Μη ύπαρξη MFA σημαίνει μη ασφαλίσιμη εταιρία

Η εκρηκτική αύξηση των επιθέσεων ransomware - οι οποίες δεν περιορίζονται από γεωγραφικά όρια - σε συνδυασμό με τη χρήση της τεχνητής νοημοσύνης και της μηχανικής μάθησης που εξελίσσει τις απειλές παγκοσμίως, καθιστούν οποιαδήποτε εταιρία δυνητικό θύμα τους και αυξάνουν τον αριθμό των ζημιών των ασφαλιστικών εταιριών δραματικά.

Η επανεκτίμηση συνοδεύτηκε με μεγαλύτερο έλεγχο των τεχνικών και οργανωτικών μέτρων κάθε εταιρίας για την αντιμετώπιση περιστατικών παραβίασης, με χρήση ειδικού λογισμικού εξέτασης των συστημάτων της, με αλλαγές των παρεχόμενων καλύψεων, με μείωση ορίων ασφαλιστικής κάλυψης , εισαγωγή συνασφάλισης , αύξηση απαλλαγών και μεγάλες αυξήσεις ασφαλίστρων.

Η νέα πολιτική ανάληψης κινδύνου ζητά από τον ασφαλισμένο ή την υπό ασφάλιση εταιρία να αποδείξει ότι έχει εφαρμόσει ενισχυμένα επίπεδα ελέγχου ασφάλειας για την πρόληψη, τον εντοπισμό και την ανταπόκριση στα σημερινά εξελιγμένα περιστατικά παραβίασης ασφάλειας.

Η έλλειψη των παρακάτω υποδομών καθιστά τις εταιρίες μη ασφαλίσιμες

1.'Ελεγχος πρόσβασης χρήστη μέσω ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) και η χρήση Εικονικού Ιδιωτικού Δικτύου (VPN) για απομακρυσμένη πρόσβαση. Η επιβολή χρήσης ισχυρής πολιτικής κωδικών πρόσβασης, η απαίτηση της χρήσης ελέγχου ταυτότητας πολλαπλών παραγόντων, η εκπαίδευση των εργαζομένων σχετικά με επιθέσεις phishing που έχουν σχεδιαστεί για την κλοπή διαπιστευτηρίων σύνδεσης και η χρήση Εικονικού Ιδιωτικού Δικτύου (VPN) για απομακρυσμένη πρόσβαση στα εταιρικά συστήματα είναι όλα κρίσιμα στοιχεία της στρατηγικής ασφάλειας στον κυβερνοχώρο ενός οργανισμού. Μη ύπαρξη MFA


Νίκος Γεωργόπουλος
cyRM, MBA, CDPO, Cyber Privacy Insurance Advisor – Cromar Insurance Brokers, Co – Founder The DPO Academy
LinkedIn: https://www.linkedin.com/in/nikos-georgopoulos/

σημαίνει μη ασφαλίσιμη εταιρία.

2.Εκπαίδευση ευαισθητοποίησης του Ανθρώπινου Δυναμικού στον κυβερνοχώρο. Ο πιο δημοφιλείς τρόπος διάδοσης κακόβουλου λογισμικού ransomware είναι τα μηνύματα ηλεκτρονικού ψαρέματος (phishing). Όταν ο χρήστης κάνοντας κλικ σε έναν σύνδεσμο ή να ανοίξει ένα συνημμένο κακόβουλο λογισμικό, οι εγκληματίες του κυβερνοχώρου μπορούν να αποκτήσουν πρόσβαση στον υπολογιστή του χρήστη και στο εταιρικό δίκτυο. Η έλλειψη εκπαίδευσης ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας για την προστασία του οργανισμού από το ransomware. Το μεγαλύτερο ποσοστό περιστατικών παραβίασης ασφάλειας οφείλεται σε ανθρώπινο λάθος και τουλάχιστον ένας στους τρείς ανεκπαίδευτους χρήστες πέφτουν θύματα περιστατικών ransomware.

3.'Υπαρξη αντίγραφου ασφαλείας δεδομένων και ελεγμένες διαδικασίες ανάκτησής τους.Ο στόχος του ransomware είναι να αναγκάσει την εταιρία θύμα να πληρώσει λύτρα προκειμένου να αποκτήσει ξανά πρόσβαση στα κρυπτογραφημένα δεδομένα του. Η βιομηχανία του ransomware πλέον δεν αρκείται μόνο στο κλείδωμα των αρχείων αλλά και στην απειλή δημοσίευσης των δεδομένων που έχουν έρθει στην κατοχή τους πριν την εκδήλωση του εκβιασμού. Για να καταβάλλει μία εταιρία θύμα θα πρέπει να μην έχει δυνατότητα πρόσβασης σε αυτά. Μια σωστή διαδικασία δημιουργίας αντιγράφων ασφαλείας δεδομένων με ελεγμένη διαδικασία ανάκτησής της είναι ένας αποτελεσματικός τρόπος για να μετριαστεί ο κίνδυνος μιας επίθεσης ransomware.

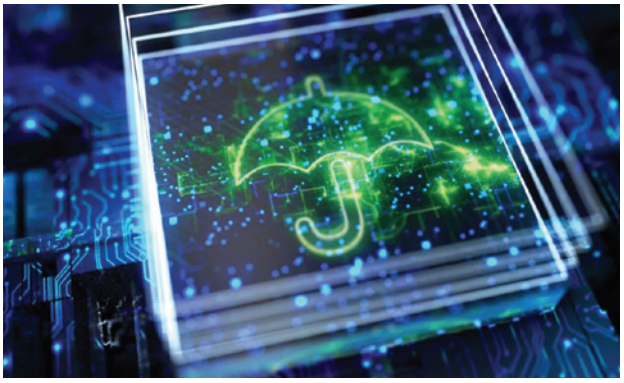
4. Εγκατάσταση ενημερώσεων διορθώσεων προγραμμάτων. Η εγκατάσταση ενημερώσεων διορθώσεων προγραμμάτων ειδικά εκείνων που χαρακτηρίζονται ως κρίσιμες μπορεί να συμβάλει στον περιορισμό των ευπαθειών ενός οργανισμού σε επιθέσεις ransomware.

Ανταγωνιστικό πλεονέκτημα η ασφάλιση

Η **ασφάλιση πλέον θα πρέπει να αντιμετωπίζεται σαν εταιρική υποδομή** η οποία προσφέρει **ανταγωνιστικό πλεονέκτημα** στις εταιρίες που την έχουν υιοθετήσει.

Η περίοδος της πανδημίας αύξησε τους κινδύνους που αντιμετωπίζει κάθε εταιρία. Ο ψηφιακός μετασχηματισμός που έλαβε χώρα κατά την διάρκεια της πανδημίας εξέθεσε τις εταιρίες σε νέους κινδύνους για τη διαχείριση των οποίων χρειάζεται και ασφάλιση **cyber insurance**. Χωρίς την υιοθέτηση νέων υπηρεσιών εξυπηρέτησης οι περισσότερες εταιρίες θα βρίσκονταν στο φάσμα της χρεωκοπίας.

Το νέο περιβάλλον απαιτεί ενεργή διαχείριση των κινδύνων



που απειλούν τις καθημερινές λειτουργίες της κάθε εταιρίας όπως οι **κυβερνοεπιθέσεις**, το **phishing**, τα περιστατικά **ransomware** κα, κίνδυνοι οι οποίοι μπορούν να οδηγήσουν σε διακοπή εργασιών, πρόστιμα και ευθύνες για μη πρόληψη και σωστή διαχείριση περιστατικών παραβίασης ασφάλειας. Λαμβάνοντας υπόψη ότι ο κίνδυνος **δεν είναι 100% διαχειρίσιμος** όποιες ενέργειες και να κάνει μία εταιρία, η ασφάλιση Cyber Insurance αποτελεί ένα **αποτελεσματικό εργαλείο διαχείριση**ς του υπολειπόμενου κινδύνου (residual risk) και οι υπηρεσίες διαχείρισης περιστατικών παραβίασης ασφάλειας που παρέχει μπορούν να καταστήσουν λειτουργικό το Πλάνο Αντιμετώπισης Περιστατικών που διαθέτει η κάθε εταιρία. Επίσης είναι ένα εργαλείο αντιμετώπισης των οικονομικών συνεπειών περιστατικών παραβίασης ασφάλειας και βοηθά στην ομαλή συνέχιση των δραστηριοτήτων της επιχείρησης.

Η ασφάλιση cyber insurance είναι ένα ασφαλιστικό προϊόν του οποίου η κάλυψη είναι παγκόσμια. Το Internet δεν έχει τόπο και ο κίνδυνος δεν κάνει διάκριση. Η **Ελλάδα ανέβηκε στην 5η** θέση παγκοσμίως στην κατάταξη των χωρών που δέχονται κυβερνοεπιθέσεις.

Αυτό που βλέπουμε είναι ότι η ύπαρξη ασφάλισης έχει καταστεί υποχρεωτική για την συμμετοχή σε έργα ασφάλειας πληροφοριακών συστημάτων, σε περιπτώσεις συγχωνεύσεων και εξαγορών και σε εταιρικές συνεργασίες.

Οι εταιρίες που δεν έχουν φροντίσει να έχουν τις κατάλληλες υποδομές και δεν έχουν δώσει **έμφαση την εκπαίδευση του ανθρώπινου δυναμικού** τους δεν έχουν πλέον δυνατότητα να ασφαλιστούν ή να διατηρήσουν το ασφαλιστικό πρόγραμμα και τις παροχές που έχουν. Για να έχετε μια πλήρη εικόνα των τεχνικών και οργανωτικών μέτρων που ζητάνε οι ασφαλιστές από τις εταιρίες που ασφαλίζουν μπορείτε να κατεβάσετε τις προτάσεις ασφάλισης που βρίσκονται στην ενότητα **Προσφορά Ασφάλισης** στην ιστοσελίδα https://www.cyberinsurancequote.gr/get-a-quote/. ITSecurity