Ο ρόλος του ανθρώπινου παράγοντα στον τομέα της Κυβερνοασφάλειας

"Η επένδυση στην κυβερνοασφάλεια είναι επένδυση στην επιβίωση της επιχείρησης"

Η τεχνολογία διαδραματίζει ένα ρόλο ζωτικής σημασίας στην εποχή μας, αφού έχει εξελιχθεί πια σε ένα καθημερινό εργαλείο στον τομέα της ενημέρωσης, της εργασίας, της ψυχαγωγίας, της επικοινωνίας και πολλών άλλων. Μαζί με τα οφέλη, η τεχνολογία φέρνει μαζί της κινδύνους τους οποίους ο κάθε οργανισμός και επιχείρηση θα πρέπει να αναγνωρίσει και να αντιμετωπίσει έγκαιρα και αποτελεσματικά. Στην εποχή του Διαδικτύου των Πραγμάτων ή «Internet of Things», όπου τα πάντα από απλές οικιακές συσκευές μέχρι βιομηχανικές μηχανές, είναι πλέον διασυνδεδεμένα με το διαδίκτυο, η κυβερνοσφάλεια είναι αναγκαία για την επιβίωση της κάθε επιχείρησης. Η υποκλοπή δεδομένων, τα ιομορφικά λογισμικά (malware) και οι επιθέσεις κοινωνικής μηχανικής (social engineering) είναι μερικά από τα είδη κυβερνοαπειλών που ενδεχομένως να επιφέρουν ακόμα και οικονομικές επιπτώσεις στο θύμα. Συνεπώς, μία από τις προτεραιότητες του οργανισμού είναι η επένδυση σε λύσεις κυβερνοασφάλειας, συμπεριλαμβανομένων προϊόντων και υπηρεσιών, με σκοπό την δημιουργία ενός ανεκτού επιπέδου ασφάλειας και προστασίας. Σύμφωνα με μια πρόσφατη έρευνα[1], το μέσο κόστος μόνο από την παραβίαση δεδομένων θα ξεπεράσει τα 150 εκατομμύρια μέχρι το έτος 2020, κάτι το οποίο δικαιολογεί και την επένδυση στην τεχνολογία της κυβερνοασφάλειας που θα ξεπεράσει το 1 τρισεκατομμύριο παγκοσμίως για τα έτη 2017-2021.

"Η ασφάλεια είναι ένας πολύπλοκος μηχανισμός, όπου μετρούν ακόμα και τα μικρότερα κομμάτια"

Το πλαίσιο κυβερνοασφάλειας, το οποίο η κάθε επιχείρηση θα πρέπει να σχεδιάσει και να υιοθετήσει, είναι ένα πολύπλοκο περιβάλλον πολλών στοιχείων τόσο σε θεωρητικό επίπεδο (π.χ. πολιτικές, διαδικασίες, σεμινάρια) όσο και πρακτικό (π.χ. έλεγχοι ασφάλειας, ανάλυση επικινδυνότητας). Παράλληλα, τα στοιχεία αυτά είναι αλληλεξαρτώμενα και χρειάζονται το ένα το άλλο έτσι ώστε η παραπάνω ασφάλεια να είναι όσο το δυνατό πιο αποδοτική. Ένα ενδεικτικό παράδειγμα είναι το ζεύγος μίας πολιτικής κωδικών ασφαλείας (password policy) και του αντίστοιχου συστημικού μηχανισμού. Από την μία πλευρά, η πολιτική οριοθετεί και καθοδηγεί τον χρήστη στις βέλτιστες πρακτικές επιλογής συνθηματικού, ενώ από την άλλη, ο μηχανισμός που έχει παραμετροποιηθεί στο σύστημα, διασφαλίζει το ότι ο χρήστης ακολούθησε τις οδηγίες, όπως αυτές ορίζονται στην αντίστοιχη πολιτική.

"Δεν χρειάζεται να παραβιάσεις έναν μηχανισμό ασφάλειας παρά μόνο τον χρήστη που τον διαχειρίζεται"

Ο υπεύθυνος ασφάλειας πρέπει να εντοπίσει και να προστατεύσει όλες τις υπάρχουσες τρωτότητες, ενώ ο επιτιθέμενος αρκεί να βρει μόνο μία για να πλήξει τον οργανισμό. Συνεπώς, η κυβερνοασφάλεια είναι μία αλυσίδα με διακριτούς κρίκους, η ισχύ της οποίας είναι ίση με τον πιο αδύναμο που είναι συνήθως ο ανθρώπινος παράγοντας. Πιο συγκεκριμένα, οι χρήστες εντοπίζονται σε όλες τις δραστηριότητες του οργανισμού, ειδικότερα στους μηχανισμούς ασφάλειας. Για παράδειγμα, υπάρχει μία ομάδα χρηστών που δημιουργεί μία πολιτική ασφάλειας, οι τελικοί χρήστες που την τηρούν και οι ελεγκτές ασφάλειας που διασφαλίζουν την ορθή τήρησή της. Το ίδιο φυσικά ισχύει και για οποιοδήποτε άλλο μηχανισμό ασφάλειας (π.χ. δικαιώματα πρόσβασης). Συνεπώς, υπάρχουν περιπτώσεις όπου ένα μόνο ανθρώπινο σφάλμα στην παραπάνω διεργασία –

[1] https://www.cybintsolutions.com/cyber-security-facts-stats/

ηθελημένο ή μη – ενδέχεται να καταλήξει στη δημιουργία ενός τρωτού σημείου που μπορεί να εκμεταλλευτεί κάποιος κακόβουλος χρήστης.

Ένα περιστατικό ασφάλειας δημιουργείται είτε εξαιτίας μιας επίθεσης, είτε ως αποτέλεσμα ενός απλού ανθρωπίνου λάθους. Η πρώτη περίπτωση, όπου ο πιο συνήθης στόχος ενός επιτιθέμενου είναι ο μέσος χρήστης, είναι μία πρακτική που έχει αποδειχθεί άκρως αποτελεσματική, ειδικά όταν δεν υπάρχουν επαρκή μέτρα προστασίας απέναντι στην απειλή που ονομάζεται κοινωνική μηχανική (social engineering). Σε αυτή την κατηγορία, ο επιτιθέμενος έχει ως στόχο να εντοπίσει και να εκμεταλλευτεί τρωτά σημεία, όχι στο δίκτυο και τις εφαρμογές, αλλά στους χρήστες που βρίσκονται πίσω από αυτά. Το αποτέλεσμα είναι άμεσο και αποδοτικό, υπό την έννοια πως αν η επίθεση είναι επιτυχημένη, υπάρχει αυξημένη πιθανότητα να παρακαμφθούν ακόμα και τα όποια υπάρχοντα μέτρα ασφάλειας. Ενδεικτικά, μία έρευνα[2] στην Ευρώπη είχε αναδείξει πως το 70% των χρηστών ήταν πρόθυμοι να αποκαλύψουν τον κωδικό ασφαλείας (password) του προσωπικού τους υπολογιστή σε έναν άγνωστο με αντάλλαγμα μία σοκολάτα.

Η δεύτερη περίπτωση περιστατικού, εντοπίζεται στο ίδιο τον μέσο χρήστη, ο οποίος δεν έχει κουλτούρα ασφάλειας και αίσθηση των αντίστοιχων κινδύνων, βάζει ως προτεραιότητα την ευκολία του. Αυτό ως ένα σημείο είναι λογικό, καθώς η λειτουργία μιας επιχείρησης επικεντρώνεται στις προσφερόμενες υπηρεσίες/προϊόντα και στους πελάτες της. Το αποτέλεσμα όμως, είναι ο χρήστης να επιλέγει να μην τηρήσει έναν κανόνα ασφάλειας, ειδικά αν είναι αρκετά πολύπλοκος, έτσι ώστε να νιώθει πως η καθημερινή εργασία του πραγματοποιείται χωρίς επιπλέον εμπόδια. Ένα κλασσικό παράδειγμα είναι ο χρήστης που επιλέγει ένα αρκετά δύσκολο συνθηματικό – όπως υπαγορεύει η αντίστοιχη πολιτική – ενώ παράλληλα το σημειώνει σε ένα χαρτί και το τοποθετεί κάτω από το πληκτρολόγιο ή ακόμα και πάνω στην οθόνη. Στην περίπτωση αυτή, έστω και αν υπάρχει μία σωστή πολιτική και ο συστημικός μηχανισμός που διασφαλίζει την τήρησή της, ο ανθρώπινος παράγοντας καταφέρνει να ακυρώσει και τα δύο μέτρα προστασίας.

“Η πρώτη γραμμή άμυνας είναι οι ίδιοι οι υπάλληλοι”

Το παραπάνω παράδειγμα αποδεικνύει το ότι ακόμα και μία παρατυπία μπορεί να αποτελέσει βάση για παραβίαση ενός συστήματος. Συνεπώς, προτείνεται από τις βέλτιστες πρακτικές ασφάλειας, η προστασία του χρήστη να είναι προτεραιότητα και να κατευθύνεται από κυρίως από τρεις οδηγούς: (α) τα διευθυντικά στελέχη, (β) τους υπεύθυνους ασφάλειας και (γ) τους ίδιους τους χρήστες.

Η Διεύθυνση, ενεργεί ως οδηγός των στρατηγικών αποφάσεων, καθώς θέτει τις βασικές αρχές σύμφωνα με τις οποίες λειτουργεί η επιχείρηση. Χωρίς αυτήν, δε θα μπορέσει να συσταθεί σωστά και αποδοτικά το αναγκαίο πλαίσιο ασφάλειας, ενώ δε θα υπάρχει η αντίστοιχη στρατηγική προσέγγιση και οριοθέτηση του πλαισίου αυτού. Οι υπεύθυνοι ασφάλειας, που αποτελούν το δεύτερο πυλώνα, είναι οι αρμόδιοι για τη διατήρηση ενός επιτρεπτού επιπέδου ασφάλειας απέναντι στην όποια απειλή. Αυτοί σχεδιάζουν, υλοποιούν, ελέγχουν και συντηρούν τους μηχανισμούς ασφάλειας, ενώ παράλληλα είναι αναγκαίο να είναι εναρμονισμένοι με τις τρέχουσες τάσεις και βέλτιστες πρακτικές ασφάλειας. Τέλος, οι χρήστες, που μπορεί να είναι υπάλληλοι ή εξωτερικοί χρήστες (π.χ. συνεργάτες, πελάτες, κτλ.), πρέπει να εφαρμόζουν τα μέσα προστασίας που προσφέρουν οι υπεύθυνοι ασφάλειας και υποστηρίζει η Διεύθυνση.

[2] http://news.bbc.co.uk/2/hi/technology/3639679.stm

Μία αποδοτική προσέγγιση για την επίτευξη του παραπάνω στόχου είναι η ενημέρωση των χρηστών μέσω εκπαιδευτικών σεμιναρίων. Τα σεμινάρια αυτά θα βοηθήσουν στη δημιουργία και την προώθηση μιας ενιαίας κουλτούρας ασφάλειας, ενώ θα λειτουργήσουν ως μέσο προστασίας απέναντι σε έναν επιτιθέμενο που στοχεύει τους χρήστες του οργανισμού. Παράλληλα, οι υπεύθυνοι ασφάλειας πρέπει να αναπτύξουν μέτρα προστασίας τα οποία να μη λειτουργούν εις βάρος του χρήστη, αλλά να μη μειώνουν την ασφάλεια που προσφέρουν, εντοπίζοντας έτσι τη χρυσή τομή ανάμεσα στις δύο αυτές περιοχές.

"Η αλυσίδα της ασφάλειας είναι τόσο ισχυρή όσο ο πιο αδύναμος κρίκος της"

Μία σύγχρονη επιχείρηση καλείται να αντιμετωπίσει μία πληθώρα κυβερνοαπειλών, για κάποιες από τις οποίες ενδεχομένως να μην υπάρχει επαρκής προστασία. Μία από τις απειλές αυτές είναι και ο μέσος χρήστης, ο οποίος μπορεί είτε να πέσει θύμα ενός έξυπνου επιτιθέμενου, είτε να είναι υπεύθυνος για καθημερινά ανθρώπινα λάθη, τα οποία πιθανόν να έχουν μεγάλη επίπτωση στη βιωσιμότητα μιας επιχείρησης. Σε κάθε περίπτωση, οι οργανισμοί θα πρέπει να σχεδιάσουν και να υλοποιήσουν ένα επαρκές πλαίσιο διακυβέρνησης της κυβερνοασφάλειας μέσα από το οποίο να τίθεται η σχετική στρατηγική καθώς και να διασφαλίζεται η υλοποίηση και εφαρμογή της σε όλα τα επίπεδα του οργανισμού. Ένα τέτοιο πλαίσιο διακυβέρνησης πρέπει να στηρίζεται σε ανθρώπους με γνώση και εμπειρίες στην κυβερνοασφάλεια, σε συστήματα και υποδομές που λειτουργούν τόσο ως ασπίδα προστασίας όσο και αντιμετώπισης σχετικών απειλών και σε διαδικασίες που συνθέτουν ένα πλαίσιο ασφαλείας γύρω από τον οργανισμό και τους χρήστες του.

Οι οργανισμοί για το σχεδιασμό και υλοποίηση ενός ολοκληρωμένου πλαισίου διακυβέρνησης της κυβερνοασφάλειας θα πρέπει να στοχεύουν σε:

- Αναγνώριση των κινδύνων που αναλαμβάνει η επιχείρηση σχετικά με τις κυβερνοαπειλές.
- Καθορισμό σχετικών πολιτικών και διαδικασιών προς οριοθέτηση του τρόπου διαχείρισης των κυβερνοαπειλών.
- Ανάθεση σε άτομο ή ομάδα, εντός ή εκτός του οργανισμού, της ευθύνης σχεδιασμού του πλαισίου κυβερνοασφάλειας και παρακολούθησης της υλοποίησης/εφαρμογής των σχετικών πολιτικών και διαδικασιών.
- Επικοινωνία αυτών και σχετική εκπαίδευση τόσο της Διεύθυνσης όσο και των χρηστών προς δημιουργία κουλτούρας κυβερνοασφάλειας.
- Ανάπτυξη και υλοποίηση τεχνολογικών μηχανισμών ασφάλειας σύμφωνα με τις βέλτιστες πρακτικές.
- Διαρκής παρακολούθηση και ανεξάρτητος έλεγχος της υλοποίησης/εφαρμογής του πλαισίου διακυβέρνησης της κυβερνοασφάλειας και τακτή επικαιροποίηση αυτού εάν και εφόσον απαιτείται.

Προφίλ Αρθρογράφου:

Ο Νίκος Τσάλης ανήκει στο τμήμα συμβουλευτικών υπηρεσιών (Business Consulting Services – BCS) της Logicom Solutions και είναι υπεύθυνος των υπηρεσιών ασφάλειας πληροφοριακών συστημάτων. Το τμήμα αυτό στοχεύει στην παροχή υψηλής ποιότητας συμβουλευτικών υπηρεσιών σε σχέση με την κυβερνοασφάλεια και γενικά την ψηφιακή αναβάθμιση των οργανισμών.

Στο παρελθόν, ο Νίκος εργάστηκε ως εσωτερικός ελεγκτής πληροφοριακών συστημάτων σε τραπεζικό ίδρυμα στην Κύπρο και ως εξωτερικός σύμβουλος ασφάλειας στην Ομάδα Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών του Οικονομικού Πανεπιστημίου Αθηνών στην Ελλάδα. Παράλληλα, ασχολήθηκε με την εκπαίδευση σε θέματα ασφάλειας πληροφοριακών συστημάτων σε δημόσια και ιδιωτικά τριτοβάθμια εκπαιδευτικά ιδρύματα σε Ελλάδα και Κύπρο.

Κατέχει BSc στην Πληροφορική από το Οικονομικό Πανεπιστήμιο Αθηνών στην Ελλάδα, MSc στον τομέα του Information Security από το Royal Holloway University of London στο Hv. Βασίλειο και PhD στην Ασφάλεια Πληροφοριακών Συστημάτων από το Οικονομικό Πανεπιστήμιο Αθηνών στην Ελλάδα. Επιπλέον, είναι κάτοχος επαγγελματικού τίτλου ελεγκτή πληροφοριακών συστημάτων από τον οργανισμό ISACA.

Πληροφορίες Επικοινωνίας:

Τηλέφωνο: 22 55 10 39

Ηλεκτρονική Διεύθυνση: n.tsalis@logicom.net

Ιστοσελίδα: www.logicomsolutions.com.cy