ΟΙ ΜΙΚΡΕΣ ΚΑΙ ΜΕΣΑΙΕΣ ΕΤΑΙΡΙΕΣ ΔΕΝ ΑΠΕΙΛΟΥΝΤΑΙ ΑΠΟ ΤΙΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ;

Υπάρχει μια λάθος αντίληψη ότι οι επιθέσεις στον κυβερνοχώρο είναι πρόβλημα των μεγάλων επιχειρήσεων γιατί οι κυβερνοεπιθέσεις στις μεγάλες επιχειρήσεις τραβούν την προσοχή των μέσων μαζικής ενημέρωσης, γίνονται γνωστές στους πελάτες τους και οι κυβερνοεγκληματίες ασχολούνται με αυτές γιατί μπορούν να κερδίσουν πολλά χρήματα από κυβερνοεκβιασμό σε σχέση με τις μικρές εταιρίες. Καθημερινά όμως χιλιάδες μικρές και μεσαίες επιχειρήσεις διεθνώς, υφίστανται περιστατικά παραβίασης ως αποτέλεσμα κυβερνοεπιθέσεων.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΚΙΝΔΥΝΟΙ ΠΟΥ ΣΥΝΗΘΩΣ ΑΝΤΙΜΕΤΩΠΙΖΟΥΝ ΟΙ ΜΙΚΡΕΣ ΚΑΙ ΜΕΣΑΙΕΣ ΕΤΑΙΡΙΕΣ;

Το **ransomware,** λογισμικό που κλειδώνει τα εταιρικά συστήματα και απαιτείται η πληρωμή λύτρων για την απόκτηση πρόσβασης στα εταιρικά συστήματα και η κλοπή εταιρικών κεφαλαίων, αποτελούν καθημερινούς κινδύνους που πρέπει να αντιμετωπίσουν οι μικρές και μεσαίες εταιρίες. Ο **εκβιασμός και οι παραβιάσεις δεδομένων** που συνήθως ξεκινούν με ένα ανθρώπινο λάθος ή μια παράβλεψη, όπως η απώλεια ενός φορητού υπολογιστή ή ένα κλικ σε έναν σύνδεσμο ενός Phishing email, επιτρέπουν στους εγκληματίες του κυβερνοχώρου να έχουν πρόσβαση στα εταιρικά συστήματα.Σύμφωνα με μελέτες το **μέσο κόστος των περιστατικών ransomware** σε μικρομεσαίες επιχειρήσεις ανέρχεται σε **€75.000** και ο μέσος χρόνος για την επαναφορά της εταιρίας στην προηγούμενη κατάσταση που ήταν πριν πέσει θύμα περιστατικού ransomware ανέρχεται σε **50 ημέρες**. Ένα μεγάλο ποσοστό εταιριών μετά από ένα περιστατικό ransomware οδηγούνται σε **χρεωκοπία** και αν πληρώσουν τα λύτρα στους κυβερνοεκλη-ματίες πέφτουν ξανά θύματα των κυβερνοεγκληματιών.


ΝΙΚΟΣ ΓΕΩΡΓΟΠΟΥΛΟΣ
Digital Risks Insurance Broker – **Cromar** Insurance Brokers SA, Co- Founder
The DPO Academy LinkedIn Profile: https://www.linkedin.com/in/nikos-georgopoulos/

ΓΙΑΤΙ ΟΜΩΣ ΟΙ ΜΙΚΡΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΑΠΟΤΕΛΟΥΝ ΣΤΟΧΟ ΤΩΝ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΙΩΝ;

1. Οι μικρές και μεσαίες επιχειρήσεις είναι πιο ευάλωτες λόγω έλλειψης εκπαίδευσης του ανθρώπινου δυναμικού τους και επενδύσεων στην κυβερνοασφάλεια: Οι κυβερνοεγκληματίες αναζητούν τον πιο εύκολο και γρήγορο τρόπο για να βγάλουν κέρδος. Οι μικρές και μεσαίες επιχειρήσεις έχουν συνήθως λιγότερους πόρους και χρόνο για να εκπαιδεύσουν το προσωπικό σχετικά με τους κινδύνους της κυβερνοασφάλειας, γεγονός που τις καθιστά πιο επιρρεπείς σε **επιθέσεις ransomware** και είναι πιο πιθανό να πληρώσουν λύτρα όταν αισθάνονται ότι δεν έχουν τη γνώση, τις υποδομές και τους ανθρώπους που μπορούν να τους βοηθήσουν στην αντιμετώπιση ενός περιστατικού.

2. Οι μικρές και μεσαίες επιχειρήσεις μπορούν να δώσουν δυνατότητα πρόσβασης στους κυβερνοεγκληματίες σε συστήματα μεγαλύτερων εταιριών με τις οποίες συνεργάζονται: Πολλές μικρές και μεσαίες εταιρείες συνδέονται με τα συστήματα πληροφορικής μεγαλύτερων οργανισμών στους οποίους παρέχουν υπηρεσίες. Έτσι, όταν οι κυβερνοεγκληματίες προσπαθούν να διεισδύσουν σε μεγαλύτερους και πιο ασφαλείς οργανισμούς, συχνά στοχεύουν τους προμηθευτές τους.

3. Οι μικρές επιχειρήσεις μπορεί να πέσουν θύματα κυβερνοεπιθέσεων που προέρχονται από οργανισμούς που τους παρέχουν υπηρεσίες τεχνολογίας: Σε περίπτωση μιας επιτυχημένης κυβερνοεπίθεσης σε ένα πάροχο υπηρεσιών τεχνολογίας με τον οποίο συνεργάζονται μπορεί να δημιουργήσει διακοπή εργασιών της επιχείρησης, παραβιάσεις δεδομένων ή ακόμη και βλάβη της φήμης τους.

ΤΙ ΖΗΤΑΝΕ ΟΙ ΑΣΦΑΛΙΣΤΕΣ ΑΠΟ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΓΙΑ ΝΑ ΤΙΣ ΑΣΦΑΛΙΣΟΥΝ;

Οι ασφαλιστικές εταιρίες ζητούν από τους πιθανούς πελάτες να υιοθετήσουν τεχνικά μέτρα ασφαλείας για την πρόληψη, τον εντοπισμό και την ανταπόκριση στα σημερινά εξελιγμένα περιστατικά παραβίασης ασφάλειας. Πιο συγκεκριμένα τα ζητούμενα μέτρα είναι τα ακόλουθα:

1. 'Ελεγχος πρόσβασης του 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 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). 'Οταν 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 αντιγράφων 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. **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.

5'Υπαρξη Πλάνου Αντιμετώπισης Περιστατικών Παραβίασης Ασφάλειας. Η ύπαρξη ενός Πλάνου Αντιμετώπισης Περιστατικών βοηθά την εταιρία στην αντιμετώπιση περιστατικών και ο συνδυασμός του με την ασφάλιση Cyber Insurance το κάνει πιο αποτελεσματικό γιατί μέσω τις ασφάλισης η εταιρία αποκτά πρόσβαση σε εξειδικευμένους παρόχους με εμπειρία στην διαχείριση περιστατικών παραβίασης ασφάλειας.

Το μεγαλύτερο πρόβλημα στις μικρές και μεσαίες επιχειρήσεις είναι η **έλλειψη κατανόησης των κινδύνων** για το λόγο αυτό είναι απαραίτητη η συνεργασία τους με εταιρίες παροχής υπηρεσιών κυβερνοασφάλειας για την υλοποίηση των έργων που θα τους εξασφαλίσουν την δυνατότητα να ασφαλιστούν, Η **ασφάλιση θα τους προσφέρει οικονομική προστασία** και θα τις βοηθήσει στην ομαλή συνέχιση των εργασιών τους.