Issue

Αναγκαία η **συνεργασία** Εταιριών, Παρόχων Υπηρεσιών Ασφάλειας Πληροφοριακών Συστημάτων & Ασφαλιστικών Εταιριών για την **αντιμετώπιση του Ransomware**

Η αγορά της ασφάλισης cyber insurance σημείωσε ταχεία ανάπτυξη και γρήγορη εξέλιξη τα προηγούμενα έτη για να ανταποκριθεί στις ανάγκες των εταιριών για ασφαλιστική καλύψη των κυβερνοκινδύνων. Οι ασφαλισμένες επιχειρήσεις για μεγάλο χρονικό διάστημα είχαν στην διάθεσή τους ασφαλιστικά προϊόντα με μεγάλο εύρος καλύψεων (Cyber Liability, Business Interruption, Cyber Crime) , ετήσια ασφάλιστρα χωρίς μεγάλες μεταβολές και παροχή υπηρεσιών πρόληψης περιστατικών παραβίασης ασφάλειας για να διαχειριστούν αποτελεσματικά τα τυχόν συμβάντα.

Ωστόσο στο τέλος του 2019 η αγορά πιέστηκε λόγω της αυξανόμενης συχνότητας, και σοβαρότητας των **περιστατικών** ransomware καθώς και της αύξησης των ποσών που ζητήθηκαν σαν **λύτρα από τους κυβερνοεγκληματίες**. Εκτός από την αύξηση των περιστατικών αυτών είχαμε την εφαρμογή του Κανονισμού Προστασίας Προσωπικών Δεδομένων στην Ευρωπαϊκή Ένωση, την εφαρμογή νέας νομοθεσίας για την χρήση των προσωπικών δεδομένων σε πολλές χώρες και την διερεύνηση της συμμετοχής από αρχές ξεπλύματος μαύρου χρήματος για την ανάπτυξη του κυβερνοεγκλήματος λόγω των ποσών που πληρώνουν οι εταιρείες σαν λύτρα για την αποκρυπτογράφηση των αρχείων τους στους κυβερνοεγκληματίες.

Το 2020 ξεκίνησε **με μεγαλύτερο έλεγχο από τους ασφαλιστές των τεχνικών και οργανωτικών μέτρων που λαμβάνει μια επιχείρηση για την διαχείριση των περιστατικών ransomware** κατά την διαδικασία ανάληψης κινδύνου, με **μείωση ορίων ασφαλιστικής κάλυψης** και **αυξήσεις** των ετησίων ασφαλίστρων οι οποίες **άνω του 20%**. Πιο συγκεκριμένα οι ασφαλιστές για να προχωρήσουν στην ασφάλιση ειδικά για το ransomware εξετάζουν την ύπαρξη **α)** διαδικασιών & πολιτικής διαχείρισης του εταιρικού email (π.χ. emails pre-screening, email quarantine services, email attachments evaluation, SPF, Phishing training, MFA,

Office 365 Advanced Threat Protection, users access email through web app or on corporate device, DKIM, DMARK, PTR, Disclaimer for Incoming Emails) **β)** διαδικασίων διαχείρισης και πολιτικών ασφάλειας (π.χ. Endpoint Protection, EDR, MFA, Vulnerability Scans, patch management, end of support software, network firewalls, protective DNS service, local admin rights, password manager software, privileged accounts management, Security Operation Center use) **γ)** διαδικασίες backup (π.χ. encryption, offline or cloud backup, Cloud syncing services, restoration & recovery of key server configurations and data backups in the last 6 months, integrity of backups testing) και **δ)** επιπλέον μέτρα που έχουν λάβει για την διαχείριση αυτών των περιστατικών.

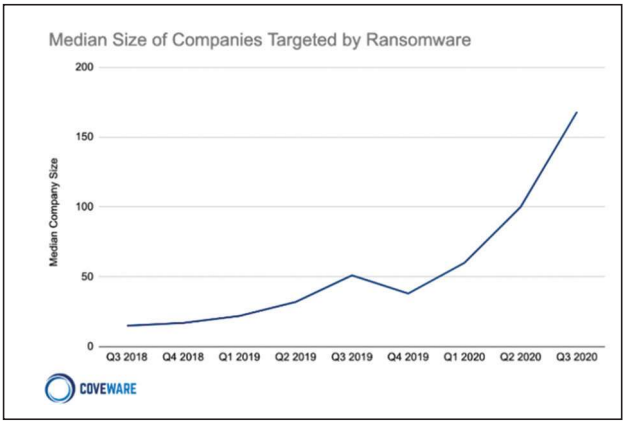
Οι περισσότεροι ασφαλιστές που παρέχουν **λύσεις cyber insurance** αποδίδουν την σκλήρυνση της αγοράς στην αύξηση των ζημιών κυρίως στην μεγάλη αύξηση των επιθέσεων ransomware. Οι επιθέσεις αυτές έχουν γίνει πιο στοχευμένες τα ποσά των λύτρων που ζητούνται έχουν σημαντικά αυξηθεί (απαιτούνται συνήθως εξαψήφια ποσά και μερικές έφτασαν εκατομμύρια δολάρια όπως στην περίπτωση της Garmin που έφθασε τα 10εκ Δολλάρια Αμερικής) και οι μέθοδοι υλοποίησής τους έχουν αλλάξει ώστε εκτός από την κρυπτογράφηση των δεδομένων να απειλούν και με δημοσιοποίησή τους σε περίπτωση μη καταβολής των λύτρων. Σύμφωνα με την Coveware, κατά το 3ο τρίμηνο του 2020, οι μισές περιπτώσεις έρευνας περιστατικών Ransomware σχετίζονται με απειλές δημοσιοποίησης δεδομένων και διπλασιάστηκαν σε σχέση με το 1ο τρίμηνο.

Οι κυβερνοεγκληματίες πριν κλειδώσουν τα δεδομένα τα αντιγράφουν. Υπάρχουν περιπτώσεις που δημιούργησαν ακόμη και ειδικούς ιστότοπους που ονομάζονται "ιστότοποι διαρροής" ("leak sites"), απειλώντας ότι θα δημοσιεύουν δεδομένα από εταιρείες που δεν αρνήθηκαν να πληρώσουν λύτρα. Έτσι, η πίεση για την πληρωμή λύτρων γίνεται ακόμη μεγαλύτερη. **Όμως, ακόμη και εάν πληρωθούν τα λύτρα δεν είναι βέβαιο ότι θα απελευθερωθούν τα αρχεία ή δεν θα δημοσιοποιηθούν** για το λόγο αυτό οι εταιρίες πρέπει να έχουν φροντίσει να έχουν τις **καταλληλες διαδικασίες, υποδομές και συνεργασίες για την αποτελεσματική διαχείριση των συμβάντων..** Η δημοσιοποίηση των δεδομένων δημιουργεί νομική ευθύνη για την εταιρεία θύμα και υποχρεωτική κοινοποίηση του συμβάντος σε πελάτες & ρυθμιστικές αρχές. Σύμφωνα με πρόσφατη μελέτη της Coveware ο μέσος χρόνος διακοπής λόγω μιας επίθεσης ransomware είναι 19 ημέρες. Αυτή η παρατεταμένη διακοπή οδηγεί συχνά στο χαμένο επιχειρηματικό κόστος που είναι πολύ μεγαλύτερο από το κόστος των λύτρων του εκβιασμού.

Το κόστος του χρόνου διακοπής εργασιών που οφείλεται σε επιθέσεις Ransomware αυξήθηκε κατά 200% από έτος σε έτος το πρώτο εξάμηνο του 2019 και συν 19% από το 1ο στο 2ο τρίμηνο του 2020

Το Ransomware θα αναζητήσει νέα θύματα, και θα γίνει πιο αυτοματοποιημένο , οι επιτιθέμενοι θα επικεντρωθούν σε στόχους που παρέχουν μεγαλύτερη απόδοση στις προσπάθειές τους. Η είσοδος σε ένα δίκτυο το οποίο έχει στοιχεία και δεδομένα από διάφορες επιχειρήσεις είναι σίγουρα πιο κερδοφόρο από την επίθεση σε μεμονωμένες εταιρείες.**Έτσι, ενώ οι μικρές επιχειρήσεις θα εξακολουθούν να είναι στο στόχαστρο, υποδομές cloud και πάροχοι διαχειριζόμενων υπηρεσιών θα γίνουν πιο πολύτιμοι στόχοι, επειδή τα συστήματά τους παρέχουν πρόσβαση στα δεδομένα πολλών πελατών.**

Οπως στο παρακάτω **γραφημα** πιο συχνά περιστατικά ransomware είχαμε σε εταιρίες με 168 εργαζόμενους.



Πηγή: Coveware .

Ενας ακόμη παράγοντας που πρέπει να ληφθεί υπόψη είναι η τηλεργασία στην οποία οδηγήθηκαν οι επιχειρήσεις λόγω την πανδημίας COVID-19, σύμφωνα με την έκθεση της Acronis οι επιθέσεις κατά των εργαζομένων σε τηλεργασία θα αυξηθούν. Ενώ το 31% των εταιρειών παγκοσμίως ανέφεραν καθημερινές κυβερνοεπιθέσεις το 2020, η συχνότητα των επιθέσεων με στόχο τους απομακρυσμένους εργαζόμενους προβλέπεται να αυξηθεί το 2021, καθώς τα υπολογιστικά συστήματα εκτός του εταιρικού δικτύου είναι πιο ευάλωτα, δίνοντας στους επιτιθέμενους πρόσβαση στα δεδομένα του οργανισμού.

Για την αντιμετώπιση των νέων δεδομένων πρέπει οι εταιρίες να συνεργαστούν με παρόχους υπηρεσιών ασφάλειας πληροφοριακών συστημάτων και με τους ασφαλιστές με στόχο την πρόληψη και την καλύτερη διαχείριση περιστατικών παραβίασης ασφάλειας για να επιτύχουν την ομαλή συνέχιση της λειτουργίας τους. ITSecurity