

ΔΡ. ΓΙΑΝΝΗΣ ΗΛΙΑΔΗΣ*
Διευθυντής Υποδομών Πληροφορικής στην **ΤΕΙΡΕΣΙΑΣ Α.Ε.**
Πρόεδρος του ΔΣ του **ISC2 Hellenic Chapter**

Ο ΤΕΛΕΙΟΣ CISO ΣΕ ΤΡΙΑ ΒΗΜΑΤΑ

Στην εποχή του ψηφιακού μετασχηματισμού, ο ρόλος του CISO μετεξελίσσεται από διαχειριστής της Ασφάλειας Πληροφοριών σε κεντρική φιγούρα που συμβάλλει στη διαμόρφωση της στρατηγικής κατεύθυνσης των οργανισμών.



Καθώς οι απειλές στον κυβερνοχώρο γίνονται πιο περίπλοκες, η πίεση στους CISO να προστατεύσουν τους οργανισμούς τους, ενώ παράλληλα να επιτρέπουν την ανάπτυξη τους, έχει αυξηθεί. Η ιδέα του να γίνει κάποιος ο "τέλειος" CISO μπορεί να φαίνεται άπιαστη, όμως το μονοπάτι βελτίωσης υπάρχει. Τρία θεμελιώδη βήματα από τους CISO, μπορούν να καθοδηγήσουν αυτήν τη βελτίωση:

1. να καθιερώσουν τους εαυτούς τους ως ηγέτες στην Ασφάλεια Πληροφοριών,
2. να βοηθήσουν τα ενδιαφερόμενα μέρη (stakeholders) να επαναπροσδιορίσουν την Ασφάλεια ως Κέντρο Επενδύσεων,
3. να τελειοποιήσουν την τέχνη της επικοινωνίας.

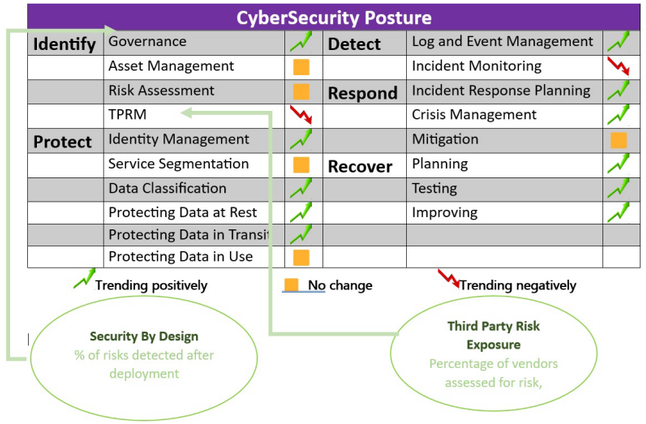
ΒΗΜΑ 1. ΚΑΘΙΕΡΩΣΤΕ ΤΟΝ ΕΑΥΤΟ ΣΑΣ ΩΣ ΗΓΕΤΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

Η ηγεσία στην Ασφάλεια Πληροφοριών ξεπερνά τη διαχείριση των firewalls και των συστημάτων ανίχνευσης εισβολών και εδράζεται στη θέσπιση ενός οράματος Ασφάλειας και την καθοδήγηση του οργανισμού μέσα στις πολύπλοκες διαδρομές του κυβερνοχώρου. Ένας αποτελεσματικός CISO διαθέτει όχι μόνο τεχνική εμπειρογνωμοσύνη, αλλά και την ικανότητα να καθοδηγήσει την αλλαγή στον οργανισμό, έχοντας φροντίσει πρώτα να βοηθήσει στον καθορισμό της διάθεσης του οργανισμού για ανάληψη κυβερνοκινδύνων (risk appetite).

Η στρατηγική επιρροή του CISO εκτείνεται πέρα από την ασφάλεια, επηρεάζοντας τις επιχειρηματικές αποφάσεις. Για παράδειγμα, σε μια επιχείρηση που στοχεύει στην ταχεία ψηφιακή ανάπτυξη, ο CISO συμμετέχει ενεργά στις συζητήσεις για τον τρόπο με τον οποίο τα ψηφιακά προϊόντα και υπηρεσίες θα προστατεύονται εκ του αρχικού σχεδιασμού, με στόχο την αποφυγή απειλών αλλά και την ενίσχυση της ανταγωνιστικής θέσης της εταιρείας στην αγορά.

Ένας CISO με στρατηγική επιρροή είναι ικανός να κατανοήσει τις επιχειρηματικές προτεραιότητες και να τις ενσωματώσει στις στρατηγικές ασφαλείας πληροφοριών. Αντί να θεωρείται η ασφάλεια ως εμπόδιο για την καινοτομία, ο CISO θα αναδείξει την ασφάλεια ως καταλύτη για την υλοποίηση καινοτόμων πρωτοβουλιών με αξιοπιστία.

Μέτρηση Απόδοσης και KPIs: Η αποτελεσματική ηγεσία απαιτεί επίσης εστίαση στη μέτρηση της απόδοσης. Οι CISOs εφαρμόζουν δείκτες απόδοσης (KPIs) που είναι σαφείς, μετρήσιμοι και άμεσα συνδεδεμένοι με τα επιχειρηματικά αποτελέσματα, αποδεικνύοντας την αξία των επενδύσεων στην ασφάλεια. Για παράδειγμα, ένας δείκτης "Ασφάλεια εκ του Σχεδιασμού", ο οποίος αποτυπώνει το ποσοστό των κινδύνων που έχουν εντοπισθεί σε κάποια υπηρεσία μετά τον αρχικό σχεδιασμό αυτής. Αυτός ο δείκτης μπορεί να δώσει μια σαφή εικόνα της προληπτικής προσέγγισης της επιχείρησης απέναντι στους κινδύνους και της ικανότητάς της να προστατεύει κρίσιμες επιχειρηματικές λειτουργίες έγκαιρα, αποτελεσματικά και αποδοτικά. Επίσης, στην εποχή μας που οι επιθέσεις σε αλυσίδες εφοδιασμού γίνονται ολοένα και πιο συχνές, ένας δείκτης που κερδίζει συνεχώς την προσοχή των επιχειρήσεων είναι η "Έκθεση σε Κίνδυνο από Τρίτους", που θα μπορούσε να περιέχει το ποσοστό των προμηθευτών που έχουν αξιολογηθεί για τον κίνδυνο και την αξιολόγησή αυτών (π.χ. μέσο όρο αξιολόγησης και διακύμανση).





ΒΗΜΑ 2. ΕΠΑΝΑΠΡΟΣΔΙΟΡΙΣΤΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΩΣ ΚΕΝΤΡΟ ΕΠΕΝΔΥΣΕΩΝ

Παραδοσιακά, η Ασφάλεια Πληροφοριών θεωρείτο ως ένα κέντρο κόστους, ένας τομέας όπου δαπανώνται χρήματα χωρίς άμεση απόδοση. Ωστόσο, το εξελισσόμενο τοπίο απειλών και η αυξανόμενη ενσωμάτωση των ψηφιακών τεχνολογιών σε κάθε πτυχή της επιχείρησης αποτελούν εφαλτήρια για την ανάδειξη της αντιπαραγωγικής διάστασης της εν λόγω άποψης περί κέντρου κόστους. Για να επιτύχει ένας CISO, είναι κρίσιμο να επαναπροσδιορίσει την Ασφάλεια Πληροφοριών ως ένα κέντρο επενδύσεων.

Ευθυγράμμιση των Επενδύσεων Ασφάλειας με τους Επιχειρηματικούς Στόχους: Ένα από τα πιο σημαντικά καθήκοντα του CISO είναι να διασφαλίσει ότι οι επενδύσεις στην Ασφάλεια ευθυγραμμίζονται με τους στρατηγικούς στόχους του οργανισμού. Αυτό απαιτεί βαθιά κατανόηση της επιχείρησης και των στόχων της. Αξιοποιώντας την Ασφάλεια ως μοχλό επιτυχίας των επιχειρήσεων, οι CISOs μπορούν να αλλάξουν το κύριο θέμα στη συζήτηση περί Ασφάλειας από το κόστος των αντιμέτρων (θεώρηση ως κέντρο κόστους) στη δημιουργία αξίας (θεώρηση ως κέ-



ντρο επένδυσης). Ο CISO κατανοεί ότι οι επενδύσεις στην Ασφάλεια δεν είναι μονοδιάστατες. Αντί να επικεντρωθεί αποκλειστικά στην προστασία από επιθέσεις, εξετάζει τους τρόπους με τους οποίους η Ασφάλεια μπορεί να υποστηρίξει την ανάπτυξη νέων επιχειρηματικών μοντέλων, τη συμμόρφωση με τους κανονισμούς, ή ακόμη και την ενίσχυση της φήμης της επιχείρησης. Με αυτόν τον τρόπο, η Ασφάλεια γίνεται μια στρατηγική επένδυση που προσθέτει αξία σε πολλαπλά επίπεδα.

Πόση επένδυση στην Ασφάλεια χρειαζόμαστε; Ένα από τα πιο σημαντικά στοιχεία στη διαχείριση των κινδύνων είναι η διάθεση για ανάληψη κινδύνου (risk appetite) που έχει κάθε οργανισμός, η οποία επηρεάζει τις στρατηγικές αποφάσεις που λαμβάνονται. Ο CISO δημιουργεί ένα αξιόπιστο και εύληπτο πλαίσιο εταιρικής διακυβέρνησης κυβερνοκινδύνων, ώστε η ηγεσία να είναι σε θέση (α) να εκτιμήσει τη διάθεση της επιχείρησης για ανάληψη κινδύνου και (β) να αποδεχθεί τον υπολειπόμενο κίνδυνο βάσει ενημερωμένων αποφάσεων που αποσκοπούν σε κερδοφόρα αποτελέσματα. Με αυτόν τον τρόπο, ο οργανισμός καθορίζει ποιες απειλές πρέπει να αντιμετωπιστούν άμεσα και ποιες μπορούν εξετασθούν σε μελλοντικό χρόνο, επιτρέποντας την αποδοτική κατανομή πόρων, την αποτελεσματική αντιμετώπιση των κινδύνων και συμβάλλοντας στη βιωσιμότητα της επιχείρησης και την κερδοφορία των επιχειρηματικών δραστηριοτήτων..

ΒΗΜΑ 3. ΤΕΛΕΙΟΠΟΙΗΣΤΕ ΤΗΝ ΤΕΧΝΗ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

Η επικοινωνία αποτελεί κλειδί για την επιτυχία ενός CISO. Η τεχνική ορολογία δεν έχει θέση όταν ο CISO απευθύνεται σε κοινό εκτός του τομέα της Ασφάλειας Πληροφοριών. Αντίθετα, πρέπει να προσαρμόζει το στυλ και το μήνυμά του ανάλογα με το ακροατήριο, εξηγώντας τα θέματα Ασφάλειας με όρους που κατανοούν οι επιχειρηματικοί ηγέτες.

Προσαρμογή του Μηνύματος στο Ακροατήριο - Κατ' αρχάς, είναι χρήσιμο να θυμόμαστε ότι η χρήση κάποιας γλώσσας με άρτια παράθεση αλλεπάλληλων τεχνικών όρων είναι άκρως αποτελεσματική μόνο όταν «ομιλούμε» σε υπολογιστικά συστήματα Ασφάλειας Πληροφοριών, μεταφέροντας σε αυτά οδηγίες και εντολές. Για την επικοινωνία με συνάδελφους, σε οποιαδήποτε βαθμίδα, πρέπει να χρησιμοποιούμε την γλώσσα που ομιλείται συνήθως στην επιχείρηση όπου εργαζόμαστε.

Η αποτελεσματικότητα της επικοινωνίας έγκειται στην ικανότητα προσαρμογής του μηνύματος στο ακροατήριο. Ενώ μια εις βάθος ανάλυση των τεχνικών πτυχών της κρυπτογράφησης "AES" μπορεί να είναι ενδιαφέρουσα για ένα εξαιρετικά μικρό ποσοστό στελεχών, είναι πιθανό να μην έχει το προσδοκώμενο αποτέλεσμα προς ένα μέλος της ανώτατης διοικητικής ομάδα της επιχείρησης. Αντίθετα, σε αυτήν την περίπτωση ο CISO θα επικεντρωθεί στα θετικά αποτελέσματα της χρήσης ισχυρής κρυπτογράφησης, όπως η διατήρηση της εμπιστευτικότητας των δεδομένων των πελατών και η αποφυγή προστίμων λόγω κανονιστικών παραβάσεων.

Η προσαρμογή του μηνύματος στο ακροατήριο δεν αφορά μόνο στην απλοποίηση της γλώσσας. Ο CISO είναι σε θέση να αντιλαμβάνεται τις προτεραιότητες του ακροατηρίου του και να συνδέει τα ζητήματα ασφαλείας με αυτές. Για παράδειγμα, όταν απευθύνεται στο τμήμα μάρκετινγκ, μπορεί να τονίσει τον τρόπο με τον οποίο η Ασφάλεια διατηρεί σε υψηλά επίπεδα την εμπιστοσύνη των πελατών και προστατεύει την φήμη της εταιρείας.

Ψυχολογικές Πτυχές στην Επικοινωνία - Η κατανόηση και αξιοποίηση των ψυχολογικών αρχών μπορεί να ενισχύσει σημαντικά την ικανότητα του CISO να επικοινωνεί αποτελεσματικά. Θα αναφερθούμε σε δύο ενδεικτικά παραδείγματα: αποφυγή ζημίας (loss aversion) και μη ανακτήσιμο κόστος (sunk cost). Σύμφωνα με την αποφυγή ζημίας (loss aversion), οι άνθρωποι τείνουν να αποφεύγουν τη ζημιά περισσότερο από ό,τι επιδιώκουν το κέρδος. Αυτή η αρχή μπορεί να χρησιμοποιηθεί στην επικοινωνία για να ενισχύσει την επιθυμία για δράση. Έστω ότι η επιχείρηση σκοπεύει να προμηθευθεί ένα προϊόν των 5.000€ στους επόμενους 12 μήνες και γνωρίζετε ότι η τιμή του θα αυξηθεί 20% τον Φεβρουάριο. Βάσει της αρχής του loss aversion, είναι προτιμότερο να αναφέρουμε ότι η επιχείρηση θα τύχει έκπτωσης 17% για το εν λόγω προϊόν εφόσον το προμηθευθεί μέχρι τον Φεβρουάριο (αντί αύξησης 20% μετά το Φεβρουάριο), διότι αυτό θα δημιουργήσει επιπρόσθετο κίνητρο σε όλα τα στελέχη να ολοκληρώσουν την αλλαγή (προμήθεια, υλοποίηση, αλλαγές διαδικασίας κτλ) προκειμένου να μην απωλέσει η επιχείρηση την έκπτωση 17% (loss aversion).

Το φαινόμενο του μη ανακτήσιμου κόστους (sunk cost) περιγράφει την τάση των ανθρώπων να συνεχίζουν να επενδύουν σε κάτι στο οποίο έχουν ήδη δαπανήσει πόρους. Αυτό μπορεί να αξιοποιηθεί στην επικοινωνία για να ενθαρρύνει τους ανθρώπους να ολοκληρώσουν μια διαδικασία ή να κάνουν μια πρόσθετη επένδυση. Ας εξετάσουμε την περίπτωση ενός έργου «ασφαλούς απομακρυσμένης πρόσβασης» μέσω της (α) άμεσης υλοποίησης ενός VPN κόστους 20.000€ για τους χρήστες ενός οργανισμού και της (β) μετέπειτα προμήθειας ενός προϊόντος 2FA κόστους 5.000€ για το VPN. Είναι δύο βήματα (VPN, 2FA) και θα χρειαστεί να διαχειριστούμε την αλλαγή δύο φορές (να αιτιολογήσουμε στα διοικητικά στελέχη την ανάγκη προμήθειας, να πείσουμε τους συνάδελφους που θα το χρησιμοποιούν για τη χρησιμότητα της λύσης, να άρουμε όποια (τεχνικά ή μη) εμπόδια υπάρχουν στην υλοποίησή της, να υποστηρίξουμε τη διαδικασία υλοποίησης κτλ).

Όταν ξεκινήσουμε το 2ο έργο (2FA), η αντίσταση στην αλλαγή που θα συναντήσουμε (π.χ. μη αναγνώριση της ανάγκης της επένδυσης, δυσκολίες στην προμήθεια του προϊόντος, τεχνικά εμπόδια και χρονικές καθυστερήσεις στην υλοποίηση) ίσως θέσουν σε κίνδυνο την υπηρεσία «ασφαλής απομακρυσμένη πρόσβαση». Αντιθέτως, αν προχωρήσουμε στην αρχική προμήθεια ενός VPN κόστους 25.000€, το οποίο συνοδεύεται (bundle) από μία υποδομή 2FA, τότε η υλοποίηση 2FA θα γίνει στα πλαίσια της ίδιας αλλαγής (προμήθεια, αποδοχή από χρήστες, υλοποίηση κτλ) καθώς θα είναι ένα μη ανακτήσιμο κόστος που όλα τα στελέχη θα αναγνωρίζουν ότι οφείλουν να αξιοποιήσουν.

ΕΠΙΛΟΓΟΣ

Ο δρόμος προς την τελειότητα διέρχεται μέσα από στάσεις κατά τις οποίες ο CISO αναπτύσσει τις επαγγελματικές ικανότητές ηγεσίας, στρατηγικής σκέψης και αποτελεσματικής επικοινωνίας. Καθιερώνοντας τον εαυτό του ως ηγέτη της Ασφάλειας Πληροφοριών στην επιχείρηση, επαναπροσδιορίζοντας την Ασφάλεια ως κέντρο επενδύσεων και διαπρέποντας στην επικοινωνία, ο CISOs είναι σε θέση να διαχειριστεί καλύτερα τις αλλαγές, να προστατεύσει την επιχείρηση αλλά και να δημιουργήσει τις συνθήκες Ασφάλειας που θα συνδράμουν στην επίτευξη περισσότερων και μεγαλύτερων επιτυχιών του οργανισμού στον οποίο εργάζεται.

**Ο Δρ. Γιάννης Ηλιάδης, CISSP, C|CISO, CRISC είναι Διευθυντής Υποδομών Πληροφορικής στην ΤΕΙΡΕΣΙΑΣ Α.Ε. Επίσης, είναι Πρόεδρος του ΔΣ του ISC2 Hellenic Chapter. Οι απόψεις που εκφράζονται στο παρόν είναι αποκλειστικά του συγγραφέα και δεν εκφράζουν απαραίτητα τις απόψεις ή τις γνώμες οποιουδήποτε τρίτου ή εργοδότη.*

