά τα θέματα. Ο σωστός σχεδιασμός και η εκτέλεση είναι κρίσιμοι παράγοντες επιτυχίας, όπως συμβαίνει σε οποιοδήποτε έργο. Δεν υπάρχει τίποτα το ασήμαντο πραγματοποιώντας ένα αποτελεσματικό πρόγραμμα συνειδητοποίησης της ασφάλειας των πληροφοριών. Είναι μια σημαντική επιχείρηση και πρέπει να αναγνωρίζεται ως τέτοια από την αρχή. Στις παραγράφους που ακολουθούν θα γίνει μια προσπάθεια προσδιορισμού των μεγάλων δυσκολιών που μπορεί να αντιμετωπίσει κανείς.

- *Αδιαφορία κι άγνοια*

Οι επαγγελματίες ασφάλειας πληροφοριών, πρέπει να κάνουν τους υπαλλήλους να ανησυχούν για τις βέλτιστες πρακτικές σχετικά με την ασφάλεια. Πριν μπορέσει κανείς να αντιμετωπίσει την άγνοια, πρέπει πρώτα να προσέξει την αδιαφορία. Οι εργαζόμενοι δεν θα έχουν κίνητρο να αλλάξουν συμπεριφορά εάν δεν βλέπουν κανένα λόγο να το κάνουν. Ετσι το πρώτο καθήκον του υπεύθυνου του προγράμματος είναι η ανύψωση της ευαισθητοποιήσης του προσωπικού καθώς και να το πείσει ότι έχει προσωπική συμμετοχή στην προσπάθεια εξασφάλισης των πληροφοριακών αγαθών του οργανισμού. Πολλοί επαγγελματίες ασφαλείας κάνουν το λάθος να βλέπουν το το ζήτημα της επίγνωσης της ασφάλειας ως ένα τεχνικό πρόβλημα. Η επίγνωση της ασφάλειας δεν είναι στην πραγματικότητα εκπαίδευση. Είναι η αύξηση της συνείδησης, στο πλαίσιο της οργάνωσης, των απειλών της, στην ευημερία και στον ρόλο που διαδραματίζουν οι εργαζόμενοι στην αντιμετώπιση αυτών των απειλών.

Σύμφωνα με την Shirley Pane (Developing Security Education and Awareness Programs) οι ακόλουθες συμπεριφορές μεταξύ των εργαζομένων εμποδίζουν την ανάπτυξη καλών πρακτικών ασφαλείας:

- Έλλειψη κατανόησης της φύσης των απειλών ασφάλειας
- Η μη θεώρηση ως κάτι σημαντικό

- Η μεταφορά ευθύνης σε κάποιον άλλο
- Η απαγόρευση οποιασδήποτε προσωπικής ευθύνης για την ασφάλεια
- Η εξέταση του θέματος ως πολύ τεχνικό

Μια προσεκτική εξέταση αυτών θα αποκαλύψει ότι είναι συγγενικά. Η έλλειψη κατανόησης της φύσης της απειλής θα μπορούσε εύκολα να οδηγήσει κάποιον στην πεποίθηση ότι το ζήτημα είναι τεχνικά πέραν της αρμοδιότητάς του. Η άρνηση της προσωπικής ευθύνης συμβάλλει στην πεποίθηση ότι είναι δουλειά κάποιου άλλου ή ότι είναι ελάχιστα ή καθόλου σημαντική. Ολα αυτά πρέπει να λαμβάνονται υπόψη κατά το σχεδιασμό που αποσκοπεί στην αντιμετώπιση αυτών των παραδοχών. Η προώθηση ορθών πρακτικών ασφαλείας μπορεί να πραγματοποιηθεί μόνο μετά την αντιμετώπιση αυτών των αρνητικών συμπεριφορών.

- *Εκτελεστικό επίπεδο αγοράς*

Η έγκριση κι η υποστήριξη του εκτελεστικού επιπέδου είναι ζωτικής σημασίας για την επιτυχία του προγράμματος. Πρέπει να πείσετε το αφεντικό σας ότι η προσπάθεια θα αξίζει τα έξοδα και την εκτελεστική υποστήριξη ότι χάρη στο παράδειγμα και στην αρχή τους, θα μεταφέρουν το μήνυμα στο προσωπικό ότι αυτό είναι κάτι το σημαντικό κι απαιτεί την προσοχή τους. Ξεκινήστε την εκστρατεία στο υψηλότερο δυνατό επίπεδο. Ξεκινήστε την εκδήλωσή σας με ένα email από τον Πρόεδρο ή τον Διευθύνοντα Σύμβουλο. Κατά προτίμηση, έχετε πολλά μέλη του εκτελεστικού γραφείου να επικυρώσουν τις προσπάθειες σας όταν ξεκινά το πρόγραμμα. Η εκτελεστική έγκριση μπορεί να αποδόσει τεράστια οφέλη κι αξίζει κάθε προσπάθεια από την πλευρά σας να το καλλιεργήσετε. Η έλλειψη εκτελεστικής υποστήριξης θα παρεμποδίσει ακόμα και την πιο καλή στο μάτι εκστρατεία. Όσο ελκυστικό κι αν είναι το υλικό, οι υπάλληλοι θα αμφισβητήσουν κατά πόσο το μήνυμα προορίζεται για αυτούς.

- *Χρήματα και κακοσχεδιασμός*

Ένα αποτελεσματικό εκπαιδευτικό πρόγραμμα απαιτεί επαρκή χρηματοδότηση. Πόσο είναι αρκετό προκειμένου να βοηθήσει να φανεί η προσπάθεια ως μια εκστρατεία δημοσίων σχέσεων, ανάλογη με την προώθηση ενός προϊόντος ή με καλές πρακτικές δημόσιας υγείας.

Ξεκινάμε προσανατολισμένοι στην τέχνη. Η αξία ενός επαγγελματία καλλιτεχνικού

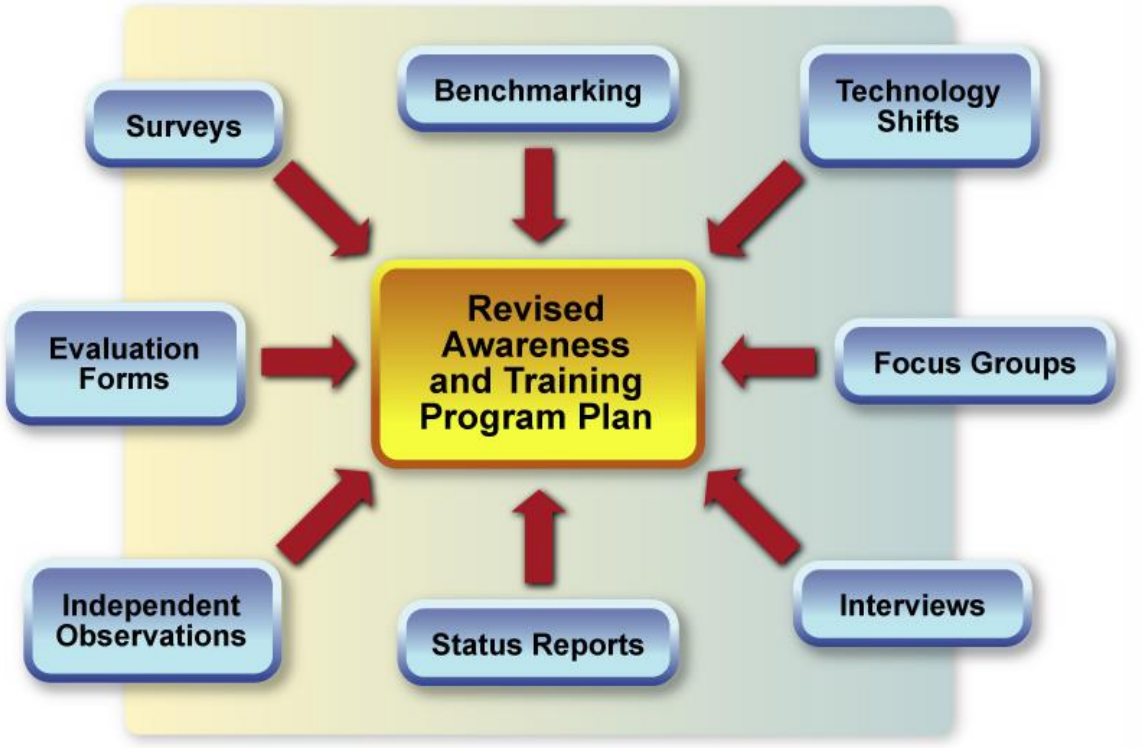
διευθυντή και διευθυντή δημοσίων σχέσεων δεν θα πρέπει να υποτιμηθεί. Όχι μόνο θα σχεδιάσουν αποτελεσματικά κι εντυπωσιακά κομμάτια, μπορούν επίσης να προσφέρουν ανεκτίμητη καθοδήγηση σχετικά με το γενικό τόξο της εκστρατείας, μπορούν να διαχειριστούν τη διαδικασία παραγωγής και μπορούν να παρέχουν αξιόπιστες εκτιμήσεις για τα πιθανά κόστη.

Κανείς δεν θα ήθελε έναν ερασιτέχνη να ρυθμίσει το τείχος προστασίας ενός οργανισμού. Ομοίως, κανείς δεν θα ήθελε ένα άτομο που δεν έχει πείρα στην εκτέλεση μιας καμπάνιας δημοσίων σχέσεων να σχεδιάσει το πρόγραμμά για την ευαισθητοποίηση της ασφάλειας. Η πηγή των πολύτιμων πληροφοριών και της διορατικότητας στη δημιουργία του προγράμματος μπορεί να είναι ο επαγγελματίας σε θέματα ασφαλείας, αλλά χρειάζεται κι ένας επαγγελματίας για να μεταφράσει αυτή τη γνώση σε μια αποτελεσματική εκστρατεία. Ένα πρόγραμμα συνειδητοποίησης της ασφάλειας δεν πρέπει να αντιμετωπίζεται λιγότερο σκόπιμα κι ευσυνείδητα από άλλες προσπάθειες που εξασφαλίζουν τα πληροφοριακά αγαθά του οργανισμού. Σε αντίθεση με άλλες μορφές ελέγχων, ωστόσο, η εμπειρογνωμοσύνη στην τοποθέτηση μιας αποτελεσματικής εκστρατείας δημοσίων σχέσεων θα βρίσκεται πιθανώς εκτός του γραφείου που χρεώνεται με την ασφάλεια πληροφοριών.

Είναι σημαντικό να βγάζετε έναν ρεαλιστικό προϋπολογισμό πριν μεταβείτε στο προϊστάμενό σας για έγκριση. Όπως και σε κάθε άλλο έργου, θα πρέπει να προσδιορίσετε πρώτα όλες τις πιθανές δαπάνες προκειμένου να καλυφθεί το κόστος της εκστρατείας και να αποφευχθεί η αμηχανία της υπέρβασης του προϋπολογισμού. Θα πρέπει πιθανώς να δώσετε στον προϊστάμενό σας μια σειρά από επιλογές προϋπολογισμού. Πάλι, επαγγελματίες άνθρωποι σχετικοί με τις δημόσιες σχέσεις μπορούν να βοηθήσουν στην παρουσίαση αυτών των αριθμών. [15]

10. Αξιολόγηση και ανάδραση

Οι τυπικοί μηχανισμοί αξιολόγησης και ανάδρασης αποτελούν κρίσιμα στοιχεία κάθε προγράμματος ευαισθητοποίησης και εκπαίδευσης. Η συνεχής βελτίωση δεν μπορεί να συμβεί χωρίς μια καλή αίσθηση του τρόπου με τον οποίο λειτουργεί το υπάρχον πρόγραμμα. Επιπλέον, ο μηχανισμός ανάδρασης πρέπει να σχεδιαστεί έτσι ώστε να ανταποκρίνεται στους στόχους που καθορίστηκαν αρχικά για το πρόγραμμα. Μόλις στερεοποιηθούν οι βασικές απαιτήσεις, μπορεί να σχεδιαστεί και να εφαρμοστεί μια στρατηγική ανάδρασης.



Εικόνα 9 - Μηχανισμοί αξιολόγησης και ανάδρασης ενός προγράμματος ευαισθητοποίησης (σύμφωνα με το NIST)

Μια στρατηγική ανατροφοδότησης πρέπει να ενσωματώνει στοιχεία που θα αφορούν την ποιότητα, το πεδίο εφαρμογής, τη μέθοδο ανάπτυξης (π.χ. web-based, onsite, offsite), το επίπεδο δυσκολίας, την ευκολία χρήσης, τη διάρκεια της συνεδρίας, τη συνάφεια καθώς και προτάσεις τροποποίησης.

Πολλές μέθοδοι μπορούν να εφαρμοστούν για να ζητήσουν ανατροφοδότηση. Οι πιο συνηθισμένες περιλαμβάνουν:

- *Έντυπα αξιολόγησης / ερωτηματολόγια*

Μπορούν να χρησιμοποιηθούν ποικίλες μορφές. Τα καλύτερα σχέδια εξαλείφουν την ανάγκη για πολλή γραφή από την πλευρά του ατόμου που τα συμπληρώνει. Το κλειδί είναι να σχεδιαστούν οι φόρμες ώστε να είναι όσο το δυνατόν φιλικότερες προς το χρήστη. Εργαστείτε με τους εσωτερικούς εμπειρογνώμονες που είναι εξοικειωμένοι με τις καλύτερες τεχνικές για το σχεδιασμό αυτών των εργαλείων αξιολόγησης ή αναζητήστε τη βοήθεια εξωτερικών εμπειρογνωμόνων.

- *Ομάδες εστίασης*

Πραγματοποιήστε μαθήματα ευαισθητοποίησης με κάποιους από τους εκπαιδευόμενους σε ανοικτά φόρουμ προκειμένου να γίνει συζήτηση των προοπτικών τους σχετικά με την αποτελεσματικότητα του προγράμματος κατάρτισης στον τομέα της ασφάλειας και ζητήστε τις ιδέες τους για βελτίωση.

- *Επιλεκτικές Συνεντεύξεις*

Αυτή η προσέγγιση προσδιορίζει πρώτα τις ομάδες-στόχους κατάρτισης βάσει των επιπτώσεων, των προτεραιοτήτων ή άλλων καθιερωμένων κριτηρίων και προσδιορίζει συγκεκριμένους τομείς για ανατροφοδότηση. Συνήθως διεξάγονται συνεντεύξεις ενός προς ένα ή σε μικρές ομοιογενείς ομάδες (συνήθως δέκα ή λιγότερες), αυτή η προσέγγιση είναι περισσότερο εξατομικευμένη και ιδιωτική από την προσέγγιση της ομάδας εστίασης και μπορεί να ενθαρρύνει τους συμμετέχοντες να είναι πιο προσεκτικοί στην κριτική τους για το πρόγραμμα.

- *Ανεξάρτητη Παρατήρηση / Ανάλυση*

Μια άλλη προσέγγιση για την αναζήτηση ανατροφοδότησης είναι η ενσωμάτωση μιας ανασκόπησης του προγράμματος ευαισθητοποίησης στον χώρο της ασφάλειας ως καθήκον ενός εξωτερικού συνεργάτη ή κάποιου τρίτου στο πλαίσιο ενός ελέγχου που ξεκινάει από έναν οργανισμό. Αυτό θα συμβεί πέρα από την κανονική δραστηριότητα εποπτείας για να ληφθεί αμερόληπτη γνώμη σχετικά με την αποτελεσματικότητα του προγράμματος.

- *Τυπικές αναφορές κατάστασης*

Ένας καλός τρόπος να κρατήσετε το προσωπικό επικεντρωμένο στην ευαισθητοποίηση σχετικά με την ασφάλεια και στις απαιτήσεις κατάρτισης του οργανισμού είναι να

εφαρμόσετε την απαίτηση για τακτική αναφορά κατάστασης από τους λειτουργικούς διαχειριστές.

- *Συγκριτική αξιολόγηση του Προγράμματος Ασφαλείας*

Πολλοί οργανισμοί ενσωματώνουν τη συγκριτική αξιολόγηση του «Προγράμματος Ασφαλείας» ως μέρος της στρατηγικής τους για συνεχή βελτίωση. Αυτός ο τύπος συγκριτικής αξιολόγησης επικεντρώνεται στην ερώτηση: Πώς αξιολογούμαι μεταξύ των συναδέλφων μου; Η εξωτερικά επικεντρωμένη μορφή αξιολόγησης συγκρίνει τις επιδόσεις ενός οργανισμού με ορισμένους άλλους οργανισμούς και παρέχει μια έκθεση πίσω στον οργανισμό σχετικά με το αν αποτυγχάνουν βάσει των παρατηρούμενων βασικών γραμμών σε όλους τους οργανισμούς με δεδομένα που είναι επί του παρόντος διαθέσιμα. Ένα στοιχείο αυτού του τύπου συγκριτικής αξιολόγησης θα πρέπει να περιλαμβάνει την ευαισθητοποίηση και την κατάρτιση στον τομέα της ασφάλειας. Αυτός ο τρόπος αξιολόγησης γίνεται συνήθως από εμπειρογνώμονες σε τεχνικές συγκριτικής αξιολόγησης, οι οποίοι διαθέτουν εκτεταμένες πληροφορίες (δεδομένα) σε ένα ευρύ φάσμα οργανισμών για αρκετά μεγάλη διάρκεια (πέντε ή περισσότερα έτη).

10.1 Ερωτηματολόγιο αξιολόγησης

Ένας τρόπος αξιολόγησης του προσωπικού μιας εταιρείας, σε ότι αναφορά τη γνώση και την ευαισθητοποίηση σε θέματα ασφάλειας πληροφοριακών συστημάτων, είναι η κατασκευή ενός ερωτηματολογίου. Με αυτόν τον τρόπο οι εργαζόμενοι θα μπορούν να γνωρίζουν σε ποιους τομείς θα πρέπει να είναι πιο προσεχτικοί, ενώ για τους υπεύθυνους ασφαλείας θα είναι ευκολότερη η επιλογή εκείνων που χρειάζονται περαιτέρω εκπαίδευση. Παρακάτω γίνεται καταγραφή ορισμένων ερωτήσεων, οι οποίες θα έβρισκαν χρήση σε ένα εταιρικό περιβάλλον κι αφορούν βασικές αρχές της ασφάλειας, κωδικούς πρόσβασης και ασφάλεια στο διαδίκτυο, καθώς κι οι πιθανές απαντήσεις τους.

10.1.1 Βασικές Αρχές

1. Δεν επιτρέπεται η ..... εμπιστευτικών πληροφοριών.
   - Φωτογράφιση
   - Παραποίηση
   - Μη εξουσιοδοτημένη κοινοποίηση

- Όλα τα παραπάνω

2. Κάθε ενδεχόμενο συμβάν που σχετίζεται με την ασφάλεια πληροφοριακών συστημάτων (π.χ. εμφάνιση κάποιου ηλεκτρονικού ιού ή Trojan) πρέπει να αναφερθεί στην Διεύθυνση:
   - Συναλλαγών Ηλεκτρικής Ενέργειας
   - Ανθρώπινου Δυναμικού και Υποστήριξης
   - Πληροφορικής και Τηλεπικοινωνιών
   - Όλα τα παραπάνω

3. Η μη τήρηση των κανόνων ασφαλείας πληροφοριακών συστημάτων ενδέχεται να επιφέρει:
   - Αδυναμία Χρήσης των Πληροφοριακών Συστημάτων
   - Απώλεια ή Αλλοίωση Δεδομένων
   - Απώλεια Χρημάτων
   - Όλα τα παραπάνω

4. Τα επίπεδα ασφάλειας ενός Πληροφοριακού Συστήματος είναι:
   - Φυσική ασφάλεια
   - Ασφάλεια Λειτουργικών Συστημάτων
   - Ασφάλεια Δικτύων
   - Ασφάλεια Λογισμικού
   - Όλα τα παραπάνω

5. Η Φυσική Ασφάλεια περιλαμβάνει την προστασία του Πληροφοριακού Εξοπλισμού από:
   - Πρόσβαση μη εξουσιοδοτημένου προσωπικού στον χώρο του εξοπλισμού
   - Φυσική καταστροφή (π.χ. φωτιά, σεισμός, πλημμύρα)
   - Διακοπή ηλεκτρικής τροφοδότησης
   - Όλα τα παραπάνω

6. Έγγραφα που περιέχουν εμπιστευτικές/σημαντικές εταιρικές πληροφορίες:
   - Μπορούν να μένουν εκτεθειμένα σε κοινόχρηστους χώρους
   - Πρέπει να φυλάσσονται σε ασφαλές μέρος
   - Μπορούν να ψηφιοποιηθούν και να μοιραστούν σε όλους
   - Όλα τα παραπάνω

7. Τα Πληροφοριακά Συστήματα κινδυνεύουν από
   - Αγνώστους εκτός εταιρείας
   - Συνεργάτες
   - Προσωπικό
   - Όλα τα παραπάνω

8. Παγκοσμίως οι απειλές των Πληροφοριακών Συστημάτων προέρχονται από:
   - Αγνώστους εκτός εταιρείας
   - Συνεργάτες
   - Προσωπικό
   - Όλα τα παραπάνω

9. Η ασφάλεια ενός Πληροφοριακού Συστήματος αφορά:
   - Τους κωδικούς πρόσβασης
   - Το ηλεκτρονικό ταχυδρομείο
   - Το λογισμικό
   - Όλα τα παραπάνω

10. Η χρήση on-line συζητήσεων (chat), επιτρέπεται μόνο για ..... λόγους.
    - Προσωπικούς
    - Υπηρεσιακούς

11. Δεν επιτρέπεται η εσκεμμένη προσπάθεια πρόσβασης ή/και παραποίησης σε Πληροφοριακά Συστήματα όπως:
    - Προσωπικούς υπολογιστές συναδέλφων

- Servers
- Λοιπό πληροφοριακό και τηλεπικοινωνιακό εξοπλισμό
- Όλα τα παραπάνω

12. Εάν ζητηθούν από την εταιρεία λύτρα για την αποκατάσταση πληροφοριακής δυσλειτουργίας και η εταιρεία δεχτεί να τα καταβάλει, είναι βέβαιη η αποκατάσταση της δυσλειτουργίας.
    - Ναι. Όταν καταβάλλονται λύτρα η αποκατάσταση της δυσλειτουργίας είναι βέβαιη.
    - Όχι. Περίπου στις μισές περιπτώσεις παγκοσμίως που έχουν καταβληθεί λύτρα η αποκατάσταση της δυσλειτουργίας δεν έχει επιτευχθεί.

13. Ποια αρχή αναφέρεται στην ιδιότητα των πόρων να καθίστανται αμέσως προσπελάσιμοι;
    - Εμπιστευτικότητα
    - Ακεραιότητα
    - Διαθεσιμότητα
    - Αυθεντικότητα

14. Ποια αρχή αναφέρεται στην υποχρέωση οι ευαίσθητες πληροφορίες να μην αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα;
    - Εμπιστευτικότητα
    - Ακεραιότητα
    - Διαθεσιμότητα
    - Αυθεντικότητα

15. Το πιο αδύναμο σημείο της ασφάλειας των Πληροφοριακών Συστημάτων είναι .....
    - Οι κωδικοί πρόσβασης
    - Το δίκτυο
    - Τα δεδομένα

- Οι προσωπικοί υπολογιστές των χρηστών

16. Η Ασφάλεια των Πληροφοριακών Συστημάτων ασχολείται με την προστασία των υπολογιστών, των δικτύων που τους διασυνδέουν και των δεδομένων.
    - Σωστό
    - Λάθος

17. Πρέπει να αποφεύγεται κατάχρηση της εταιρικής τηλεφωνίας για προσωπικούς λόγους.
    - Σωστό
    - Λάθος

18. Οι φορητοί υπολογιστές πρέπει να φυλάσσονται σε ασφαλή τοποθεσία.
    - Σωστό
    - Λάθος

19. Πρέπει να αποφεύγεται η χρήση του διαδικτύου για προσωπικούς λόγους.
    - Σωστό
    - Λάθος

20. Ο χρήστης επιτρέπεται να εγκαταστήσει λογισμικά πακέτα στον υπολογιστή του χωρίς σχετική αδειοδότηση από τη Διεύθυνση Πληροφορικής.
    - Σωστό
    - Λάθος

21. Ο κάθε χρήστης έχει προσωπική ευθύνη για το λογισμικό που είναι εγκατεστημένο στον προσωπικό υπολογιστή του.
    - Σωστό
    - Λάθος

22. Δεν επιτρέπεται η εσκεμμένη προσπάθεια παρεμπόδισης της ομαλής λειτουργίας εταιρικών Πληροφοριακών Συστημάτων.
    - Σωστό
    - Λάθος

23. Η ασφάλεια των Πληροφοριακών Συστημάτων είναι υπόθεση όλων όσων έχουν πρόσβαση σε αυτά.
    - Σωστό
    - Λάθος

24. Ενδέχεται εάν ο χρήστης δεν τηρεί τα προβλεπόμενα μέτρα ασφαλείας να συνεισφέρει άθελά του στη διαρροή των σημαντικών πληροφοριών της επιχείρησης;
    - Σωστό
    - Λάθος
25. Οι πληροφορίες που εμπεριέχονται στα εταιρικά Πληροφοριακά Συστήματα είναι εν γένει εμπιστευτικές και κάθε ένας είναι προσωπικά υπεύθυνος για να μην τις γνωστοποιήσει συνειδητά ή ασυνείδητα.
    - Σωστό
    - Λάθος

10.1.2 Κωδικοί πρόσβασης

1. Εάν ένας κωδικός πρόσβασης υποκλαπεί, μπορεί να χρησιμοποιηθεί από τον κακόβουλο χρήστη για:
    - Πρόσβαση σε σημαντικότερα συστήματα
    - Να υποκλαπούν τα σημαντικά αρχεία
    - Να καταστραφούν τα αρχεία
    - Όλα τα παραπάνω

2. Οι κωδικοί πρέπει να έχουν μήκος τουλάχιστον έξι χαρακτήρων (κατά προτίμηση 8-10) και να περιέχουν:

- Γράμματα
- Αριθμούς
- Ειδικούς χαρακτήρες
- Όλα τα παραπάνω

3. Εύκολα προβλέψιμοι κωδικοί είναι:
   - Ονόματα, ημερομηνίες γενεθλίων
   - Τηλεφωνικοί αριθμοί
   - Προφανείς ακολουθίες αριθμών π.χ. 123456
   - Όλα τα παραπάνω

4. Ποιός από τους παρακάτω κωδικούς είναι ο πιο ισχυρός;
   - 230484
   - M@ria!728
   - maria7
   - maRia888

5. Ορισμένοι χώροι διαθέτουν συστήματα ελεγχόμενης πρόσβασης (access control). Οι κάρτες πρόσβασης για αυτούς τους χώρους ..... να δίδονται σε άλλους.
   - Επιτρέπεται
   - Απαγορεύεται
   - Επιτρέπεται εν μέρει
   - Πρέπει

6. Σε περίπτωση που θα πρέπει να δοθεί φυσική πρόσβαση στους χώρους που διαθέτουν σύστημα ελέγχου πρόσβασης (access control) σε άτομα που δεν διαθέτουν ατομική κάρτα εισόδου, τα άτομα αυτά θα πρέπει:
   - Τα άτομα αυτά να συνοδεύονται καθ όλο το χρόνο της παρουσίας τους
   - Να τους δοθεί κάρτα πρόσβασης

7. Κάθε χρήστης επιτρέπεται να έχει πρόσβαση σε .....
   - Κανένα πληροφοριακό σύστημα
   - Όλα τα πληροφοριακά συστήματα
   - Όσα πληροφοριακά συστήματα είναι απαραίτητα για την τέλεση των καθηκόντων του

8. Ποιο από τα παρακάτω ΔΕΝ θεωρείται κακόβουλο λογισμικό;
   - Trojans
   - Worms
   - Viruses
   - Θεωρούνται όλα κακόβουλα λογισμικά

9. Ποιος είναι ο συνδιασμός πλήκτρων για κλείδωμα του υπολογιστή σε λειτουργικό Windows;
   - Shift + Alt
   - Ctrl + F1 + Delete
   - Ctrl + Alt + Delete
   - Shift + Alt + Delete

10. ..... είναι μια συμβολοσειρά χαρακτήρων που χρησιμοποιεί ένας χρήστης για να συνδεθεί σε έναν υπολογιστή και να έχει πρόσβαση σε αρχεία, προγράμματα και άλλους πόρους.
    - Η κάρτα πρόσβασης
    - Ο κωδικός πρόσβασης
    - Το λογισμικό

11. Οι χρήστες δεν πρέπει να χρησιμοποιούν στο εταιρικό δίκτυο κωδικούς ίδιους με αυτούς που χρησιμοποιούν στο διαδίκτυο για προσωπική τους χρήση (π.χ. κωδικούς facebook, twitter).
    - Σωστό

- Λάθος

12. Οι χρήστες επιτρέπεται να καταγράφουν τους κωδικούς πρόσβασης σε εμφανή σημεία.
    - Σωστό
    - Λάθος

13. Οι χρήστες δεν πρέπει σε καμία περίπτωση να αποστέλλουν κωδικούς μέσω ηλεκτρονικού ταχυδρομείου γιατί εύκολα μπορούν να υποκλαπούν.
    - Σωστό
    - Λάθος

14. Οι κωδικοί πρόσβασης για λόγους ασφαλείας πρέπει να αλλάζονται τακτικά.
    - Σωστό
    - Λάθος

15. Το προσωπικό ΔΕΝ πρέπει να ασφαλίζει την πρόσβαση στον προσωπικό υπολογιστή του όταν απομακρύνεται από αυτόν (κλείδωμα υπολογιστή ή αποσύνδεση χρήστη).
    - Σωστό
    - Λάθος

16. Έχοντας ένα αντίγραφο ασφαλείας των δεδομένων σας είναι αρκετό για την ασφάλεια.
    - Σωστό
    - Λάθος

17. Οι κωδικοί πρόσβασης είναι αυστηρά προσωπικοί και δεν είναι ανακοινώσιμοι σε καμία περίπτωση.
    - Σωστό

- Λάθος

18. Οι αρχικοί κωδικοί πρόσβασης που δίδονται σε κάθε χρήστη δεν πρέπει να αλλάζονται από αυτόν.
    - Σωστό
    - Λάθος

10.1.3 Ασφάλεια στο διαδίκτυο

1. Το ..... επιδιώκει στην οικοδόμηση εμπιστοσύνης με τους εργαζομένους με σκοπό την απόκτηση ευαίσθητων πληροφοριών ή προνομίων μη εξουσιοδοτημένης πρόσβασης.
    - Social engineering
    - Hacking
    - Phishing
    - Spamming

2. Η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών λέγεται:
    - Spamming
    - Phishing
    - Social Engineering
    - Trekking

3. Η παράνομη/μη εξουσιοδοτημένη πρόσβαση στα Πληροφοριακά Συστήματα με στόχο την υποκλοπή των προσωπικών δεδομένων λέγεται:
    - Spamming
    - Phishing
    - Social Engineering
    - Όλα τα παραπάνω

4. Η ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο κακόβουλος υποδύεται μία αξιόπιστη οντότητα, με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων λέγεται:
   - Hacking
   - Phishing
   - Spamming
   - Pharming

5. Λάβατε ένα e-mail από κάποιο άγνωστο πρόσωπο που ισχυρίζεται ότι είναι εκπρόσωπος της τράπεζας σας και ζητά τον αριθμό λογαριασμού και τον κωδικό σας, ώστε να μπορεί να διορθώσει το λογαριασμό σας. Μια τέτοια προσπάθεια λέγεται:
   - Shoulder Surfing
   - Phishing
   - Mountaineering
   - Trekking

6. Με τον όρο ..... ορίζουμε συνήθως ανώνυμη, μαζική αποστολή ενός ή περισσοτέρων μηνυμάτων ηλεκτρονικού ταχυδρομείου προς πολλαπλούς αποδέκτες
   - Phishing
   - Spamming
   - Hacking
   - Software

7. Μέσω ηλεκτρονικού ταχυδρομείου επιτρέπεται να στέλνουμε:
   - Εκτελέσιμα Αρχεία
   - Αρχεία αμφιβόλου προέλευσης
   - Αρχεία μολυσμένα με virus
   - Κανένα από τα παραπάνω

8. Ακόμα και στην περίπτωση όπου κάποιο λογισμικό είναι προβλεπόμενο για την τέλεση εταιρικών καθηκόντων δεν επιτρέπεται η εγκατάσταση του εάν δεν είναι κατάλληλα .....
   - Τοποθετημένο
   - Αδειοδοτημένο
   - Εγκατεστημένο
   - Διαμορφωμένο

9. Αφού λάβετε ένα e-mail από "ύποπτο" αποστολέα που έχει ένα συννημένο αρχείο, θα πρέπει να:
   - Ανοίξετε το συνημμένο αρχείο
   - Σβήσετε το e-mail χωρίς να ανοίξετε το συνημμένο
   - Προωθήσετε το συνημμένο σε όλους τους φίλους και συναδέλφους
   - Μην κάνετε καμία ενέργεια και να διατηρήσετε το e-mail στα εισερχόμενα

10. Η τεχνική ..... μέσω email κατευθύνει μέσα από email σε ιστοσελίδες στοχευμένες στα ενδιαφέροντα των επιτήδειων.
   - Antivirus
   - Trojan
   - Phishing
   - Όλα τα παραπάνω

11. Δεν επιτρέπεται η χρήση του διαδικτύου για πρόσβαση σε ιστοσελίδες:
   - Τυχερών παιχνιδιών (τζόγου)
   - Σεξουαλικού περιεχομένου
   - Κοινωνικής δικτύωσης (facebook, twitter)
   - Όλα τα παραπάνω

12. Σε ποιους από τους παρακάτω μηχανισμούς ασφάλειας δεν επιτρέπεται η απενεργοποίηση ή η μεταβολή ρυθμίσεων;
   - Antivirus

- Secure agent
- Κλειδώματος Η/Υ
- Όλα τα παραπάνω

13. Ποια από τις παρακάτω διευθύνσεις ιστοσελίδων μπορεί να χρησιμοποιηθεί για τη διαβίβαση σημαντικών δεδομένων (πχ κωδικών πρόσβασης);
    - Η διεύθυνση URL web που ξεκινά με http://
    - Η διεύθυνση URL web που καταλήγει σε .com
    - Η διεύθυνση URL της ιστοσελίδας που ξεκινάει με https://
    - Η διεύθυνση URL web που περιλαμβάνει αριθμούς, π.χ. με http://192.168.0.1

14. Οι χρήστες θα πρέπει να χρησιμοποιούν στο διαδίκτυο αποκλειστικά και μόνο αξιόπιστες ιστοσελίδες.
    - Σωστό
    - Λάθος

15. Οι ιστοσελίδες που σου επιτρέπουν να κατεβάσεις ατελώς λογισμικά πακέτα ή κινηματογραφικές ταινίες μπορούν να εμφυτεύσουν στον υπολογιστή σου κακόβουλο λογισμικό
    - Σωστό
    - Λάθος

16. Εάν εγκαταστήσετε ένα λογισμικό αμφιβόλου προέλευσης ενδέχεται να υποκλαπούν εμπιστευτικά σας δεδομένα όπως κωδικοί πρόσβασης σε Τραπεζικούς λογαριασμούς και πιστωτικές κάρτες
    - Σωστό
    - Λάθος

17. Πρέπει να αποφεύγεται η χρήση του εταιρικού ηλεκτρονικού ταχυδρομείου για προσωπικούς λόγους
    - Σωστό

- Λάθος

18. Η διακίνηση, μη εξουσιοδοτημένων, εταιρικών πληροφοριών επιτρέπεται μέσω του ηλεκτρονικού ταχυδρομείου
    - Σωστό
    - Λάθος

19. Η χρήση του ηλεκτρονικού ταχυδρομείου για την διακίνηση εμπιστευτικών πληροφοριών παρέχει ασφάλεια
    - Σωστό
    - Λάθος

20. Η παράδοση/παραλαβή ηλεκτρονικού ταχυδρομείου είναι εγγυημένη και θεωρείται δεδομένη
    - Σωστό
    - Λάθος

21. Επιτρέπεται η μη εγκεκριμένη μαζική αποστολή ή προώθηση ηλεκτρονικών μηνυμάτων
    - Σωστό
    - Λάθος

22. Πρέπει πάντα να γίνεται αξιολόγηση του περιεχομένου του μηνύματος και αν υπάρχει αμφιβολία τότε πρέπει να γίνει τηλεφωνική εξακρίβωση της προέλευσής του
    - Σωστό
    - Λάθος

23. Δεν επιτρέπεται η αποστολή ή προώθηση αρχείων και λογισμικού αμφιβόλου προέλευσης μέσω ηλεκτρονικού ταχυδρομείου
    - Σωστό

- Λάθος

24. Η αποστολή του υλικού όπου υπόκειται σε κατοχυρωμένα πνευματικά δικαιώματα μπορεί να γίνει χωρίς σχετική αδειοδότηση
    - Σωστό
    - Λάθος

25. Η καταχώρηση οποιασδήποτε εταιρικής πληροφορίας στο διαδίκτυο, επιτρέπεται χωρίς εταιρική έγκριση
    - Σωστό
    - Λάθος

26. Η τεχνική Phishing μπορεί να επιτευχθεί και μέσω τηλεφώνου
    - Σωστό
    - Λάθος

27. Δεν επιτρέπεται η χρήση ασύρματων Wi-Fi δικτύων για πρόσβαση στο εταιρικό δίκτυο λόγω των κινδύνων που εγκυμονούνται
    - Σωστό
    - Λάθος

28. Είναι δυνατόν πατώντας ένα click σε μια ιστοσελίδα να εκτελείται κρυφός κώδικας λογισμικού;
    - Σωστό
    - Λάθος

29. Εκτελώντας ένα αρχείο μπορείς να δώσεις απομακρυσμένη εξωτερική πρόσβαση στον υπολογιστή σου
    - Σωστό
    - Λάθος

10.1.4 Κακόβουλα προγράμματα

1. Ένας τρόπος εντοπισμού κάποιου ιού γίνεται με χρήση .....
   - Safe mode
   - Antivirus
   - Web Browser

2. Αν ένας υπολογιστής μολυνθεί από κάποιο ιό .....
   - Αποσυνδεθείτε από το Ίντερνετ
   - Εκτελέστε μια πλήρη σάρωση του συστήματός σας με κάποιο Antivirus
   - Επικοινωνήστε με το Τμήμα Πληροφορικής της επιχείρησής σας
   - Όλα τα παραπάνω

3. Ένα σκουλήκι υπολογιστή είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να .....
   - Στείλει αντίγραφα του εαυτού του σε άλλους κόμβους
   - Περιηγηθεί στο διαδίκτυο
   - Τερματίσει τη λειτουργία του υπολογιστή
   - Όλα τα παραπάνω

4. Ένα κακόβουλο πρόγραμμα, όπως ο δούρειος ίππος, μπορεί να φτάσει σε κάποιο χρήστη .....
   - Μέσω e-mail
   - Μέσω CD ή DVD
   - Μέσω προγραμμάτων Instant Messaging
   - Όλα τα παραπάνω

5. Ένας δούρειος ίππος μπορεί να έχει ως αποτέλεσμα ...
   - Απενεργοποίηση λογισμικού ασφαλείας
   - Επιθέσεις άρνησης υπηρεσιών
   - Καταστροφή αρχείων
   - Όλα τα παραπάνω

6. Τα spyware είναι γραμμένα με κακόβουλη πρόθεση και μπορούν να ....
   - Παρακολουθήσουν τις συνήθειες περιήγησης ιστού
   - Καταστρέψουν την κάρτα γραφικών του υπολογιστή
   - Τίποτα από τα παραπάνω

7. Προστασία απο τα spyware μπορεί να επιτευχθεί με τη.....
   - Λήψη προγραμμάτων ή λογισμικού μόνο από αξιόπιστους ιστότοπους
   - Λειτουργία ενημερωμένου λογισμικού anti-spyware
   - Σύνδεση λογαριασμού με περιορισμένα δικαιώματα
   - Όλα τα παραπάνω

8. ..... είναι ένα κακόβουλο πρόγραμμα
   - Το Antivirus
   - Το Trojan
   - Το Phishing
   - Όλα τα παραπάνω

11. Συμπεράσματα

Εν κατακλείδι, η εκπαίδευση για την ευαισθητοποίηση σχετικά με την ασφάλεια, εάν εφαρμοστεί σωστά, είναι μια σημαντική αναγκαιότητα για οποιαδήποτε οργάνωση. Εάν η βάση των χρηστών ενημερωθεί σωστά για το τι πρέπει να προσέξει, την πρόληψη, τις διαδικασίες αποκατάστασης, αυτό μόνο του θα μπορούσε να αποτρέψει πολλά πιθανά προβλήματα που θα μπορούσαν να επηρεάζουν την υποδομή και την εταιρεία ως σύνολο. Συχνά η απλή συνειδητοποίηση είναι το κλειδί για την πρόληψη και την προστασία.

Μέσω ενός προγράμματος εκπαίδευσης και ευαισθητοποίησης θα μειωθούν τα ανθρώπινα λάθη κατά ένα μεγάλο ποσοστό αυξάνοντας έτσι την ασφάλεια του οργανισμού. Ένα εκπαιδευμένο προσωπικό αυξάνει επίσης και τη συμμόρφωση σε νόμους οι οποίοι θα μπορούσαν να επιφέρουν αγωγές και πρόστιμα μειώνοντας τη φήμη του οργανισμού. Επιπλέον, με εκπαιδευμένο προσωπικό σώζονται χρήματα και χρόνος που θα χρειαζόταν για ανάκαμψη του οργανισμού από μια επικείμενη επίθεση. Τέλος, το πρόγραμμα εκπαίδευσης ανεβάζει το ηθικό των εργαζομένων, ενώ παράλληλα βοηθά και στην επικράτηση ηρεμίας μέσα σε έναν οργανισμό. [16]

«Οι εργαζόμενοι μπορούν και πρέπει να είναι η τελευταία γραμμή άμυνας». Η εκπαίδευση στην ευαισθητοποίηση σχετικά με την ασφάλεια μπορεί να αποδώσει με την εκπαίδευση των χρηστών για το τι μπορούν να κάνουν για να αποτρέψουν κακόβουλες δραστηριότητες και τι πρέπει να κάνουν σε περίπτωση τέτοιας δραστηριότητας. Φυσικά, η εκπαίδευση για την ευαισθητοποίηση στην ασφάλεια δεν αρκεί από μόνο του, αλλά είναι ένα σημαντικό επίπεδο ασφάλειας που προστίθεται στα υπάρχοντα μέτρα ασφαλείας (Rothman, 2007).

Βιβλιογραφία

[1] Infosec Institute - Best Practices for Implementing Security Awareness Training

[2] SANS Institute InfoSec Reading Room - The Importance of Security Awareness

[3] American Public Transportation Association Security Awareness - Training for Transit Employees

[4] Mark Wilson and Joan Hash - Building an Information Technology Security Awareness and Training Program

[5] https://security.tennessee.edu/training/topic-6-desktop-security/

[6] Μπλέτσας Ιωάννης – Πτυχιακή εργασία

[7] https://blog.trendmicro.com/trendlabs-security-intelligence/how-can-social-engineering-training-work-effectively/

[8] Kaspr Prei - Measuring personnel cyber security awareness level through phishing assessment

[9] https://security.tennessee.edu/training/topic-5-email-hoaxes-and-scams/

[10] https://el.wikipedia.org/wiki/Δούρειος_Ίππος_(υπολογιστές)

[11] https://security.tennessee.edu/training/topic-4-spyware/

[12] https://it.tufts.edu/reporting-information-security-incident

[13] Πολιτική Ασφαλείας ΑΔΜΗΕ

[14] InfoSec Institute - Best Practices for Implementing Security Awareness Training

[15] SANS Institute InfoSec Reading Room - Social Engineering Your Employees to Information Security

[16] https://resources.infosecinstitute.com/7-benefits-of-security-awareness-training/#gref