ΑΝΤΙΜΕΤΩΠΕΣ ΜΕ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ

Ένα σημαντικό μέρος της εφαρμογής του πλαισίου Κυβερνοασφάλειας σε μια επιχείρηση είναι η δημιουργία ενός Συστήματος Διαχείρισης Κινδύνων

Logicom Solutions

cisco Partner
Gold Certified

Οι επιχειρήσεις απαιτείται να μελετούν διαρκώς τις αλλαγές που διαδραματίζονται στο εξωτερικό και εσωτερικό τους περιβάλλον και να προσαρμόζονται σε αυτές διαμορφώνοντας ανάλογα τις συνθήκες και τον τρόπο λειτουργίας τους. Ταυτόχρονα, οι επιχειρήσεις έρχονται αντιμέτωπες με τους κινδύνους που κρύβει ο Κυβερνοχώρος. Οι κίνδυνοι αυτοί αυξάνονται, εξελίσσονται ή/και μετασχηματίζονται συνεχώς και οι επιχειρήσεις θα πρέπει να τους αντιμετωπίσουν άμεσα και αποτελεσματικά για να προστατέψουν τα δεδομένα, τους πελάτες και τη φήμη τους. Για την επιτυχή αντιμετώπιση των κινδύνων αυτών χρειάζεται πρώτιστα μια ολοκληρωμένη αξιολόγηση των κινδύνων και ένα ολοκληρωμένο σχέδιο Κυβερνοασφάλειας.

ΤΑ ΠΡΩΤΑ ΒΗΜΑΤΑ

Ένα σημαντικό μέρος της εφαρμογής του πλαισίου Κυβερνοασφάλειας σε μια επιχείρηση είναι η δημιουργία ενός Συστήματος Διαχείρισης Κινδύνων (Risk Management System). Το σύστημα αυτό χρησιμοποιείται για την αποτίμηση του επιπέδου της επικινδυνότητας που διατρέχει η επιχείρηση και αποτελείται από ένα σύνολο διαδικασιών και μεθοδολογιών που στοχεύουν στη μείωση του σχετικού κινδύνου. Η μείωση αυτή επιτυγχάνεται μέσω της δημιουργίας, επιλογής και εφαρμογής των κατάλληλων μέτρων ασφάλειας. Για παράδειγμα, η ανάπτυξη μιας ορθής Πολιτικής Δημιουργίας Συνθηματικών (Password Creation Policy), σε συνδυασμό με το σύστημα που τεχνικά υποστηρίζει τη δημιουργία των συνθηματικών αυτών, αποτελεί ένα επαρκές μέτρο προστασίας για τον κίνδυνο επιλογής ενός ασθενούς συνθηματικού, που είναι επιρρεπές σε αντίστοιχες επιθέσεις παραβίασης. Παρόμοιου είδους τεχνικές διαχείρισης κινδύνων προτείνονται τόσο από τις διεθνείς πρακτικές και πρότυπα ασφάλειας (π.χ. ISO 27001) όσο και από τα αντίστοιχα νομοθετικά πλαίσια (π.χ. GDPR). Αξίζει όμως να σημειωθεί ότι η επιλογή ενός κατάλληλου μέτρου προστασίας δεν επαρκεί από μόνη της, αλλά χρειάζεται να γίνει μετέπειτα έλεγχος κατά πόσο το συγκεκριμένο μέτρο έχει υλοποιηθεί και αν χρησιμοποιείται με αποτελεσματικό τρόπο. Η διαδικασία δημιουργίας του Συστήματος Διαχείρισης Κινδύνων αποτελείται από διακριτά βήματα, τα οποία πρέπει να εκτελεστούν σωστά για να διασφαλιστεί η αποτελεσματική διαχείριση των κινδύνων. Αρχικά απαιτείται να οριστεί το σχετικό πλαίσιο ανάλυσης, που περιλαμβάνει την καταγραφή των αναγκών και των στόχων που έχουν τεθεί. Η ενέργεια αυτή, βασιζόμενη στην εφαρμογή διεθνών πρακτικών, χρειάζεται ως βάση πληροφορίες που διέπουν το προφίλ κινδύνου της επιχείρησης, και στοχεύει στο να καθορίζει τις προτεραιότητες των ενεργειών που απαιτούνται να εκτελεστούν σε μετέπειτα επίπεδο. Αφού δημιουργηθεί το οργανωτικό πλαίσιο, απαιτείται η πλήρης αναγνώριση των πόρων που συνθέτουν το περιβάλλον της επιχείρησης, όπως ανθρώπινο δυναμικό, συσκευές δικτύου, εξυπηρετητές, laptops, τηλεφωνικές συσκευές, δεδομένα πελατών/υπαλλήλων, έγγραφα, υπηρεσίες κτλ.

ΑΝΑΓΝΩΡΙΣΗ ΚΙΝΔΥΝΩΝ

Στη συνέχεια, πρέπει να αναγνωριστούν οι κίνδυνοι που απειλούν αυτούς τους πόρους και οι σχετικές ιδιότητές τους, όπως για παράδειγμα η κρισιμότητα και η συχνότητα εμφάνισής τους. Παράλληλα, υπολογίζεται και η επίπτωση που μπορεί να επιφέρουν στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα του εκάστοτε πόρου. Η διαδικασία αυτή ονομάζεται ανάλυση επικινδυνότητας και εκτελείται τουλάχιστον μία φορά τον χρόνο ή και πιο συχνά, σε περίπτωση που υπήρχε κάποια σημαντική αλλαγή στην επιχείρηση που επηρεάζει τον τρόπο λειτουργίας της. Αξίζει να σημειωθούν οι παρακάτω όροι για να κατανοηθεί πλήρως ο τρόπος με τον οποίο ένας κίνδυνος μπορεί να επιδράσει σε έναν πόρο (π.χ. πληροφορία, υπηρεσία, συσκευή):

- Η παραβίαση της εμπιστευτικότητας ορίζεται ως η προσπέλαση ενός πόρου από μη εξουσιοδοτημένη οντότητα.
- Η παραβίαση της ακεραιότητας περιλαμβάνει την αλλοίωση ενός πόρου από μη εξουσιοδοτημένη οντότητα.
- Η παραβίαση της διαθεσιμότητας αφορά στην περίπτωση όπου το αγαθό/υπηρεσία δεν είναι διαθέσιμο/η όταν μια εξουσιοδοτημένη οντότητα χρειάζεται να το/την προσπελάσει.

Ένα παράδειγμα για να κατανοηθεί ο τρόπος ανάλυσης ενός κινδύνου, είναι η προστασία των δεδομένων μισθοδοσίας που τηρεί το Τμήμα Ανθρώπινου Δυναμικού και το Λογιστήριο. Για να προστατευτεί η επιχείρηση από τον κίνδυνο απώλειας των δεδομένων αυτών, θα πρέπει να υλοποιήσει το μέτρο δημιουργίας αντιγράφων ασφάλειας (back-up control). Συνεπώς, αν τα δεδομένα δεν είναι διαθέσιμα (παραβίαση της διαθεσιμότητας), θα χρησιμοποιηθούν τα σχετικά αντίγραφα. Ομοίως, ενδέχεται να υπάρξει αλλοίωση των δεδομένων αυτών, που μπορεί να είναι είτε ηθελημένη είτε αποτέλεσμα ενός ανθρώπινου ή συστημικού λάθους. Σε αυτή την περίπτωση, ένα αποδοτικό μέτρο ασφάλειας είναι μια διαδικασία που θα ορίζει τον έλεγχο των σχετικών στοιχείων από τουλάχιστον έναν επιπλέον υπάλληλο (4-eyes principle), ώστε να εντοπιστεί έγκαιρα το λάθος και να διορθωθεί.

Αφού λοιπόν αναγνωριστούν και αναλυθούν όλοι οι σχετικοί κίνδυνοι, η επιχείρηση καλείται να υλοποιήσει τα μέτρα ασφάλειας που έχουν επιλεγεί. Όμως, στην πλειονότητα των περιπτώσεων, δεν είναι δυνατόν να δημιουργηθούν όλα αυτά τα μέτρα, καθώς η υλοποίησή τους είναι μια διαδικασία που επηρεάζεται από διάφορους παράγοντες. Για παράδειγμα, δεδομένου πως ενδέχεται να υπάρξει οικονομικό κόστος (π.χ. αγορά ενός εξειδικευμένου λογισμικού), θα πρέπει η επιχείρηση να το λάβει υπόψη στον σχετικό προϋπολογισμό. Έτσι, καθορίζονται οι προτεραιότητες ανάλογα με την κρισιμότητα των μέτρων αυτών, σε σχέση με τα αγαθά/υπηρεσίες που προστατεύουν. Παράλληλα, απαιτείται να καθοριστεί η διάθεση ανάληψης κινδύνων (risk appetite), στην οποία απεικονίζεται ο κίνδυνος τον οποίο μπορεί να «ανεχτεί» η επιχείρηση χωρίς να υλοποιήσει κανένα μέτρο προστασίας. Οι σχετικές τιμές υπολογίζονται στο επίπεδο επίπτωσης, π.χ. οικονομικές ζημιές, λειτουργικές ζημιές, επίπτωση στην υστεροφημία της επιχείρησης κλπ.

ΝΙΚΟΣ ΤΣΑΛΗΣ, PhD

ΑΠΟΔΟΤΙΚΟ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΩΝ

Σύμφωνα με τον διεθνή οργανισμό προτύπων NIST, η εφαρμογή ενός αποδοτικού Συστήματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας πρέπει να έχει τα εξής χαρακτηριστικά:

1. Διαρκή καθοδήγηση από τη διοίκηση της επιχείρησης.
2. Υποστήριξη και συμμετοχή του τμήματος πληροφορικής.
3. Ικανή ομάδα διαχείρισης κινδύνων.
4. Ευαισθητοποίηση και συνεργασία όλων των υπαλλήλων.
5. Διαρκή ανάλυση των σχετικών κινδύνων.

ΕΝΑΛΛΑΚΤΙΚΕΣ ΛΥΣΕΙΣ

Συνεπώς, στο παραπάνω παράδειγμα της προστασίας των δεδομένων μισθοδοσίας, υπάρχουν και άλλες εναλλακτικές λύσεις που θα μπορούσαν να εφαρμοστούν. Η αντιμετώπιση των σχετικών κινδύνων μέσα από την εφαρμογή μέτρων μετριασμού/μείωσης (risk mitigation/reduction) είναι η πιο συχνή επιλογή, τουλάχιστον για τα περισσότερα αγαθά/υπηρεσίες της επιχείρησης. Αυτή ήταν και η επιλογή που επιλέχθηκε στο παραπάνω παράδειγμα. Εναλλακτικά, η επιχείρηση ενδεχομένως να αποφάσιζε πως δεν χρειάζεται πλέον το αγαθό/υπηρεσία αυτό/ή και δεν αξίζει να υλοποιήσει τα σχετικά μέτρα προστασίας για να μετριάσει τον σχετικό κίνδυνο. Σε αυτή την περίπτωση, αποφασίζεται η μη χρήση του συγκεκριμένου αγαθού/υπηρεσίας (risk avoidance) και η αφαίρεσή του/της από το ενεργητικό της επιχείρησης. Ομοίως, θα μπορούσε να γίνει μεταφορά του κινδύνου (risk transfer), συνήθως μέσω της χρήσης ασφαλιστικών υπηρεσιών, ή αποδοχή του κινδύνου (risk acceptance) χωρίς να υλοποιηθεί οποιοδήποτε μέτρο προστασίας. Η τελευταία επιλογή είναι άρρηκτα συνδεδεμένη με τη διάθεση ανάληψης κινδύνων (risk appetite) της επιχείρησης, που αναλύθηκε παραπάνω.

ΔΙΑΡΚΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗ

Το τελευταίο βήμα της διαδικασίας διαχείρισης κινδύνων είναι η διαρκής παρακολούθηση, συντήρηση και βελτίωση του σχετικού συστήματος. Το σύνολο αυτών των ενεργειών θα πρέπει να εκτελείται ανά τακτά χρονικά διαστήματα και έχει ως στόχο τη συνεχή βελτίωση του συστήματος, με γνώμονα τις αλλαγές που διέπουν τη λειτουργία της επιχείρησης και τους σχετικούς κινδύνους.

Η διαδικασία αυτή απαιτεί την ορθή εκτέλεση όλων των βημάτων που απαιτούνται, για να μπορέσει η επιχείρηση να διασφαλίσει ότι έχει αναπτύξει ένα επαρκές πλαίσιο προστασίας από τους κινδύνους που εντοπίζονται στο περιβάλλον της Κυβερνοασφάλειας.

Ένα σύνηθες σφάλμα που γίνεται, είναι η λανθασμένη αποτίμηση των κινδύνων και πιο συγκεκριμένα η εκτίμηση της πιθανότητας του κινδύνου να πραγματοποιηθεί – όσο απίθανο και αν είναι να πραγματοποιηθεί ένας κίνδυνος, αυτό δεν σημαίνει πως δεν πρέπει να υπάρχουν αντίστοιχα μέτρα ασφάλειας. Η κρισιμότητα και η πιθανότητα πραγματοποίησης ενός κινδύνου, οι οποίες καθορίζονται στο στάδιο της ανάλυσης επικινδυνότητας, επηρεάζουν τον τρόπο με τον οποίο θα αντιμετωπιστεί ο κίνδυνος. Για παράδειγμα, αν το ιστορικό ενός κινδύνου παρουσιάζει ότι εμφανίζεται σπάνια και παράλληλα έχει μικρή επίπτωση, τότε ενδεχομένως να επιλεγεί ένα λιγότερο ισχυρό μέτρο προστασίας ή ακόμα και να γίνει αποδοχή του συγκεκριμένου κινδύνου, χωρίς λήψη οποιουδήποτε μέτρου προστασίας. Αντιθέτως, αν ο κίνδυνος έχει μέτρια συχνότητα και αντίστοιχη επίπτωση, τότε θα πρέπει να γίνει προεργασία για το πώς θα αντιμετωπιστεί. Οι παραπάνω περιπτώσεις, συμπεριλαμβανομένων και όλων των πιθανών συνδυασμών, είναι στοιχεία που υπολογίζονται κατά την ανάλυση επικινδυνότητας. Η αντιμετώπιση των κινδύνων μιας επιχείρησης θα πρέπει να γίνεται μεθοδικά, από ειδικούς εμπειρογνώμονες που έχουν την απαιτούμενη τεχνογνωσία, για να επιτευχθεί το καλύτερο δυνατό αποτέλεσμα.

ΥΠΟΧΡΕΩΣΗ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ Η ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Είναι εμφανές πως η εφαρμογή ενός αποδοτικού Συστήματος Διαχείρισης Κινδύνων Κυβερνοασφάλειας θα ωφελήσει και θα ενισχύσει την προστασία του περιβάλλοντος λειτουργίας της επιχείρησης.

WHO IS WHO

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, 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 επαγγελματικών τίτλων από τους οργανισμούς Offensive Security και ISACA, σχετικά με τον έλεγχο ασφάλειας πληροφοριακών συστημάτων και υποδομών.
n.tsalis@logicom.net
www.logicomsolutions.com.cy

«Η ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΩΝ ΚΙΝΔΥΝΩΝ ΜΙΑΣ ΕΠΙΧΕΙΡΗΣΗΣ ΘΑ ΠΡΕΠΕΙ ΝΑ ΓΙΝΕΤΑΙ ΜΕΘΟΔΙΚΑ, ΑΠΟ ΕΙΔΙΚΟΥΣ ΕΜΠΕΙΡΟΓΝΩΜΟΝΕΣ ΠΟΥ ΕΧΟΥΝ ΤΗΝ ΑΠΑΙΤΟΥΜΕΝΗ ΤΕΧΝΟΓΝΩΣΙΑ, ΓΙΑ ΝΑ ΕΠΙΤΕΥΧΘΕΙ ΤΟ ΚΑΛΥΤΕΡΟ ΔΥΝΑΤΟ ΑΠΟΤΕΛΕΣΜΑ»

ΛΥΣΕΙΣ ΠΡΟΛΗΨΗΣ ΚΑΙ ΠΡΟΣΤΑΣΙΑΣ ΕΝΑΝΤΙΑ ΣΤΟ RANSOMWARE ΑΠΟ ΤΗ LOGICOM SOLUTIONS

Η καλύτερη προστασία από κακόβουλο λογισμικό τύπου Ransomware ή/και Malware θεωρείται η έγκαιρη πρόληψη των κυβερνο-απειλών. Η Logicom Solutions, ως Cisco Gold Certified Partner, προσφέρει άμεσες και γρήγορες λύσεις πρόληψης και προστασίας ενάντια στο Ransomware. Λύσεις όπως τα Cisco Cloud Email Security, Cisco Umbrella και Cisco Advanced Malware Protection for Endpoints βασίζονται σε τεχνολογίες Cloud και προσφέρονται για άμεση πρόληψη (Cisco Quick Prevention) από επιθέσεις Ransomware.

Επίσης, η λύση Cloud Email Security της Cisco αποτρέπει την πρόσβαση του Ransomware μέσω κακόβουλων emails. Μέσω της λύσης Cisco Umbrella, ο χρήστης είναι προστατευμένος και εντός και εκτός δικτύου, καθώς εμποδίζεται η είσοδος του Ransomware από όλες τις πιθανές διαδικτυακές διόδους. Τέλος, η λύση Cisco Advanced Malware Protection for Endpoints προστατεύει τον υπολογιστή από το να τεθεί σε ομηρία από κακόβουλο λογισμικό. Πέρα από την άμεση πρόληψη, η Cisco προσφέρει και υψηλή προστασία από κυβερνο-επιθέσεις μέσω των λύσεων Advanced Protection, με μια σειρά λύσεων και υπηρεσιών που διασφαλίζουν υψηλή κυβερνο-ασφάλεια. Παραδείγματα τέτοιων λύσεων που εντοπίζουν και αποτρέπουν επιθέσεις είναι τα Cisco Next Generation Firewall, Cisco Identity Services Engine, Cisco TrustSec και Cisco StealthWatch.

Καταρχήν, καλύπτει τις απαιτήσεις των βέλτιστων πρακτικών ασφάλειας, καθώς και της σχετικής νομοθεσίας (π.χ. GDPR). Η επιχείρηση είναι υποχρεωμένη να προστατεύσει τα δεδομένα τόσο των υπαλλήλων της όσο και των πελατών και συνεργατών της. Συνεπώς, απαιτείται να αναλύσει επαρκώς τους σχετικούς κινδύνους και να εφαρμόσει τα κατάλληλα μέτρα προστασίας. Παράλληλα, αιτιολογείται επαρκώς το κόστος της επένδυσης στην επιλογή των απαραίτητων μέτρων προστασίας, καθώς, όπως αναφέρθηκε, ο προϋπολογισμός της επιχείρησης κατέχει σημαντικό ρόλο και επηρεάζει σε μεγάλο βαθμό τη λήψη των σχετικών αποφάσεων.

Πέρα από τα πιο πάνω άμεσα ωφελήματα, υπάρχουν και αρκετά έμμεσα, τα οποία αφορούν στη λειτουργία της επιχείρησης. Αρχικά, ενισχύεται το στοιχείο της επικοινωνίας και της κατανόησης του εσωτερικού περιβάλλοντος, δεδομένου ότι το πλαίσιο απαιτεί τη συνεργασία όλων των τμημάτων, με στόχο την αποτελεσματική αντιμετώπιση των κινδύνων που απειλούν την επιχείρηση. Επίσης, δημιουργείται μια ανεπτυγμένη κουλτούρα/νοοτροπία που προωθεί διεθνείς βέλτιστες πρακτικές διαχείρισης κινδύνων και ενισχύει την επαγγελματική θέση της επιχείρησης.

Όλες οι επιχειρήσεις αντιμετωπίζουν διάφορους κινδύνους που απειλούν τις δραστηριότητες και τα αγαθά/υπηρεσίες που προσφέρουν. Για τον λόγο αυτό, είναι απαραίτητο να αναπτύξουν ένα αποτελεσματικό σύστημα αντιμετώπισης κινδύνων, ώστε να ελαχιστοποιήσουν τις επιπτώσεις από αυτούς. Αν αποτύχουν σε αυτό, τότε θα έρθουν αντιμέτωπες με σοβαρές επιπτώσεις/συνέπειες, για τις οποίες θα πρέπει να μοχθήσουν αρκετά, προτού καταφέρουν να επιστρέψουν στην αρχική τους κατάσταση. Η δημιουργία συστήματος αντιμετώπισης κινδύνων αποτελείται από συγκεκριμένα, εύκολα βήματα, που, αν εκτελεστούν σωστά, θα επιφέρουν το καλύτερο δυνατό αποτέλεσμα σχετικά με τη λήψη αποφάσεων για το ποια αγαθά/υπηρεσίες πρέπει να προστατευτούν και με ποιον τρόπο. Επιπλέον, κατά τη διαδικασία της δημιουργίας συστήματος αντιμετώπισης κινδύνων, η επιχείρηση θα κερδίσει πολλαπλά ωφελήματα, αφού μέσα από αυτήν θα καταφέρει να ωριμάσει, τόσο τεχνικά όσο και οργανωτικά, και θα δημιουργήσει μια επαγγελματική κουλτούρα/νοοτροπία που θα υποστηρίζει και θα προωθεί την Κυβερνοασφάλεια.

Πέρα όμως από τις πιο πάνω βέλτιστες πρακτικές, οι επιχειρήσεις θα πρέπει να εισαγάγουν και τεχνολογίες ασφάλειας για την προστασία των υποδομών πληροφορικής και επικοινωνίας. Εξειδικευμένοι κατασκευαστές τεχνολογιών ασφάλειας, όπως η Cisco Systems, προσφέρουν μια ολιστική προσέγγιση στην ασφάλεια των υποδομών πληροφορικής και επικοινωνίας για τις επιχειρήσεις. Τέτοιες λύσεις είναι η ευρεία γκάμα της Cisco Systems για Quick Prevention καθώς και η γκάμα λύσεων για Advanced Prevention.