

Issue

Πως αντιμετωπίζεται από ένα ασφαλιστήριο **cyber insurance** το **ransomware**;

Τα περιστατικά Ransomware αυξάνονται διαρκώς και πέρα από τους τρόπους προστασίας των δεδομένων θα πρέπει να λαμβάνονται σοβαρά υπόψη και οι δυνατότητες και τα οφέλη αντιμετώπισης του φαινομένου με ένα ασφαλιστήριο cyber insurance.



Tο Ransomware, ως γνωστόν είναι κακόβουλο λογισμικό που “κλειδώνει” τις λειτουργίες υπολογιστών και συστημάτων, ενώ παράλληλα μπορεί να κρυπτογραφήσει δεδομένα και αρχεία, ζητώντας “λύτρα”, σε κάποιο κρυπτονόμισμα (πχ Bitcoins), για να ανακτηθεί ο έλεγχος του υπολογιστή ή των συστημάτων και να χρησιμοποιηθούν ξανά τα μολυσμένα αρχεία. Όπως έχει αποδειχθεί, είναι μια απάτη η οποία εξελίχθηκε από εγκληματικές οργανώσεις που δραστηριοποιούνται στο χώρο του κυβερνοεγκλήματος και επιδιώκουν παράνομο κέρδος.

Μία επιτυχημένη επίθεση σε μια εταιρία, μπορεί ενδεχομένως να μολύνει πολλούς υπολογιστές, **προκαλώντας ζημιά στα έσοδα της και στη φύμη της**. Σε περίπτωση που οι συμμορίες του κυβερνοεγκλήματος δουν μια επιχειρόση να υποκύπτει σε μια κυβερνοεπίθεση και να πληρώνει τα λύτρα, ακολουθούν και άλλες κυβερνοεπιθέσεις σε αυτήν με στόχο να πάρουν και αυτοί το μερίδιό τους.

Τα **περιστατικά αποζημιώσεων** λόγω Ransomware που διαχειρίστηκε η Ομάδα Διαχείρισης των Beazley **υπερτετρα-**

πλασιάστηκαν το 2016 με το 50% περίπου αυτών να αφορά εταιρίες που δραστηριοποιούνται στο χώρο της υγείας. Η εκτίμηση της εταιρίας είναι ότι και **το 2017 θα διπλασιαστούν τα περιστατικά αυτά**. Οι οργανισμοί είναι ευάλωτοι σε τέτοιου είδους επιθέσεις οι οποίες έχουν σαν αποτέλεσμα την μη διαθεσιμότητα των συστημάτων και των αρχείων τους, ιδιαίτερα σε περίδους εορτών και κλεισιμάτων τριμήνων και συνδιάζονται με την απάτηση καταβολής λύτρων για να γίνει εφικτή η επαναφορά των αρχείων στην πρότερη κατάσταση.

Περιστατικά ransomware παρατηρούνται τον τελευταίο καιρό σε ιδιώτες, ελεύθερους επαγγελματίες (λογιστές, δικηγόρους, μηχανικούς, γιατρούς) και επιχειρήσεις (φαρμακευτικές, εταιρίες στοιχημάτων, νοσοκομεία).

Για να κατανοήσουμε **πως αντιμετωπίζεται από ένα ασφαλιστήριο cyber insurance ένα περιστατικό ransomware** ας δούμε το παρακάτω σενάριο.

Ένας εργαζόμενος μιας επιχείρησης παροχής συμβουλευτικών υπηρεσιών έκανε κλικ σε ένα μολυσμένο Link που περιείχε ένα email που έλαβε και ένα malware κατέβηκε στον εταιρικό server. Το Malware κρυπτογράφησε όλα τα αρχεία που περιείχε ο server.

Ένα μήνυμα εμφανίστηκε στον υπολογιστή του εργαζομένου ζητώντας την πληρωμή **7 Bitcoin (€ 10.900)** στις επόμενες 24 ώρες για να παραλάβει το κλειδί αποκρυπτογράφησης των αρχείων. **Το συμβάν αυτό αποτελεί ένα Περιστατικό Παραβίασης Ασφάλειας Εταιρικού Δικτύου.** Η επιχείρηση επικοινώνησε με την ασφαλιστική της εταιρία για να την ενημερώσει για το συμβάν και να ζητήσει βοήθεια για την διαχείρισή του. Ο **Incident Response Manager** που ανέλαβε την διαχείριση του συμβάντος επικοινώνησε με τους Forensic Investigators της ασφαλιστικής εταιρίας για να διερευνήσουν τις συνθήκες του περιστατικού και να γνωμοδοτήσουν αν η εταιρία μπορεί να αποφύγει την πληρωμή λύτρων.



Νίκος Γεωργόπουλος

Cyber Privacy Risks Insurance Advisor Cromar Coverholder at Lloyd's
Email: Nikos.georgopoulos@cromar.gr, www.cyberinsurancequote.gr

Πιθανές Οικονομικές Επιπτώσεις – Καλύψεις Ασφαλιστηρίου που ενεργοποιούνται

Cyber Extortion – Κυβερνοεκβιασμός Κόστη τα οποία σχετίζονται με την αντιμετώπιση του κακόβουλου λογισμικού και την επαναφορά των αρχείων σε περίπτωση μη καταβολής του ποσού των λύτρων		
• Αμοιβή Συμβούλου Πληροφορικής ο οποίος θα διερευνήσει την δυνατότητα επαναφοράς των μολυσμένων από το κακόβουλο λογισμικό αρχείων από το back up που διατηρεί ο ασφαλισμένος		€15.000
Incident Response Expenses – Έξοδα ανταπόκρισης Περιστατικού Παραβίασης		
• Αμοιβές ειδικών διερεύνησης εγκλημάτων που σχετίζονται με την παραβίαση πληροφοριακών συστημάτων (Forensics Investigators) για τον εντοπισμό του κακόβουλου λογισμικού, την ανάλυση των επιπτώσεων του συμβάντος, τον περιορισμό τους και την εκτίμηση του κόστους του συμβάντος	€21.000	
• Αμοιβή Εξειδικευμένου Νομικού Συμβούλου		€8.500
• Αμοιβή Incident Response Manager		€7.200
Data Asset Loss Κόστη επαναφοράς / αντικατάστασης κατεστραμένων αρχείων από το κακόβουλο λογισμικό.		€18.000
Συνολικό Κόστος Διαχείρισης Συμβάντος		€69.750

Πρέπει να ενημερώνεται η Αρχή Προστασίας Προσωπικών Δεδομένων για αυτά τα συμβάντα;

Σε περίπτωση περιστατικών κυβερνοεκβιασμού πρέπει να ενημερώνονται οι αρμόδιες αρχές σύμφωνα με το νέο Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR), γιατί το περιστατικό αυτό αφορά παραβίαση ασφάλειας του εταιρικού δικτύου και δείχνει ανεπάρκεια των υφιστάμενων διαδικασιών της εταιρίας κατά το οποίο μπορεί να οδηγήσει και σε περιστατικά διαρροής προσωπικών δεδομένων.

Τι πρέπει να θυμόμαστε

Αν και το κόστος της πληρωμής λύτρων σε Bitcoin είναι μικρότερο από το κόστος που θα πληρώσει ο ασφαλιστική εταιρία σύμφωνα με τους όρους του ασφαλιστηρίου, οι αστυνομικές αρχές (FBI, Europol) συνιστούν να μην πλη-

ρώνονται τα λύτρα σε περιπτώσεις κυβερνοεκβιασμού. Η καταβολή των λύτρων αυξάνει την εγκληματικότητα και δείχνει την ανεπάρκεια διαδικασιών και πολιτικών της εταιρίας και την μη ύπαρξη back up. Επίσης δεν διασφαλίζει ότι μπορεί να γίνει η επαναφορά των αρχείων που έχουν κρυπτογραφηθεί ούτε ότι η εταιρία δεν θα ξαναγίνει στόχος σε σύντομο χρονικό διάστημα. Τα αντίγραφα των δεδομένων θα πρέπει να φυλάσσονται σε ασφάλες μέρος. Η ασφαλιστική εταιρία αν χρειασθεί θα πληρώσει το ποσό των λύτρων σε Bitcoin θα είναι όμως η τελευταία επιλογή της.

Cyber Secure Solution

Η αγορά των Lloyd's παρέχει τις κατάλληλες ασφαλιστικές λύσεις, για να αντιμετωπίσουν και να διαχειρισθούν οι εταιρίες τέτοιου είδους περιστατικά. Η Cromar coverholder at Lloyd's δημιούργησε την λύση αντιμετώπισης περιστατικών **Cyber Secure Solution** σε συνεργασία με το μεγαλύτερο συνδικάτο της αγοράς στον τομέα αυτό τους Beazley με ετήσια παραγωγή ασφαλίστρων στον συγκεκριμένο τομέα άνω των \$400εκ και μεγάλη εμπειρία στην διαχείριση περιστατικών (η ομάδα της έχει διαχειρισθεί πάνω από 5.000 περιστατικά). Μεγάλο ρόλο στην αντιμετώπιση τέτοιων περιστατικών παίζει η εκπαίδευση του ανθρώπινου δυναμικού μια εταιρίας, για το λόγο αυτό δημιουργήσαμε την καινοτόμα εκπαιδευτική μηχανή www.cyberinsurancequote.gr η οποία βραβεύθηκε από την αγορά των Lloyd's στον ετήσιο διαγωνισμό Lloyd's Market Innovation Awards. **IT Security**

