ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μελέτη της ελληνικής αγοράς κυβερνο-ασφάλισης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Του

ΕΝΤΣΟ ΒΕΛΙΟΥ

Επιβλέπων: Καθηγητής Σωκράτης Κάτσικας

Πειραιάς, Φεβρουάριος 2017

Ευχαριστίες

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Ασφάλειας Ψηφιακών Συστημάτων» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς. Προ της παρουσίασης των αποτελεσμάτων της παρούσας διπλωματικής εργασίας, αισθάνομαι την υποχρέωση να ευχαριστήσω ορισμένους από τους ανθρώπους που γνώρισα, συνεργάστηκα μαζί τους και έπαιξαν πολύ σημαντικό ρόλο στην πραγματοποίησή της. Πρώτο από όλους θέλω να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής εργασίας, Καθηγητή Σωκράτη Κάτσικα για την πολύτιμη καθοδήγηση του και την εμπιστοσύνη και εκτίμηση που μου έδειξε. Στη συνέχεια θα ήθελα να ευχαριστήσω τον Καθηγητή Χρήστο Ξενάκη, Κωνσταντίνο Λαμπρινουδάκη, που υπήρξαν καθηγητές μου και στο προπτυχιακό και τους υποψήφιους διδάκτορες Χριστόφορο Νταντογιάν, Λίλιαν Μήτρου και Παναγιώτη Ριζομυλιώτη οι οποίοι με τα πλούσια πνευματικά προσόντα και το ήθος τους συνέβαλαν ουσιαστικά στην ολοκλήρωση αυτής της εργασίας. Τις ευχαριστίες μου εκφράζω και στους καθηγητές που δέχτηκαν να είναι μέλη της τριμελούς επιτροπής αξιολόγησης της μεταπτυχιακής εργασίας. Ιδιαίτερες ευχαριστίες θέλω να απευθύνω στον Σωκράτη Κάτσικα για την καθοριστική του βοήθεια, ο οποίος στάθηκε σημαντικός αρωγός στην προσπάθειά μου και με υποστήριξε σε κάθε φάση της πορείας μου και ελπίζω να συνεχίσει να με στηρίζει απο εδώ και πέρα σε όλη μου τη ζωή και εργασιακή πρόοδο. Τέλος, θέλω να ευχαριστήσω τους γονείς μου, καθώς και τον αδερφό μου, που με υπομονή και κουράγιο πρόσφεραν την απαραίτητη ηθική συμπαράσταση για την ολοκλήρωση της μεταπτυχιακής μου εργασίας.

Περίληψη

Οι ηλεκτρονικοί και διαδικτυακοί κίνδυνοι αποτελούν καθημερινή πραγματικότητα στον κόσμο των πληροφοριών και πληροφοριακών συστημάτων. Κάθε εταιρία που ασχολείται με ηλεκτρονικά δεδομένα, ανεξάρτητα από το εάν αυτά βρίσκονται σε υπολογιστές, servers ή το διαδίκτυο, μπορεί να βρεθεί αντιμέτωπη με αντίστοιχες περιπτώσεις. Οι κίνδυνοι μπορεί να αφορούν απώλεια ή διαρροή δεδομένων από εσωτερικές ή εξωτερικές «επιθέσεις» ή αμέλεια στην χρήση. Μπορεί να προέρχονται από ένα μεμονωμένο υπολογιστή, ή μία επίθεση σε μονάδες αποθήκευσης, data warehouses, routers, private ή common servers και clouds. Μία επιχείρηση ενδέχεται επίσης να αντιμετωπίσει την αλλοίωση ή ακόμη και τη διακοπή της παρουσίας της στο διαδίκτυο, καθώς και προβλήματα εξυπηρέτησης, αν λόγω επίθεσης διακοπεί ο server της. Οι κίνδυνοι αυτοί συνεχώς εξελίσσονται και γίνονται πιο σύνθετοι. Ενώ στο παρελθόν οι οργανισμοί επένδυαν στην ασφάλεια των φυσικών περιουσιακών τους στοιχείων, σήμερα το ενδιαφέρον επιβάλλεται να εστιάζεται στην προστασία των δικτύων και των συστημάτων. Η νομοθεσία για την προστασία των ευαίσθητων εταιρικών ή προσωπικών δεδομένων γίνεται ολοένα και πιο αυστηρή, ενώ η προστασία της οικονομικής κατάστασης και της εταιρικής φήμης αποτελούν προτεραιότητες. Με στόχο την υποστήριξη των επιχειρήσεων στην διαχείριση αυτών των κινδύνων, οι ασφαλιστικές εταιρίες στην Ελλάδα και στο εξωτερικό προτείνουν καινοτόμα προϊόντα σχεδιασμένα να αντιμετωπίζουν τις περισσότερες από τις συνέπειες των διαρροών και παραβιάσεων δεδομένων. Οι ηλεκτρονικές και διαδικτυακές απειλές αποτελούν τις μεγαλύτερες πηγές ανησυχίας για τις επιχειρήσεις, ειδικά στην τρέχουσα ψηφιακή εποχή. Το γεγονός αυτό, σε συνδυασμό με το χαμηλό ποσοστό ασφάλισης έναντι της συγκεκριμένης κατηγορίας κινδύνων, αναδεικνύουν ένα πρόσφορο έδαφος για τους ασφαλιστικούς συμβούλους, με στόχο τις νέες πωλήσεις. Η έρευνα, η οποία πραγματοποιείται παρακάτω, χωρίζεται σε δύο μέρη.

Το αντικείμενο της διπλωματικής είναι η αποτύπωση της προσφοράς και της ζήτησης σε ασφαλιστικά προϊόντα έναντι κυβερνοεπίθεσης στην Ελλάδα. Αναφορικά με την πλευρά της προσφοράς θα εντοπιστούν ασφαλιστικές εταιρείες στην Ελλάδα που προσφέρουν ασφαλίσεις έναντι κυβερνο-επιθέσεων και πραγματοποιούνται συνεντεύξεις με στελέχη των εταιρειών αυτών προκειμένου να δούμε τη φύση των προϊόντων, τις ρυθμίσεις, τις καλύψεις κ.λπ. Για την πλευρά της ζήτησης θα πρέπει πάλι με συνεντεύξεις να εξετάσουμε εταιρείες που είτε έχουν ασφαλιστεί είτε θέλουν να ασφαλιστούν κατά τέτοιων κινδύνων.

Περιεχόμενα

1. Εισαγωγή

Οι κίνδυνοι που αφορούν στην ασφάλεια συστημάτων και δεδομένων, είναι πλέον τόσο απτοί και συνήθεις, όσο και οι φυσικές απειλές των λοιπών περιουσιακών στοιχείων μίας επιχείρησης. Ενδέχεται μάλιστα να αποτελέσουν την αρχή μίας σειράς ιδιαίτερα σοβαρών προβλημάτων.

1.1 Ηλεκτρονικοί και διαδικτυακοί κίνδυνοι

Διαρροή δεδομένων: Μία εταιρία καλείται να αντιμετωπίσει την απώλεια ή διαρροή ψηφιακών δεδομένων από το σύστημά της. Θα μπορούσε επίσης να υπόκειται την απώλεια δεδομένων από σταθερό ή φορητό υπολογιστή, smartphone ή tablet. Η διαρροή αυτή δύναται να οδηγήσει σε κλοπή προσωπικών στοιχείων, παραβίαση πληροφοριών πελατών ή σε μια πλήρους κλίμακας επίθεση μέσω του διαδικτύου με αρνητικό αντίκτυπο σε ευαίσθητα και σημαντικά δεδομένα, είτε από τρίτους, είτε από τους ίδιους τους υπαλλήλους της.

Προβλήματα στο τμήμα IT: Το τμήμα IT καλείται να αντιμετωπίσει τον οποιονδήποτε ηλεκτρονικό ή και διαδικτυακό κίνδυνο ενώ εξακολουθεί να διαχειρίζεται τα συνήθη ζητήματα της επιχείρησης. Καλείται να προσδιορίσει εάν το πρόβλημα αφορά διαρροή ή απώλεια δεδομένων ή κακόβουλη επίθεση από hackers, το πώς χάθηκαν ή διέρρευσαν τα δεδομένα ενώ απαιτείται να έχει την εμπειρία σε παραβιάσεις ασφαλείας και μεγάλες επιθέσεις από hackers έτσι ώστε να μπορεί να καταστείλει τη διαρροή, να διακόψει, αν χρειαστεί, τη λειτουργία του server ή να αντικαταστήσει το λογισμικό του και γενικά να διαθέτει σχέδιο έκτακτης ανάγκης και τον τρόπο εκτέλεσής του.

Κρίση Εταιρικής Φήμης: Οι ειδήσεις των διαρροών εξαπλώνονται γρήγορα, ιδιαίτερα στην εποχή των social media. Τα συγκεκριμένα περιστατικά μπορούν να θέσουν σε κίνδυνο τη φήμη μίας εταιρίας. Σε αυτές τις περιπτώσεις απαιτείται προσεκτική διαχείριση και αντιμετώπιση των Μέσων Μαζικής Ενημέρωσης, των πελατών, του προσωπικού και των ενδιαφερομένων μερών. Είναι σημαντικό να διασαφηνιστεί εάν πρέπει να ενημερωθούν οι πελάτες για τη διαρροή ή απώλεια των δεδομένων τους, ποιος άλλος πρέπει να ενημερωθεί και ποιος είναι ο καλύτερος τρόπος για να γίνει αυτό. Απαιτείται άμεση και προσεκτικά ελεγχόμενη δράση στον τομέα των Δημοσίων Σχέσεων προκειμένου να ανακτηθεί η εμπιστοσύνη και να προστατευτεί η φήμη της εταιρείας.

Οικονομικές προεκτάσεις: Οι οικονομικές επιπτώσεις αρχίζουν να συσσωρεύονται. Προκύπτει το ερώτημα αν θα κινηθούν δικαστικές διαδικασίες απο πρόσωπα που θεωρούν ότι διέρρευσαν τα δεδομένα τους. Τρίτοι οι οποίοι χρειάστηκε να αποζημιώσουν τους δικούς τους πελάτες για τη διαρροή δεδομένων από μία εταιρία, ενδέχεται να διεκδικήσουν αποζημίωση. Αυτά τα έξοδα έρχονται να προστεθούν στα έξοδα για την εξακρίβωση της προέλευσης της απώλειας ή παραβίασης, την αναδιαμόρφωση των δικτύων, την αποκατάσταση της ασφάλειας και την επαναφορά δεδομένων και συστημάτων. Και όσο η επιχείρηση βρίσκεται, ενδεχομένως, εκτός λειτουργίας, είναι δυνατό να υπάρξει περαιτέρω απώλεια κερδών.

Κρίση στη διοίκηση της εταιρίας: Μια κρίση που σχετίζεται με ηλεκτρονικά δεδομένα μπορεί να επηρεάσει σημαντικά την τιμή της μετοχής, καθώς και τη φήμη των στελεχών και της εταιρίας.

1.2 Ασφαλιστικές εταιρίες

Παρακάτω παραθέτονται οι ασφαλιστικές εταιρίες που λειτουργούν στην Ελλάδα και τις κατηγοριοποιούμε σε αυτές που είναι αμιγώς Ελληνικές και στις πολυεθνικές που έχουν έδρα στην Ελλάδα και λειτουργούν σύμφωνα με το Ελληνικό δίκαιο και τους νόμους.[1]

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΕΛΛΗΝΙΚΗ	ΠΟΛΥΕΘΝΙΚΗ
AIG		√
ALLIANZ		√
ARAG		√
ATRADIUS		√
AXA		√
CNP		√
CREDIT AGRICOLE		√
DAS		√
ERGO		√
EULER HERMES		√
EURO INSURANCES		√
EUROLIFE ERB	√	
EUROP ASSISTANCE		√

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΕΛΛΗΝΙΚΗ	ΠΟΛΥΕΘΝΙΚΗ
GENWORTH		√
GROUPAMA	√	
GENERALI		√
HDI GERLING		√
INTERAMERICAN	√	
INTERASCO	√	
INTERLIFE	√	
INTER PARTNER		√
INTERNATIONAL LIFE	√	
MARSH		√
METLIFE		√
MONDIAL ASSISTANCE		√
MALAYAN		√
MAPFRE		√
NP	√	
PRIME		√
PERSONAL	√	
RSA		√
SOGECAP		√
Α.Ε.Γ.Α	√	
AIGAION	√	
ΑΤΕ	√	
ΑΤΛΑΝΤΙΚΗ ΕΝΩΣΗ	√	
ΓΕΝΙΚΗ ΠΑΝΕΛΛΑΔΙΚΗ	√	
ΔΥΝΑΜΙΣ	√	
ΕΘΝΙΚΗ	√	
LLOYD'S		√
ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΙΣ(ΜΙΝΕΤΤΑ)	√	
ΕΥΡΩΠΑΙΚΗ ΠΙΣΤΗ	√	
ΕΥΡΩΠΗ	√	
ΙΝΤΕΡΣΑΛΟΝΙΚΑ	√	

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΕΛΛΗΝΙΚΗ	ΠΟΛΥΕΘΝΙΚΗ
ΝΝ		√
ΟΡΙΖΩΝ	√	
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ	√	
ΥΔΡΟΓΕΙΟΣ	√	

Πίνακας 1.1: Ασφαλιστικές εταιρίες που λειτουργούν στην Ελλάδα

Το κοινό χαρακτηριστικό των παραπάνω ασφαλιστικών εταιριών είναι ότι όλες εδρεύουν στην Ελλάδα. Φυσικά, εκείνες που λογίζονται, παραπάνω, ως Ελληνικές δεν σημαίνει ότι δεν λειτουργούν και σε πολυεθνικό επίπεδο, απλά ο τόπος ίδρυσης τους είναι η Ελλάδα.

1.3 Ειδίκευση στόν κυβερνοχώρο

Ύστερα από μελέτη της ελληνικής αγοράς κυβερνο-ασφάλισης και των συμβολαίων παροχών υπηρεσιών των περισσοτέρων ασφαλιστικών εταιριών που αναφέρονται παραπάνω, κατέληξα, για την ανάλυσή μου, στις δυο καλύτερες, με βάση το κριτήριο ότι τα συμβόλαιά τους καλύπτουν όλες τις κατηγορίες καλύψεων που υπάρχουν στήν ελληνική αγορά σε σχέση με τις υπόλοιπες ασφαλιστικές εταιρίες. Οι εταιρίες αυτές είναι η **AIG** και η **LLOYDS**, των οποίων τα συμβόλαια είναι αρκετά όμοια με μικροδιαφορές που θα αναφερθούν.

AIG

Ως παγκόσμιος ασφαλιστικός ηγέτης έναντι των ηλεκτρονικών και διαδικτυακών κινδύνων, η AIG έχει αποκτήσει πολύτιμη εμπειρία, η οποία αντανακλάται στο εύρος της κάλυψής τους και των υποστηρικτικών υπηρεσιών τους, καθώς και στην ικανότητα και την εμπειρία των ομάδων απαιτήσεων. Το πρόγραμμα, το οποίο παρέχει για κυβερνοεπιθέσεις στις εταιρίες η AIG, ονομάζεται Cyberedge. Είναι ότι καλύτερο κυκλοφορεί στήν ελληνική αγορά αυτή τη στιγμή.

LLOYDS

Η LLOYDS είναι ένας απο τους μεγαλύτερους ανταγωνιστές της AIG στα ελληνικά αλλά και παγκόσμια δεδομένα, οχι μόνο στόν χώρο της αγοράς

κυβερνο-ασφάλισης αλλά σε γενικότερο πλαίσιο. Τα δύο αυτά μεγαθήρια ανταγωνίζονται για μία θέση στην κορύφη των ασφαλιστικών εταιριών. Ξεκάθαρα αυτή η θέση ανήκει στην AIG στο χώρο της κυβερνο-ασφάλισης, με την LLOYDS να ακολουθεί με ένα πολύ καλό και πλήρες σχετικό συμβόλαιο.

1.4 Λειτουργία σε σχέση με το εξωτερικό

Ο παρακάτω πίνακας παρουσιάζει τις ασφαλιστικές εταιρείες που προσφέρουν διαφορετικές καλύψεις έναντι κυβερνοεπιθέσεων σε άλλες χώρες σε σύγκριση με την Ελλάδα.

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΔΙΑΦΟΡΕΤΙΚΕΣ ΚΑΛΥΨΕΙΣ	ΙΔΙΕΣ ΚΑΛΥΨΕΙΣ
AIG		√
ALLIANZ		√
ARAG	□	
ATRADIUS		√
AXA		√
CNP	□	
CREDIT AGRICOLE	□	
DAS	□	
ERGO	□	
EULER HERMES	□	
EURO INSURANCES	□	
EUROP ASSISTANCE	□	
GENWORTH		√
GENERALI	□	
HDI GERLING		√
INTER PARTNER	□	
MARSH		√
METLIFE	□	
MONDIAL ASSISTANCE	□	
MALAYAN		√
MAPFRE	□	

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΔΙΑΦΟΡΕΤΙΚΕΣ ΚΑΛΥΨΕΙΣ	ΙΔΙΕΣ ΚΑΛΥΨΕΙΣ
PRIME	□	
RSA		√
SOGECAP	□	
LLOYD'S		√
NN		√

Πίνακας 1.2: Διαφορετικές καλύψεις σε Ελλάδα και εξωτερικό

Μετά την οικονομική κρίση, οι περισσότερες από τις εταιρείες που προσέφεραν διαφορετικές καλύψεις στο εξωτερικό από την Ελλάδα, σταμάτησαν γενικώς να προσφέρουν συμβόλαια για καλύψεις έναντι κυβερνοεπιθέσεων στην Ελλάδα.

2. Σύγκριση και ορολογία

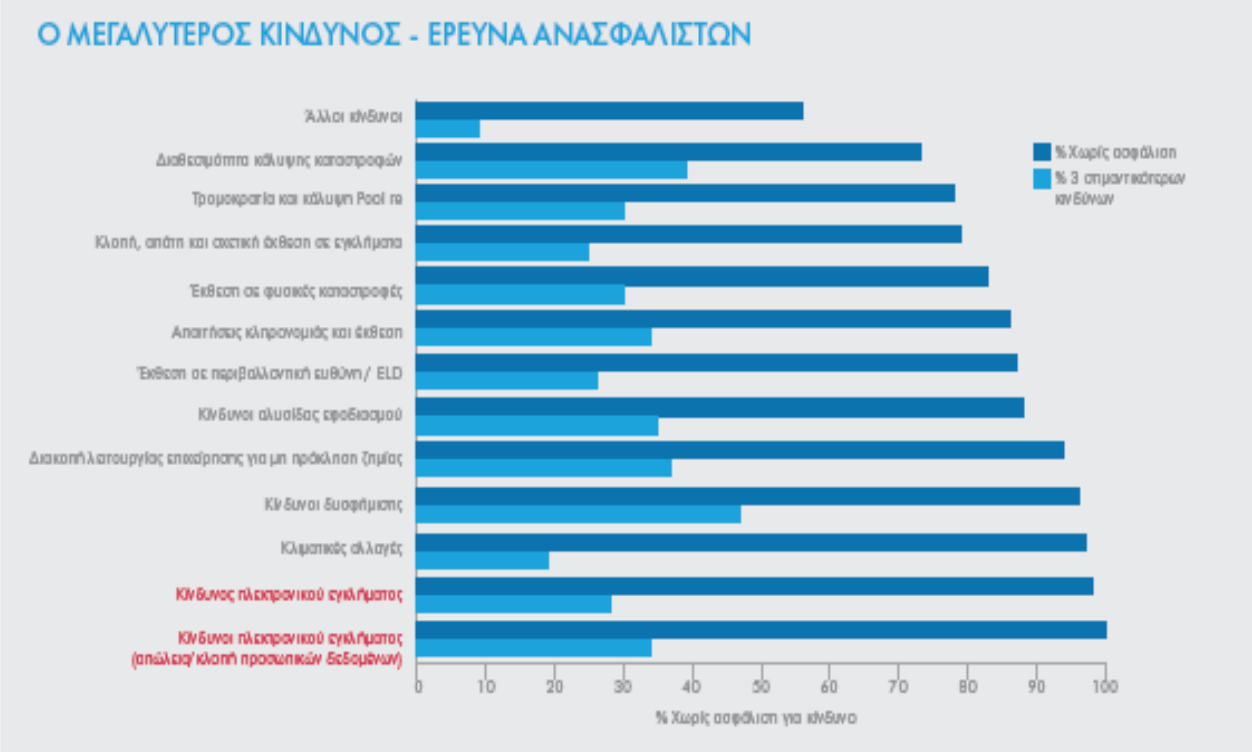
Στο παρόν κεφάλαιο θα αναλύσουμε περαιτέρω τον κυβερνοχώρο, θα δούμε στατιστικά πωλήσεων, αναφορές για διαφορετικές περιπτώσεις καλύψεων, θα γίνει μια σύγκριση μεταξύ των δύο βασικών μας εταιριών και θα γίνει μια γενική αναφορά στοιχείων, αναφορών και παροχών των δυο εταιριών, για να κατανοήσουμε καλύτερα την λειτουργία τους πριν αναφέρουμε τις καλύψεις που προσφέρουν έναντι των κυβερνοεπιθέσεων.

2.1 Ευκαιρία για πωλήσεις στον κυβερνοχώρο

Παρακάτω θα δούμε διάφορους τρόπους με τους οποίους μια εταιρία δύναται να πειστεί ότι η ασφάλεια πληροφοριών και γενικά η ασφάλιση στον κυβερνοχώρο είναι πλέον πιο σημαντική απο οποιαδήποτε ασφάλιση.

2.1.1 Ευαισθητοποίηση των πελατών – εταιριών

Πολλές ευρωπαϊκές εταιρείες ήδη κατανοούν την ανάγκη για ασφάλιση έναντι ηλεκτρονικών και διαδικτυακών κινδύνων, ενώ οι Risk Managers στο Ηνωμένο Βασίλειο κατατάσσουν τις συγκεκριμένες απειλές μεταξύ των πιο σημαντικών. Σε αυτό συμβάλλει η πληθώρα στατιστικών στοιχείων που αποδεικνύει τη συνεχή αύξηση των παραβιάσεων συστημάτων και διαρροών δεδομένων. Υπεύθυνοι διαχείρισης κινδύνου κλήθηκαννα προσδιορίσουν τους 3 σημαντικότερους κινδύνους και να δηλώσουν εάν είναι καλυμμένοι για τη συγκεκριμένη κατηγορία απειλών. Παρακάτω βλέπουμε τον πίνακα σε σχέση με αυτό.[2]



Πίνακας 2.1: Μεγαλύτεροι ασφαλιστικοί κίνδυνοι[2]

Διαπιστώνεται ότι οι κίνδυνοι στον κυβερνοχώρο και στο ηλεκτρονικό έγκλημα λογίζονται ως αρκετά σημαντικοί και υπάρχει μεγάλη ανάγκη ασφάλισης έναντι τέτοιων κινδύνων.

2.1.2 Ένας μεγάλος ανασφάλιστος κίνδυνος

Αν και, σύμφωνα με τους υπεύθυνους διαχείρισης κινδύνου, ο κίνδυνος που προκύπτει από τη συνεχή τους έκθεση στο διαδίκτυο είναι μεγάλος, σύμφωνα με έρευνα οι εταιρείες δεν είναι ακόμη επαρκώς ασφαλισμένες ως προς τον τομέα αυτόν. Αυτή ακριβώς η έλλειψη ασφάλισης υποδεικνύει και μια μεγάλη ευκαιρία για τους ασφαλιστικούς συμβούλους, ακριβώς λόγω του ενδιαφέροντος που αναμένεται, στο εγγύς μέλλον, να δείξουν οι πελάτες τους. Υπάρχουν αρκετά εντυπωσιακά στοιχεία σχετικά με τους κινδύνους του κυβερνοχώρου που συνηγορούν σε αυτό. Ακολουθούν ορισμένα από αυτά:

- Το 2011 υπήρχαν 855 παραβιάσεις δεδομένων που κατέστρεψαν περισσότερα από 174 εκατομμύρια αρχεία
- Κάθε λεπτό, 232 υπολογιστές «μολύνονται» από κακόβουλο λογισμικό

- Το Κέντρο Καταπολέμησης Απάτης (RSA) διέκοψε περισσότερες από 550.000 επιθέσεις ηλεκτρονικού «ψαρέματος» (phishing)
- Οι νέες, εξελιγμένες επιθέσεις αναπτύσσονται συνεχώς, συμπεριλαμβανομένων δράσεων που προέρχονται από συνδικάτα εγκλήματος, από ανεξάρτητους χάκερ, εργαζόμενους, ακτιβιστές χάκερ (hacktivists), κ.λπ.
- Το μέσο κόστος της παραβίασης της ασφάλειας δικτύου είναι μεγαλύτερο από 5 εκατομμύρια δολ. ΗΠΑ
- Το μέσο κόστος ανά αρχείο που εμπλέκεται σε μια παραβίαση της ασφάλειας δικτύου είναι 197 δολ. ΗΠΑ
- Το ευρωπαϊκό κόστος για το ηλεκτρονικό έγκλημα εις βάρος των καταναλωτών είναι 16 δισεκατομμύρια δολ. ΗΠΑ [8][9].

2.1.3 Μια μεγάλη αγορά

Κάθε επιχείρηση που συγκεντρώνει, διαχειρίζεται ή μεταβιβάζει δεδομένα μέσω του εταιρικού της δικτύου, αντιμετωπίζει τον κίνδυνο της ηλεκτρονικής υποκλοπής τους. Αυτό έχει ως αποτέλεσμα όλοι οι οργανισμοί, ανεξαρτήτως τομέα δραστηριοποίησης, να είναι συνεχώς εκτεθειμένοι σε κίνδυνο, γεγονός που δημιουργεί έναν τεράστιο αριθμό με πιθανούς πελάτες για τους ασφαλιστικούς συμβούλους.

Σε γενικές γραμμές, οι πελάτες έχουν επίγνωση των ηλεκτρονικών και διαδικτυακών κινδύνων, αλλά δεν γνωρίζουν επαρκώς το βαθμό στον οποίο είναι εκτεθειμένοι. Το στοιχείο αυτό, σε συνδυασμό με τον μικρό αριθμό των ασφαλισμένων εταιριών και το μεγάλο μέγεθος της αγοράς – στόχου, προσφέρει την ευκαιρία στους ασφαλιστικούς συμβούλους να προτείνουν στους πελάτες την αντιμετώπιση αυτού του κινδύνου μέσω της σχετικής ασφάλισης κατά του ηλεκτρονικού εγκλήματος.

2.2 Αναγνώριση πελατών – στόχων

Η δυνητική αγορά για το CyberEdge (AIG) και το DUAL (LLOYDS) είναι μεγάλη, διότι κάθε εταιρεία που αποθηκεύει, διαχειρίζεται ή μεταφέρει δεδομένα κινδυνεύει από διαδικτυακή ή φυσική κλοπή. Παρακάτω βλέπουμε μερικές απο τις κατηγορίες πιθάνων πελατών:

ΠΑΝΕΠΙΣΤΗΜΙΑ

Τα Πανεπιστήμια και τα κολέγια συγκεντρώνουν πολλά εμπιστευτικά δεδομένα (αριθμούς πιστωτικών καρτών των αιτούντων, ακαδημαϊκά αντίγραφα, ερευνητικά δεδομένα και μητρώα υγείας). Πολλά από αυτά αποθηκεύονται σε φορητές συσκευές που ανήκουν στο προσωπικό και τους σπουδαστές, οι οποίες μπορεί να χαθούν ή να παραμείνουν αφύλακτες. Η απομακρυσμένη πρόσβαση στα εταιρικά δίκτυα, τα μέσα κοινωνικής δικτύωσης και το λογισμικό διαχείρισης ακαδημαϊκών συναλλαγών επιβαρύνουν την έκθεση στον κίνδυνο, ενώ κάποια από τα εκπαιδευτικά αυτά ιδρύματα ενδέχεται να μην έχουν ιδιαίτερα υψηλά επίπεδα ασφάλειας.

ΕΠΙΧΕΙΡΗΣΕΙΣ ΛΙΑΝΙΚΗΣ ΠΩΛΗΣΗΣ

Οι επιχειρήσεις λιανικής πώλησης διαθέτουν πολλές πληροφορίες πελατών, συμπεριλαμβανομένων των στοιχείων πιστωτικών και χρεωστικών καρτών, ενώ οι online λιανικές πωλήσεις βρίσκονται σε άνοδο σε παγκόσμιο επίπεδο. Αυτό επιφέρει υποχρεώσεις συμμόρφωσης με τη νομοθεσία της εκάστοτε χώρας και με τα Πρότυπα Ασφαλείας Δεδομένων Καρτών Πληρωμής (PCI DSS) που εκθέτουν την επιχείρηση σε πιθανά πρόστιμα και κυρώσεις. Οι ιστοσελίδες λιανικής πώλησης είναι ευάλωτες σε «πάγωμα» από τους χάκερ, με αντίκτυπο στα έσοδα από τις online πωλήσεις. Παράλληλα, τα αυξανόμενα περιστατικά υποκλοπής πιστωτικών καρτών έχουν αντίκτυπο στις επιχειρήσεις που χρησιμοποιούν τερματικά για συναλλαγές με κάρτες (POS).

ΞΕΝΟΔΟΧΕΙΑΚΕΣ, ΤΑΞΙΔΙΩΤΙΚΕΣ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΑΝΑΨΥΧΗΣ

Οι εταιρείες που δραστηριοποιούνται σε αυτούς τους τομείς είναι εκτεθειμένες, μεταξύ άλλων, σε υψηλούς κινδύνους σχετικά με τα προσωπικά δεδομένα καθώς αποτελούν μέρος μιας παγκόσμιας βάσης δεδομένων με online συναλλαγές, Dos επιθέσεις και απάτες πιστωτικών καρτών. Ο τομέας αυτός έχει κτυπηθεί από πολλές ζημιές «υψηλού προφίλ» μετά από hacking σε συστήματα πληρωμών. Εταιρείες που δουλεύουν με δικαιοπάροχους (franchisees) πρέπει να εξασφαλίζουν οτι οι τελευταίοι τηρούν τα προβλεπόμενα πρότυπα ασφαλείας δεδομένων για την προστασία της επωνυμίας από οποιαδήποτε δυσφήμιση σχετίζεται με την παραβίαση της ασφάλειας των δεδομένων ή της ιδιωτικής ζωής.

ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ

Οι εταιρείες τηλεπικοινωνιών είναι υπεύθυνες για την ασφάλεια τεράστιων όγκων διαβιβαζόμενων προσωπικών πληροφοριών. Η σχετική Οδηγία που έχει εκδοθεί από την ΕΕ έχει ως αποτέλεσμα πολλές χώρες να απαιτούν να

γίνεται κοινοποίηση των παραβιάσεων στους πελάτες. Αυτό συνεπάγεται σημαντικές δαπάνες, αυξημένη πιθανότητα προστίμων, ποινών, δυσφημίσεων και απαιτήσεων τρίτων. Οι συναλλαγές με κάρτες πληρωμών απαιτούν τη συμμόρφωση με τα πρότυπα PCI DSS, ενώ παράλληλα οι επιχειρήσεις τηλεπικοινωνιών καλούνται να αντιμετωπίσουν εξελιγμένους ιούς που τις απειλούν με διακοπή λειτουργίας και απώλεια εσόδων.

ΚΥΒΕΡΝΟΤΡΟΜΟΚΡΑΤΙΑ

Πολλοί υποσταθμοί ενέργειας, φράγματα και αγωγοί έχουν μειώσει το κόστος μέσω τηλεχειρισμού και συστημάτων παρακολούθησης, ωστόσο, αυτό έχει αυξήσει την έκθεση στον κυβερνοχώρο - η οποία μερικές φορές επιδεινώνεται από τις κακές πρακτικές ασφάλειας. Ο κίνδυνος από την έκθεση ενισχύεται από τις επιθέσεις στα εθνικά δίκτυα υποδομών. Στη Μελέτη Ασφαλείας της KMPG, οι εταιρείες κοινής ωφέλειας αποτελούν τον πλέον τρωτό τομέα που επηρεάζεται από θέματα έκδοσης του λογισμικού των διακομιστών ιστού τους. Παράλληλα, οι εταιρείες κοινής ωφέλειας συλλέγουν μεγάλο όγκο προσωπικών δεδομένων για συναλλαγές με πιστωτικές κάρτες και υπόκεινται σε συμμόρφωση με τα PCI DSS.[2]

ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ

Τα χρηματοπιστωτικά ιδρύματα αποτελούν μία από τις πιο στοχευμένες βιομηχανίες από τους χάκερ και η πλειονότητα των παραβιασμένων αρχείων προέρχεται από τον συγκεκριμένο τομέα. Τα χρηματοπιστωτικά ιδρύματα κατέχουν σημαντικές προσωπικές πληροφορίες όπως οι εξής: πλήρη ονόματα, αριθμούς τηλεφώνου, διευθύνσεις, στοιχεία πιστωτικών καρτών, ιστορικά πιστώσεων. Οι τραπεζικές συναλλαγές μέσω διαδικτύου ή κινητού τηλεφώνου έχουν υποβάλει τον κλάδο σε νέες απειλές εισβολής. Ο ακτιβισμός των χάκερ έχει επίσης ως αποτέλεσμα την αύξηση των επιθέσεων άρνησης υπηρεσίας κατά των υπηρεσιών επεξεργασίας πληρωμών και άλλων χρηματοοικονομικών υπηρεσιών [2].

2.3 Κατανόηση του κυβερνοχώρου

Οι νέοι πελάτες που δεν έχουν αποφασίσει ακόμη να επενδύσουν σε ασφάλιση προστασίας έναντι των ηλεκτρονικών και διαδικτυακών κινδύνων, πρέπει να

κατανοήσουν αφενός την έκτασή τους και αφετέρου την προστασία που τους παρέχεται μέσω της ασφάλισης. Ακολουθούν ορισμένα προτεινόμενα σημεία προς συζήτηση.

ΚΑΤΑΝΟΟΥΝ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ;

Πολλές επιχειρήσεις ανησυχούν για την έκθεση στον κυβερνοχώρο, αλλά έχουν άραγε μια σαφή εικόνα για τους κινδύνους που εμπεριέχει ώστε να προστατευτούν;

Οι επιχειρήσεις αντιμετωπίζουν κινδύνους από τους χάκερ, τους ακτιβιστές χάκερ, το κακόβουλο λογισμικό, τους αμελείς και κακούς εργαζόμενους, τους ελλιπείς ελέγχους IT. Το CybeEdge και το DUAL παρέχουν σαφή και δομημένη προστασία: βοήθεια από ειδικούς όταν η κατάσταση παίρνει άσχημη τροπή, προστασία από τις οικονομικές συνέπειες, καθώς και προστασία φήμης.[4]

ΚΑΤΑΝΟΟΥΝ ΤΙΣ ΠΙΘΑΝΕΣ ΔΑΠΑΝΕΣ;

Μια παραβίαση στον κυβερνοχώρο ή διαρροή δεδομένων μπορεί να προκαλέσει πολλαπλές επιπτώσεις.

Οι οικονομικές συνέπειες μπορεί να είναι σοβαρές: κόστος κοινοποιήσεων, εμπειρογνώμονες για τον έλεγχο των ζημιών, κόστος παρακολούθησης χρήσης στοιχείων, κόστος έρευνας, αστική ευθύνη προς τρίτους, μακροπρόθεσμο κόστος δυσφήμισης και διακοπή λειτουργίας επιχείρησης.

Η ΑΜΕΣΗ ΕΠΕΜΒΑΣΗ ΕΙΝΑΙ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ

Κατανοεί η επιχείρηση πόσο σημαντική είναι μια έγκαιρη και αποτελεσματική ανταπόκριση για την προάσπιση της φήμης της;

Η ανταπόκριση της εταιρείας στις πρώτες 24-48 ώρες είναι κρίσιμης σημασίας. Θα πρέπει να συντονιστεί με εγκληματολόγους, νομικούς και ειδικούς στις Δημόσιες Σχέσεις για τον έλεγχο του αντίκτυπου στη φήμη απέναντι στους πελάτες, τους προμηθευτές, το προσωπικό, τους επενδυτές, τις ρυθμιστικές αρχές και το ευρύ κοινό.

Μικρές και μεσαίες επιχειρήσεις: ΕΥΠΑΘΕΙΣ ΣΤΗΝ ΠΡΟΣΒΟΛΗ

Αντιλαμβάνονται οι συγκεκριμένες επιχειρήσεις πόσο εκτεθειμένες είναι σε σχέση με τις μεγαλύτερες επιχειρήσεις;[4]

Οι μικρότερες επιχειρήσεις μπορεί να έχουν λιγότερο ισχυρή ασφάλεια και μη ελεγμένα πρωτόκολλα αντιμετώπισης (ίσως θεωρούνται δαπανηρά). Συχνά αποτελούν ευκαιριακούς στόχους και οι εγκληματίες ενδέχεται να τις χρησιμοποιήσουν ως το μέσο για να επιτεθούν σε μεγαλύτερους οργανισμούς.

Μικρές και μεσαίες επιχειρήσεις: ΕΥΑΛΩΤΕΣ ΣΕ ΖΗΜΙΕΣ

Έχουν αναλογιστεί οι συγκεκριμένες επιχειρήσεις τη ζημιά και τον αντίκτυπο που θα επιφέρει μια επίθεση;[4]

Οι μικρότερες επιχειρήσεις ενδεχομένως να μην έχουν πρόσβαση σε νομικούς και ειδικούς Δημοσίων Σχέσεων μετά από μια αποτυχία της ασφάλειας: η απώλεια εσόδων, η αδυναμία κάλυψης των λειτουργικών εξόδων και η δυσφήμιση μπορεί να είναι καταστροφικές για αυτές.

ΜΕΓΑΛΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ: ΜΕΓΑΛΥΤΕΡΟΙ ΣΤΟΧΟΙ

Οι μεγαλύτερες εταιρείες έχουν περισσότερα δεδομένα να χάσουν και θεωρούνται καλύτεροι στόχοι για λήψη αποζημίωσης.

Για τις μεγάλες εταιρείες με περισσότερα δεδομένα, οι παραβιάσεις μπορεί να οδηγήσουν σε κλοπές περισσότερων αρχείων και μεγαλύτερο κόστος για τη διαχείριση της απώλειας. Επίσης, είναι πιο ευπαθείς προς δράσεις τρίτων και μετόχων.

ΜΕΓΑΛΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ: ΠΙΟ ΔΥΣΚΟΛΟ ΝΑ ΕΝΤΟΠΙΣΤΟΥΝ

Μπορεί να είναι πιο δύσκολο για τις μεγάλες επιχειρήσεις να ελέγξουν χιλιάδες εργαζόμενους.

Η παρακολούθηση της δραστηριότητας των εργαζομένων (για κακόβουλες ή αμελείς πράξεις), ο εντοπισμός κλεμμένων και απολεσθέντων εξοπλισμών και η αντίστοιχη κλοπή των αποκλειστικών πληροφοριών είναι ακόμη πιο δύσκολη στους μεγάλους οργανισμούς και οι παραβιάσεις δεδομένων μπορεί να αργήσουν περισσότερο να επιλυθούν.

ΜΕΓΑΛΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ: ΔΙΑΣΥΝΟΡΙΑΚΑ ΖΗΤΗΜΑΤΑ

Οι επιχειρήσεις με διεθνείς δραστηριότητες μπορεί να αντιμετωπίσουν πρόσθετες επιπλοκές μετά από μια παραβίαση[2]

Η διασυνοριακή κοινή χρήση των δεδομένων, ακόμη και στο εσωτερικό των οργανισμών, μπορεί να οδηγήσει σε υψηλό κόστος διαχείρισης μετά από μια

παραβίαση. Οι διασυνοριακοί εγκληματολόγοι και νομικοί θα πρέπει να ευθυγραμμιστούν με την παροχή του βέλτιστου δυνατού αποτελέσματος για τον πελάτη.

2.4 Συγκριτικά πλεονεκτήματα της AIG

Ως παγκόσμιος ασφαλιστικός ηγέτης έναντι των ηλεκτρονικών και διαδικτυακών κινδύνων, έχουν αποκτήσει πολύτιμη εμπειρία, η οποία αντανακλάται στο εύρος της κάλυψής τους και των υποστηρικτικών υπηρεσιών τους, καθώς και στην ικανότητα και την εμπειρία των ομάδων απαιτήσεων. Προσφέρει το καλύτερο πακέτο που κυκλοφορεί αυτή τη στιγμή στην αγορά. Παρακάτω εξετάζεται τι είναι αυτό που την κάνει τόσο δυνατότερη από τις άλλες εταιρίες.[4]

ΕΙΣ ΒΑΘΟΣ ΚΑΤΑΝΟΗΣΗ

Με περισσότερα από 10 χρόνια εμπειρίας διεθνώς στην ασφάλιση των ηλεκτρονικών και διαδικτυακών κινδύνων, κατανοούν εις βάθος τις απειλές που αντιμετωπίζουν οι επιχειρήσεις κατά τη διαχείριση των πληροφοριών. Αυτή η εμπειρία βοηθά στο να παρέχουν την πιο ολοκληρωμένη κάλυψη που μπορεί να παρέχει ο ασφαλιστικός κλάδος.[4]

ΥΠΟΣΤΗΡΙΞΗ ΑΠΟ ΕΙΔΙΚΟΥΣ

Έχουν εργαστεί εκτενώς και με τον δέοντα ζήλο σε όλη την Ευρώπη και παγκόσμια για να διασφαλίσουν ότι οι ασφαλισμένοι με CyberEdge επωφελούνται από κορυφαίους εγκληματολόγους και νομικούς, οι οποίοι παρέχουν εγγυημένη ποιότητα υποστήριξης μετά από μια παραβίαση στον κυβερνοχώρο.[4]

ΚΑΙΝΟΤΟΜΙΑ ΠΡΟΪΟΝΤΩΝ

Διαθέτουν ομάδα εξειδικευμένων underwriters στον τομέα ανάληψης κινδύνου στη συγκεκριμένη ασφάλιση, η όποια αναλύει την έκθεση των πελατών τους στον κυβερνοχώρο. Αυτό σημαίνει ότι κατανοούν τις ανησυχίες των πελατών τους και χρησιμοποιούν αυτή τη γνώση για να εξελίσσουν και να αναπτύσσουν συνεχώς την κάλυψη των ασφαλιστήριων συμβολαίων τους - ένας ακόμη λόγος για τον οποίο είναι σε θέση να προσφέρουν το βέλτιστο προϊόν στην αγορά.[4]

ΕΜΠΕΙΡΙΑ ΣΤΙΣ ΑΠΑΙΤΗΣΕΙΣ

Έχουν αναπτύξει, παγκοσμίως, κορυφαίες ομάδες διαχείρισης απαιτήσεων ευθύνης για περιστατικά που σχετίζονται με ηλεκτρονικούς και διαδικτυακούς κινδύνους, ενώ η παγκόσμια διάρθρωσή τους επιτρέπει να μοιράζονται την εμπειρία σε θέματα ασφάλειας και ιδιωτικού απορρήτου σε παγκόσμιο επίπεδο. Αυτό σημαίνει ότι οι τοπικές ομάδες απαιτήσεων βρίσκονται στην πρώτη γραμμή της γνώσης και των βέλτιστων πρακτικών κατανοώντας τους κινδύνους, τις τάσεις και τη σημασία της άμεσης ανταπόκρισης στη διαχείριση θεμάτων σχετικά με τον κυβερνοχώρο.[4]

ΔΙΕΘΝΗΣ ΠΑΡΟΥΣΙΑ

Έχουν αναπτύξει τις ικανότητες PassportSM, έτσι ώστε να μπορούν να προσφέρουν το CyberEdge σε πολλές χώρες σε όλο τον κόσμο. Αυτό επιτρέπει στους πελάτες να έχουν πρόσβαση στην εκάστοτε τοπική τεχνογνωσία σε περίπτωση διασυνοριακού συμβάντος παραβίασης στον κυβερνοχώρο.[4]

2.5 Έλλειψη γνώσης των επιχειρήσεων για ζητήματα κυβερνο-ασφάλισης

Παρόλο που οι επιχειρήσεις δείχνουν μεγάλο ενδιαφέρον για τους ηλεκτρονικούς και διαδικτυακούς κινδύνους, δεν γνωρίζουν το πραγματικό μέγεθος της έκτασής τους αναφορικά με συγκεκριμένες απειλές, κάτι που μπορεί να προκαλέσει εμπόδια στις πωλήσεις. Παρακάτω παραθέτονται μερικοί από τους λόγους που οι εταιρίες δεν ασφαλίζονται για κυβερνοεπιθέσεις. Αυτό που θα κάνουμε είναι να διαχειριστούμε αυτές τις αντιρρήσεις και να πείσουμε με εφικτά επιχειρήματα ότι δεν είναι αρκετά τα υπάρχοντα αμυντικά συστήματα.[5]

ΔΙΑΘΕΤΟΥΜΕ ΗΔΗ ΑΣΦΑΛΙΣΗ ΜΕΣΩ ΑΛΛΩΝ ΠΡΟΓΡΑΜΜΑΤΩΝ

Τα κλασικά προγράμματα Αστικής Ευθύνης δεν καλύπτουν τους ηλεκτρονικούς και διαδικτυακούς κινδύνους. Άλλοι τύποι ασφάλισης, όπως η ασφάλιση εγγυήσεων, μπορεί να καλύψουν ορισμένα στοιχεία με πρόσθετη πράξη, αλλά δεν παρέχουν συνολική προστασία, ενώ συχνά περιορίζονται σε συμβολικές αμοιβές.

ΈΧΟΥΜΕ ΕΝΑ ΙΣΧΥΡΟ ΤΜΗΜΑ IT

Καμία εταιρεία δεν είναι ασφαλής από τον κίνδυνο παραβίασης των δεδομένων, ανεξάρτητα από τα πρότυπα ασφαλείας, καθώς είναι πολύ δύσκολη η παρακολούθηση και η αντιμετώπιση όλων των εσωτερικών και εξωτερικών απειλών. Το κακόβουλο λογισμικό δημιουργείται συχνά έτσι ώστε να εκμεταλλεύεται τις αδυναμίες του λειτουργικού συστήματος που είναι πέρα από τον έλεγχο των τμημάτων IT, αλλά και το ανθρώπινο σφάλμα, όπως η ευπάθειά του σε επιθέσεις «ψαρέματος» phishing και vishing.

ΔΕΝ ΑΠΟΤΕΛΟΥΜΕ «ΣΤΟΧΕΥΜΕΝΗ» ΒΙΟΜΗΧΑΝΙΑ

Οι εισβολείς, οι εργαζόμενοι ή οι ανταγωνιστές μπορούν επίσης να ενδιαφέρονται για τα ψηφιακά περιουσιακά στοιχεία μιας εταιρίας. Οι εισβολείς χρησιμοποιούν συχνά άλλους «μη στοχευμένους» οργανισμούς ως «παράθυρο» για την είσοδο σε μεγαλύτερους και πιο επιθυμητούς στόχους. Αν μια εγκληματολογική έρευνα ενέπλεκε αυτή την εταιρεία – «παράθυρο» ως την αιτία για μια διείσδυση, θα μπορούσε να αναλάβει την ευθύνη που συνδέεται με τη μετάδοση κακόβουλου λογισμικού;

Η ΑΣΦΑΛΙΣΗ ΚΟΣΤΙΖΕΙ ΑΡΚΕΤΑ

Τα ασφάλιστρα είναι πολύ χαμηλά σε σύγκριση με την πιθανότητα εμφάνισης μίας διαρροής ή επίθεσης συμπεριλαμβανομένης της πιθανότητας απώλειας εσόδων από δυσφήμιση. Δεν είναι ασυνήθιστο άλλωστε οι ζημίες να ανέρχονται σε μερικά εκατομμύρια ευρώ. Η ασφάλιση κατά των ηλεκτρονικών εγκλημάτων αποτελεί μια προσιτή επένδυση για την προστασία ενός οργανισμού από παραβιάσεις δεδομένων.

ΔΙΑΘΕΤΟΥΜΕ ΙΣΧΥΡΕΣ ΥΠΟΔΟΜΕΣ

Οι απολεσθέντες αλλά και οι κλεμμένοι φορητοί υπολογιστές και εξοπλισμοί αντιπροσωπεύουν ένα σημαντικό ποσοστό των παραβιάσεων δεδομένων. Εάν οι εταιρείες δεν τηρούν τα πρότυπα ασφαλείας του φυσικού εξοπλισμού, εξακολουθούν να θέτουν σε πολύ μεγάλο κίνδυνο την προστασία των δεδομένων, ακόμη και αν έχουν τις πιο εξελιγμένες λύσεις IT.

ΕΙΜΑΣΤΕ ΕΠΟΠΤΕΥΟΜΕΝΟΙ ΣΤΙΣ ΗΠΑ

Ο κανονισμός αποτελεί ένα μόνο στοιχείο κόστους της παραβίασης στον κυβερνοχώρο. Οι οργανισμοί έχουν ευθύνη έναντι των πελατών τους για την ασφαλή διατήρηση των δεδομένων τους. Η δυσφήμιση που προκύπτει από την παραβίαση δεδομένων μπορεί να υπερβεί οποιοδήποτε κόστος συνδέεται

με την παραβίαση των δεδομένων. Ακόμη και χωρίς κρατική εποπτεία, οι βιομηχανίες (όπως η βιομηχανία καρτών πληρωμών) μπορούν και εκδίδουν αυστηρά πρόστιμα.[5]

ΑΝΑΘΕΤΟΥΜΕ ΣΕ ΕΞΩΤΕΡΙΚΟΥΣ ΣΥΝΕΡΓΑΤΕΣ ΤΗΝ ΑΣΦΑΛΕΙΑ ΜΑΣ

Οι περισσότερες εταιρείες αναθέτουν τα στοιχεία αποθήκευσης δεδομένων στην πλατφόρμα νέφους (cloud) και άλλες πλατφόρμες τρίτων. Τα πρότυπα ασφαλείας των εξωτερικών συνεργατών πρέπει να ελέγχονται για να διασφαλίζεται ότι πληρούν τις απαραίτητες απαιτήσεις, ιδίως εφόσον η φύση της δραστηριότητάς τους και ο όγκος των δεδομένων που αποθηκεύουν τους καθιστά ως ελκυστικό στόχο. Οι συμβάσεις με εξωτερικούς παρόχους ασφάλειας συχνά εξαιρούν την ευθύνη από παραβιάσεις, οπότε η επιχείρηση πρέπει να επιβαρυνθεί με τις δαπάνες μετριασμού και υπεράσπισης.

ΕΙΜΑΣΤΕ ΠΟΛΥ ΜΙΚΡΗ ΕΠΙΧΕΙΡΗΣΗ ΓΙΑ ΝΑ ΑΝΗΣΥΧΟΥΜΕ

Καθώς οι μεγάλοι οργανισμοί συνεχίζουν να βελτιώνουν τις υποδομές της ασφάλειάς τους, οι εγκληματίες έχουν αρχίσει να αναζητούν μικρότερους και «ευκολότερους» στόχους. Το 75% των παραβιάσεων δεδομένων συνέβη σε οργανισμούς με λιγότερους από 100 εργαζομένους. Οι μικρότεροι οργανισμοί ενδεχομένως δεν διαθέτουν τους πόρους για αποτελεσματική ασφάλεια έτσι ώστε να αποτρέψουν μια απώλεια ή για αποτελεσματικές στρατηγικές αποκατάστασης μετά από μια απώλεια.

ΤΟ ΚΟΣΤΟΣ ΤΩΝ ΠΑΡΑΒΙΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ ΔΕΝ ΑΞΙΖΕΙ ΤΗΝ ΑΣΦΑΛΙΣΗ

Το 2011 το μέσο κόστος για την επίλυση μιας παραβίασης ασφάλειας δικτύου ήταν μεγαλύτερο από 5 εκατομμύρια δολ. ΗΠΑ, ή 197 δολ. ΗΠΑ ανά αρχείο. Ενώ πολλές παραβιάσεις ασφάλειας δικτύου βρίσκονται κάτω από το μέσο όρο, η επίλυση των συμβάντων ηλεκτρονικού εγκλήματος έχει κοστίσει εκατοντάδες εκατομμύρια στους οργανισμούς.[8]

ΔΕΝ ΜΟΥ ΕΤΥΧΕ ΠΟΤΕ ΠΑΡΑΒΙΑΣΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΟΠΟΤΕ ΔΕΝ ΧΡΕΙΑΖΟΜΑΙ ΑΥΤΗΝ ΤΗΝ ΚΑΛΥΨΗ

Μολονότι η πλειοψηφία των επιχειρήσεων δεν είχε καμία αξίωση, το περιβάλλον έχει αλλάξει. Οι εταιρείες είναι πιο ευαίσθητες στις απειλές ασφάλειας και ιδιωτικού απορρήτου από ποτέ. Η μελλοντική νομοθεσία είναι πιθανό να αυξήσει τα ισχύοντα πρότυπα της βιομηχανίας, υποδηλώνοντας ότι

οι οικονομικές και λειτουργικές επιπτώσεις μιας παραβίασης δεδομένων θα καταστούν πιο επαχθείς για τους οργανισμούς που έχουν υποστεί, παραβίαση.

2.6 Γενική ορολογία καλύψεων

Η παράγραφος αυτή χωρίζεται σε δύο μέρη. Στο πρώτο μέρος παρατίθεται μία σειρά σεναρίων, βασισμένων σε πραγματικά περιστατικά, τα οποία απεικονίζουν το εύρος των καλύψεων που παρέχει κυρίως το CyberEdge και το DUAL.

2.6.1 Σενάρια απαιτήσεων

ΚΑΚΟΒΟΥΛΕΣ ΠΡΑΞΕΙΣ ΕΡΓΑΖΟΜΕΝΩΝ

Ένας υπάλληλος ενός μεγάλου οργανισμού ελέγχου πιστοληπτικής ικανότητας κλέβει τις προσωπικές πληροφορίες εκατομμυρίων πελατών.

ΚΑΛΥΨΕΙΣ

- Το κόστος των εγκληματολόγων που θα καθορίσουν ποια στοιχεία έχουν κλαπεί και από ποια άτομα.
- Το κόστος της ενημέρωσης του πλήθους των ατόμων των οποίων τα δεδομένα έχουν κλαπεί
- Το κόστος παρακολούθησης της πίστωσης για τα πρόσωπα που έχουν επηρεαστεί, για να βεβαιωθούμε ότι δεν υφίστανται συνεχείς απώλειες μετά την κλοπή των πληροφοριών
- Το κόστος της νομικής ενημέρωσης παραβιάσεων για την προετοιμασία της επιχείρησης για έρευνα των αρχών
- Το κόστος της εκπροσώπησης και της υπεράσπισης της επιχείρησης στην επακόλουθη προσφυγή που ασκήθηκε εναντίον της
- Το κόστος των ζημιών που αποδίδονται στην επιχείρηση[5]

ΑΠΩΛΕΙΑ ΣΤΟΥΣ ΠΑΡΟΧΟΥΣ

Έχει κλαπεί ο διακομιστής e-mail και ο σκληρός δίσκος μιας επιχείρησης ενώ ήταν στην κατοχή ενός εξωτερικού συνεργάτη

ΚΑΛΥΨΕΙΣ

- Το κόστος των εγκληματολόγων που θα καθορίσουν ποια στοιχεία έχουν κλαπεί και από ποια άτομα.

- Το κόστος της ενημέρωσης των ατόμων των οποίων τα δεδομένα έχουν κλαπεί
- Το κόστος παρακολούθησης της πίστωσης για τα πρόσωπα που έχουν επηρεαστεί, για να διαβεβαιώσουμε ότι δεν υφίστανται συνεχείς απώλειες μετά την κλοπή των πληροφοριών
- Το κόστος των συμβούλων δημοσίων σχέσεων για να συμβουλεύσουν και να καθοδηγήσουν την εταιρεία στην επαφή της με τα μέσα επικοινωνίας σχετικά με το συμβάν[5]

ΠΑΡΑΒΙΑΣΗ ΔΙΚΤΥΟΥ- ΞΕΝΟΔΟΧΕΙΑ

Οι χάκερ απέκτησαν πρόσβαση σε συστήματα υπολογιστών ξενοδοχείων σε 26 Τοποθεσίες

ΚΑΛΥΨΕΙΣ

- Το κόστος των εγκληματολόγων που θα καθορίσουν ποια στοιχεία έχουν κλαπεί και από ποια
- Σύμβουλοι δημοσίων σχέσεων για να συμβουλεύσουν την επιχείρηση σχετικά με το μετριασμό της δυσφήμισης μετά το περιστατικό[5]

ΠΑΡΑΒΙΑΣΗ ΔΙΚΤΥΟΥ- ΚΑΡΤΕΣ

Ένα σύστημα πληρωμών με κάρτες έχει παραβιαστεί θέτοντας σε κίνδυνο τα δεδομένα πιστωτικών καρτών

ΚΑΛΥΨΕΙΣ

- Το κόστος των συμβούλων δημοσίων σχέσεων για να μετριάσουν τη δυσφήμιση της επιχείρησης μετά την παραβίαση
- Το κόστος επαγγελματικής εκπροσώπησης για την έρευνα από τη βιομηχανία πληρωμής με κάρτες
- Κόστος νομικής εκπροσώπησης και υπεράσπισης για τη νομική διαδικασία που ασκήθηκε κατά της εταιρείας[5]

Μερικά ακόμα παραδείγματα:

ΤΕΡΜΑΤΙΚΟ ΠΩΛΗΣΕΩΝ

Το τερματικό ενός σουπερμάρκετ δέχθηκε επίθεση από εξωτερικό κακόβουλο λογισμικό, διακόπτοντας την επικοινωνία μεταξύ των μητρώων και του μηχανήματος απογραφής. Το σουπερμάρκετ παρουσίασε έλλειψη

αποθέματος και έπρεπε να κλείσει μέχρι να διορθωθεί το σύστημα και να αναπληρωθεί το απόθεμα.[2]

ΚΑΤΑΓΡΑΦΗ ΕΓΓΡΑΦΩΝ

Πραγματοποιήθηκε διείσδυση στο σύστημα του σημείου πωλήσεων σε περισσότερα από 200 καταστήματα λιανικής πώλησης (συμπεριλαμβανομένων 150 υποκαταστημάτων μεγάλης αλυσίδας fast food), με αποτέλεσμα τα κακόβουλα προγράμματα καταγραφής να καταγράφουν όλα τα δεδομένα που πληκτρολογούνται ή σαρώνονται μέσω του συστήματος.[2]

ΕΦΕΔΡΙΚΕΣ ΤΑΙΝΙΕΣ

Μια πολυεθνική ασφαλιστική εταιρεία τιμωρήθηκε με πρόστιμο πολλών εκατομμυρίων λιρών από τη ρυθμιστική αρχή του Ηνωμένου Βασιλείου, όταν έχασε μια εφεδρική ταινία που περιείχε προσωπικά στοιχεία περισσότερων από 46.000 ασφαλισμένων.[2]

ΜΑΚΡΟΧΡΟΝΙΕΣ ΕΓΚΛΗΜΑΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ

Για περισσότερα από 4 χρόνια, γινόταν υποκλοπή αποκλειστικών πληροφοριών πολλών από τους μεγαλύτερους οργανισμούς πετρελαίου και φυσικού αερίου. Εφαρμόστηκαν τεχνικές τεμαχισμού για υπεξαίρεση επικοινωνιών και δεδομένων σχετικά με συγκεκριμένα θέματα της βιομηχανίας, συμπεριλαμβανομένης της διερεύνησης για πετρέλαιο και συνεργασιών μεταξύ των «μολυσμένων» οργανισμών.[2]

2.6.2 Περίληψη καλύψεων

Στη συνέχεια παρατίθεται μια περίληψη των καλύψεων που παρέχονται από τις AIG και LLOYDS.

2.6.2.1 Οικονομικό κόστος

ΟΙΚΟΝΟΜΙΚΟ ΚΟΣΤΟΣ ΕΑΝ Η ΕΠΙΧΕΙΡΗΣΗ ΠΡΟΞΕΝΗΣΕΙ ΖΗΜΙΑ ΣΕ ΤΡΙΤΟΥΣ

- Το κόστος της ειδοποίησης των πελατών (ή της ρυθμιστικής αρχής) ότι τα δεδομένα τους έχουν επηρεαστεί από την παραβίαση. Εύλογα έξοδα για την ενημέρωση αναφορικά με κλοπές ταυτότητας και παρακολούθηση αρχείων πίστωσης όσων ενεπλάκησαν.

- Κόστος υπεράσπισης και ζημιές εάν η επιχείρηση (ή ο εξωτερικός συνεργάτης διαχείρισης) προκαλέσει παραβίαση προσωπικών ή εταιρικών δεδομένων.
- Κόστος υπεράσπισης και ζημιές εάν η επιχείρηση μολύνει τα δεδομένων τρίτων με ιό.
- Κόστος υπεράσπισης και ζημιές εάν η επιχείρηση υποστεί κλοπή κωδικού πρόσβασης στο σύστημα με μη ηλεκτρονικά μέσα.
- Κόστος υπεράσπισης και ζημιές εάν η επιχείρηση υποστεί κλοπή εξοπλισμού που περιέχει προσωπικά δεδομένα.
- Κόστος υπεράσπισης και ζημιές εάν κάποιος εργαζόμενος της επιχείρησης προκαλέσει αποκάλυψη δεδομένων.

ΟΙΚΟΝΟΜΙΚΟ ΚΟΣΤΟΣ ΝΟΜΟΘΕΣΙΑΣ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

- Το κόστος παροχής νομικών συμβουλών και εκπροσώπησης σε σχέση με μια έρευνα προστασίας δεδομένων.
- Ασφαλιστέα πρόστιμα και κυρώσεις που επιβάλλονται από τη ρυθμιστική αρχή προστασίας δεδομένων.

2.6.2.2 *Συμβουλευτικές υπηρεσίες*

ΕΙΔΙΚΟΙ ΣΥΜΒΟΥΛΟΙ ΙΤ ΓΙΑ ΤΗΝ ΕΠΙΧΕΙΡΗΣΗ ΚΑΤΑ ΤΗ ΔΙΑΡΚΕΙΑ ΚΑΙ ΜΕΤΑ ΑΠΟ ΗΛΕΚΤΡΟΝΙΚΗ ΠΑΡΑΒΙΑΣΗ

- Ομάδα αντιμετώπισης περιστατικών στον κυβερνοχώρο για να βοηθά τον πελάτη, εάν νομίζει ότι δέχεται επίθεση.
- Βοήθεια σε ασφαλισμένους από ειδικούς, μετά από παραβίαση δεδομένων, για την αποκατάσταση των συστημάτων τους και των τειχών προστασίας, που θα επιτρέπει στην επιχείρηση να επανέλθει στην κανονική λειτουργία.
- Το κόστος των επαγγελματικών αμοιβών που προκύπτουν προκειμένου να προσδιοριστεί αν τα ηλεκτρονικά δεδομένα μπορούν ή όχι να αποκατασταθούν, να επανασυλλεχθούν ή να αναδημιουργηθούν.

ΕΙΔΙΚΟΙ ΣΥΜΒΟΥΛΟΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΤΗΝ ΑΠΟΚΑΤΑΣΤΑΣΗ ΤΗΣ ΦΗΜΗΣ ΜΙΑΣ ΕΤΑΙΡΕΙΑΣ ΜΕΤΑ ΑΠΟ ΠΑΡΑΒΙΑΣΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

- Κόστος επαγγελματικών συμβουλών για την πρόληψη ή την ελαχιστοποίηση ενδεχόμενων αρνητικών επιπτώσεων κάποιου σημαντικού συμβάντος ηλεκτρονικού εγκλήματος.

- Κόστος επαγγελματικών συμβουλών για την ελαχιστοποίηση ενδεχόμενης ζημιάς στη φήμη οποιουδήποτε ατόμου στην εταιρεία (π.χ. του γενικού Διευθυντή).

2.6.2.3 *Προαιρετικές καλύψεις*

ΔΙΑΚΟΠΗ ΛΕΙΤΟΥΡΓΙΑΣ ΤΟΥ ΔΙΚΤΥΟΥ

Απώλεια καθαρού κέρδους, ως αποτέλεσμα της διακοπής λειτουργίας στο δίκτυο του ασφαλισμένου, που προκλήθηκε από παραβίαση της ασφάλειας.

ΚΑΛΥΨΗ ΕΚΒΙΑΣΜΟΥ

Πληρωμές λύτρων (απώλεια από εκβίαση) προς τρίτους που προκύπτουν για την αντιμετώπιση μιας απειλής για την ασφάλεια δεδομένων.

ΕΥΘΥΝΗ ΠΟΛΥΜΕΣΩΝ

Κόστος ζημιών και υπεράσπισης που προκύπτει σε σχέση με την παραβίαση πνευματικής ιδιοκτησίας τρίτων, ή αμέλεια σε σχέση με ηλεκτρονικό περιεχόμενο.

3. Ανάγκες της αγοράς

Στο κεφάλαιο αυτό θα κάνουμε έναν απολογισμό των αναγκών των εταιρειών οι οποίες είναι ευπαθείς σε κυβερνοεπιθέσεις, καθώς και των σχετικών αναγκών τους για μια καλύτερη και ασφαλέστερη λειτουργία. Επίσης, θα ελέγξουμε, βάσει κάποιον νέων νόμων, τις κυρώσεις προς τις εταιρίες οι οποίες διέπονται από τις ευπάθειες που αναφέρθηκαν παραπάνω και, παράλληλα, δεν ενεργούν για την αντιμετώπισή τους.

3.1 Εισαγωγή

Ο Νέος Ευρωπαϊκός κανονισμός για τα Προσωπικά Δεδομένα, ο οποίος ψηφίστηκε στις 14/04/2016 και η εφαρμογή του αρχίζει το 2018, προβλέπει, για τις εταιρείες που δε θα καταφέρουν να διατηρήσουν την ασφάλεια των δεδομένων τους, διοικητικά πρόστιμα για παραβίαση των κανόνων που φθάνουν μέχρι τα €20 εκατομμύρια ή έως 4% του ετήσιου κύκλου εργασιών του προηγούμενου έτους τους. Βάσει αυτού του νόμου, πολλές εταιρείες, πέραν της καλής και ασφαλούς λειτουργίας τους, αναγκάζονται να προχωρήσουν σε καλύψεις έναντι κυβερνοεπιθέσεων. Παρακάτω αναλύουμε τη ζήτηση που ανοίγει ο νόμος αυτός στην αγορά και τις πραγματικές ανάγκες αυτής χωρίς τον εξαναγκασμό του νόμου.

3.1.1 Διαχείριση του κινδύνου

Πολλές χώρες εντός και εκτός των συνόρων της ΕΕ, έχουν δημοσιεύσει στρατηγικές που ακολουθούν, στις οποίες περιγράφουν την επίσημη στάση τους για τον κυβερνοχώρο, την ασφάλειά τους και το κυβερνοέγκλημα. Παρόλα αυτά, παρατηρείται ότι λίγες από αυτές τις πηγές δείχνουν να διαχωρίζουν τις έννοιες τις κυβερνοασφάλειας και της ασφάλειας πληροφοριών. Η αυξανόμενη εξάρτηση από τις τεχνολογίες πληροφοριών και επικοινωνιών σε όλους του τομείς της ανθρώπινης ζωής είναι δεδομένη, με το διαδίκτυο να παίζει πρωταγωνιστικό ρόλο. Η διαχείριση, όμως, των πόρων, των πρωτοκόλλων, καθώς και των εργαλείων ανάπτυξης των διαδικτυακών χώρων δε ρυθμίζεται από συγκεκριμένα όργανα, αλλά αντίθετα ακολουθεί την αρχή μιας πολυμερούς διακυβέρνησης, στην οποία συμμετέχει ένα πλήθος, κυβερνητικών και μη, παραγόντων. Όλοι οι εμπλεκόμενοι φορείς, ήτοι οι κυβερνήσεις, οι δημόσιες αρχές, ο ιδιωτικός τομέας ή οι μεμονωμένοι πολίτες, πρέπει να αναγνωρίσουν τη συνυπευθυνότητα, να αναλάβουν δράση για να αυτοπροστατευθούν και να

συνεργάζονται για την εξασφάλιση συντονισμένης αντίδρασης με σκοπό την ενίσχυση της ασφάλειας του κυβερνοχώρου.

3.1.2 Ασφάλεια των πληροφοριών

Η ασφάλεια πληροφοριών ερμηνεύεται με πολλούς και διαφορετικούς τρόπους, όπως:

1) Η διατήρηση της ακεραιότητας, του απορρήτου και της προσβασιμότητας των πληροφοριών, οι οποίες μπορούν να έχουν πολλές μορφές (πχ. έντυπη, ηλεκτρονική), (ISO/IEC 27002, 2005).

2) Η προστασία της πληροφορίας και των κρίσιμων στοιχείων της (συστήματα και hardware που τη μεταφέρουν, την αποθηκεύουν, τη χρησιμοποιούν).

Ορισμένα κρίσιμα χαρακτηριστικά της πληροφορίας, τα οποία έχουν αξία για τους οργανισμούς και τους απλούς χρήστες, είναι τα εξής:

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity)
- Προσβασιμότητα (Availability) ,ISO/IEC 27002(2005)

Η διασφάλιση των τριών αυτών χαρακτηριστικών είναι γνωστή ως το μοντέλο CIA, το οποίο έχει ενταχθεί στα βιομηχανικά πρότυπα. Το μοντέλο αυτό, όμως, δεν μπορεί να είναι επαρκές απέναντι στο διαρκώς εξελισσόμενο περιβάλλον της βιομηχανίας των υπολογιστών. Έτσι, προστέθηκαν από τους Whitman και Mattord (2009) στη λίστα των χαρακτηριστικών της πληροφορίας, που πρέπει να προστατευτούν, τα παρακάτω:

- Ακρίβεια (accuracy)
- Αυθεντικότητα (authenticity)
- Χρησιμότητα (utility)
- Κατοχή (possession)

Τα παραπάνω χαρακτηριστικά προστέθηκαν για να αντιμετωπιστούν οι πρόσθετες ανάγκες ασφάλειας των οργανισμών στο σημερινό διαδικτυακό περιβάλλον. Τα παραπάνω χαρακτηριστικά παίζουν σπουδαίο ρόλο στην ασφάλεια των πληροφοριών. Το καθένα από αυτά, όμως, έχει διαφορετική σημασία ανάλογα με το είδος της πληροφορίας, και ίσως, κάποια από αυτά, σε ορισμένες περιπτώσεις, να μην απαιτούνται. Για παράδειγμα, δεν

απαιτείται η εμπιστευτικότητα, όταν μία πληροφορία είναι δεδομένο ότι είναι προσβάσιμη από όλους. Βέβαια, ένας οργανισμός για να βεβαιωθεί για την ασφάλεια των πληροφοριών που τον αφορούν, το ζήτημα δεν είναι να αποφασίσει ποια από τα χαρακτηριστικά της ασφάλειας πληροφοριών εφαρμόζονται αλλά να καθορίσει τις εξουσιοδοτημένες οντότητες καθώς και κάθε άλλη παράμετρο για κάθε δοθείσα πληροφορία.

3.1.3 Εμπιστοσύνη των χρηστών στο διαδίκτυο και τις εταιρείες

Η εμπιστοσύνη έχει πολύ μεγάλη αξία σε μια κοινωνία: από ένα απλό ραντεβού με κάποιον που μας ενδιαφέρει μέχρι κάθε εμπορική συμφωνία, η δυνατότητα να εμπιστευτούμε καθορίζει το αν θα δεχτούμε να συμμετέχουμε σε οποιαδήποτε "κοινωνική συναλλαγή". Το αίσθημα εμπιστοσύνης όμως δεν εμφανίζεται αυθαίρετα.

Εδώ και αιώνες βασίζουμε την πίστη μας στους άλλους στα κοινά μας σημεία: η φυλή, η οικογένεια, η θρησκεία, ο τόπος διαβίωσης κλπ. είναι πτυχές της ζωής οι οποίες μας συνδέουν με άλλους (ή μας χωρίζουν!) και συντελούν στη δημιουργία ενός αμοιβαίου, στοιχειώδους έστω, αισθήματος εμπιστοσύνης. Το πρόβλημα με αυτά τα κριτήρια είναι ότι το άτομο έχει ελάχιστη ως καθόλου δυνατότητα να τα καθορίσει. Έτσι, κάποιος μπορεί να δυσκολεύεται στις κοινωνικές επαφές του λόγω της καταγωγής του ενώ κάποιος άλλης μπορεί να χαίρει εμπιστοσύνης που δεν του αξίζει, λόγω της καλής φήμης της οικογενείας του. Χάρη στο διαδίκτυο όμως, ένα νέο είδες εμπιστοσύνης έχει εμφανιστεί τελευταία: η εμπιστοσύνη σε ένα προσωπικό online προφίλ.

Περίπου στα μέσα της δεκαετίας του '90 εμφανίστηκαν οι πρώτες ιστοσελίδες μέσω των οποίων μπορούσαν να πραγματοποιηθούν συναλλαγές (εμπορικές ή όχι) μεταξύ ατόμων. Ψηφιακές πλατφόρμες, δηλαδή, που συνέδεαν ανθρώπους που είχαν κάτι να προσφέρουν με άλλους που το είχαν ανάγκη. Μια από τις πρώτες και πιο χαρακτηριστικές είναι το eBay το οποίο δημιουργήθηκε το 1995 ως μια πλατφόρμα μέσω της οποίας οποιοσδήποτε θα μπορούσε να αγοράσει και να πουλήσει μεταχειρισμένα αντικείμενα σε άλλους ιδιώτες οπουδήποτε στον κόσμο. Ένα άλλο παράδειγμα είναι το Couchsurfing το οποίο δημιουργήθηκε λίγο πριν το 2000 και μέσω του οποίου ταξιδιώτες μπορούν να γνωρίζουν ντόπιους εκεί που ταξιδεύουν με σκοπό να συνδεθούν καλύτερα με τον τόπο στον οποίο

βρίσκονται ή και να φιλοξενηθούν. Τέτοιες υπηρεσίες διαμοιρασμού και κοινής χρήσης πόρων εμφανίζονται έκτοτε συνεχώς, με το "κίνημα" να περιγράφεται συνοπτικά ως συνεργατική κατανάλωση και να χαρακτηρίζεται το 2010 από το περιοδικό TIME ως μια από τις σημαντικότερες ιδέες της χρονιάς.

Εν έτει 2016 μπορεί κανείς να μοιραστεί στο διαδίκτυο από αυτοκίνητα, εργαλεία και κατοικίες μέχρι μωρουδιακά είδη και κοσμήματα. Πλεονέκτημα αυτής της μορφής κατανάλωσης είναι ότι επιτρέπει την πιο αποδοτική αξιοποίηση πόρων οι οποίοι υπο-χρησιμοποιούνται. Σκεφτείτε, για παράδειγμα, πόσες ώρες την ημέρα παραμένει παρκαρισμένο το αυτοκίνητό σας ενώ θα μπορούσε να χρησιμοποιηθεί από ένα γείτονά ο οποίος το έχει ανάγκη για να "πεταχτεί" κάπου. Κατ' αυτό τον τρόπο μπορούμε να αγοράζουμε λιγότερα και συνεπώς να παράγουμε και λιγότερα, με ότι θετικές συνέπειες έχει αυτό για το φυσικό περιβάλλον.

Ένα ακόμα αποτέλεσμα, και αυτό που μας ενδιαφέρει πιο πολύ είναι ότι μέσω αυτών των δικτύων δημιουργούνται κοινωνικές επαφές μεταξύ αγνώστων. Οι χρήστες των υπηρεσιών συνεργατικής κατανάλωσης δημιουργούν σε αυτές ένα, δημόσιο και ορατό στους άλλους χρήστες, online προφίλ: συμπληρώνουν το όνομά τους, ανεβάζουν μια φωτογραφία τους και προσθέτουν κατά περίπτωση άλλα στοιχεία που τους αφορούν. Για παράδειγμα, στην υπηρεσία BlaBlaCar , μέσω της οποίας μπορούμε να βρούμε κάποιον για να συνταξιδέψουμε με το αυτοκίνητό του, θα ήταν χρήσιμο και ασφαλές να γνωρίζουμε τις πινακίδες του αυτοκινήτου και τον αριθμό τηλεφώνου του οδηγού. Ωστόσο, το στοιχείο του προφίλ που συνεισφέρει περισσότερο στο αίσθημα ασφάλειας είναι οι κριτικές που έχει λάβει ο χρήστης από άλλους χρήστες της υπηρεσίας τους οποίους γνώρισε σε παλιότερες συναλλαγές του. Η κριτική γίνεται δημόσια, είναι ορατή στο προφίλ και σε αυτή δεν μπορεί να παρέμβει ο κάτοχος του προφίλ για να την αλλοιώσει προς όφελός του. Έτσι, για παράδειγμα, δύο άγνωστοι που ήρθαν σε επαφή μέσω του Couchsurfing καλούνται μετά τη γνωριμία τους να γράψουν μια δημόσια κριτική ο ένας για τον άλλο. Κατ' αυτό τον τρόπο, οποιοσδήποτε μελλοντικός επισκέπτης κάποιου από αυτά τα προφίλ έχει τη δυνατότητα να γνωρίζει αν μπορεί να εμπιστευτεί τον συγκεκριμένο χρήστη πριν κάνει το βήμα να επικοινωνήσει μαζί του. Αυτό ενισχύει το αίσθημα ασφάλειας στα πλαίσια της κοινότητας των μελών της υπηρεσίας και διευκολύνει τη δημιουργία επαφών μεταξύ των χρηστών.

Οι κριτικές τις οποίες συγκεντρώνουμε συμμετέχοντας στα online κοινωνικά δίκτυα διαμοιρασμού και κοινής χρήσης πόρων δημιουργούν την online φήμη μας (reputation). Πρόκειται για δεδομένα διάσπαρτα στις διάφορες διαδικτυακές υπηρεσίες τα οποία αποδεικνύουν ότι είμαστε αξιόπιστα άτομα γιατί έχουμε υπάρξει επανειλημμένα "εντάξει" στις συναλλαγές που κάναμε με άλλους ανθρώπους, αγνώστους με τους οποίους ήρθαμε σε επαφή μέσω του ίντερνετ.

Ο κάθε χρήστης μπορεί να έχει μερικές δεκάδες "συστάσεις" από άλλους σχετικά με το πόσο καλός υπήρξε σε δεδομένες κοινωνικές συναλλαγές. Σαν οικοδεσπότης, σαν συνταξιδιώτης ή απλά όταν δανείστηκε κάποιο εργαλείο από κάποιον και το επέστρεψε στην ώρα του και σε καλή κατάσταση. Σε αυτά τα δεδομένα μπορούν να προστεθούν και στοιχεία που αφορούν τη συνεισφορά μας σε online κοινότητες, όπως για παράδειγμα το Stack Exchange ή το Quora ή διάφορες άλλες κοινότητες συζητήσεων στις οποίες συμμετέχουμε επώνυμα. Από την ανάγκη να αξιοποιήσουμε την online φήμη μας, η οποία βρίσκεται κατακερματισμένη στους διάφορους λογαριασμούς μας στο διαδίκτυο, προέκυψαν υπηρεσίες που συγκεντρώνουν τα παραπάνω δεδομένα και τα αναδεικνύουν, προβάλλοντας σε (ακόμα) ένα ψηφιακό προφίλ τις "επιδόσεις αξιοπιστίας" μας.

3.2 Η λύση Cyber Secure της Ελληνικής αγοράς.

Το κόστος των κυβερνοεπιθέσεων που θα δεχτούν επιχειρήσεις και οργανισμοί την επόμενη δεκαετία (2015-2025) ανέρχεται σε $1.06 δις δολάρια του εκτιμώμενου Α.Ε.Π. της Ελλάδας. Οι παραβιάσεις συστημάτων και η κυβερνοασφάλεια είναι μία πηγή ανησυχίας κάθε εταιρίας δεδομένης της φύσης των πληροφοριών που διαχειρίζεται.

Όπως αποδεικνύεται από πρόσφατες παραβιάσεις συστημάτων, το πώς ένας οργανισμός χειρίζεται μια κρίση παίζει σημαντικό ρόλο στο κατά πόσο ο Διευθύνων Σύμβουλος και τα ανώτατα στελέχη (CIO, COO, CMO, CRO, CFO κ.λπ.) παραμένουν στη θέση τους. Σύμφωνα με τη νέα Ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, οι εταιρίες που δε θα καταφέρουν να διατηρήσουν την ασφάλεια των δεδομένων τους κινδυνεύουν με διοικητικά πρόστιμα για παραβίαση των κανόνων που φθάνουν μέχρι €20 εκατομμύρια ή έως 4% του ετήσιου κύκλου εργασιών της εταιρίας.

Λαμβάνοντας υπόψη τις συνθήκες της αγοράς η Cromar σχεδίασε την λύση Cyber Secure Solution, η οποία υποστηρίζεται από την αγορά, της Lloyd's. Πιο συγκεκριμένα, μέσω της λύσης Cyber Secure Solution διατίθεται στην ελληνική αγορά, σε συνεργασία με τους Beazley, μία από τις καλύτερες ασφαλιστικές λύσεις διαχείρισης περιστατικών απώλειας εμπιστευτικών πληροφοριών και προσωπικών δεδομένων παγκοσμίως το "Beazley Global Breach Solution". Το "Beazley Global Breach Solution" αποτελεί μια συνολική λύση αποτελεσματικής διαχείρισης των κινδύνων παραβίασης συστημάτων και απώλειας δεδομένων και επιτρέπει στις επιχειρήσεις να διαχειριστούν την αυξανόμενη ευθύνη τους και να μετριάσουν τον κίνδυνο να θιγεί η εταιρική φήμη από πιθανή παραβίαση συστημάτων και απώλεια των δεδομένων αυτών.Το "Beazley Global Breach Solution" προσφέρει, εκτός από τις χρηματικές αποζημιώσεις, πρόσβαση στην Ομάδα Διαχείρισης Περιστατικών του η οποία έχει αντιμετωπίσει πάνω από 3.000 περιστατικά παγκοσμίως.

3.2.1 Ανάγκες που δημιουργούνται βάσει του νέου νόμου

Βάσει του νέου νόμου, που θα ισχύσει από το 2018, οι περισσότερες αν όχι όλες οι εταιρείες που λειτουργούν στην Ελλάδα υπόκεινται σε διάφορες κυρώσεις σε περίπτωση που δεν καλύψουν τις παρακάτω ανάγκες που αναμένεται να εμφανιστούν. Αυτές είναι:

- Αστική Ευθύνη έναντι τρίτων οι οποίοι υπέστησαν ζημιά λόγω απώλειας των προσωπικών τους δεδομένων από την εταιρία στην οποία τα είχαν δώσει.
- Ανταπόκριση: Έξοδα και Υπηρεσίες διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών.
- Διακοπή Εργασιών: Κάλυψη για απώλεια εσόδων λόγω διακοπής της επιχειρηματικής δραστηριότητας από περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών.
- Κυβερνοεκβιασμός: Κάλυψη για διαχείριση περιστατικών εκβιασμού από απειλές που μπορεί να βλάψουν ένα δίκτυο ή να οδηγήσουν σε διαρροή εμπιστευτικών πληροφοριών.
- Υπηρεσίες υψηλού επιπέδου σε Ευρωπαϊκά πρότυπα.

3.2.2 Εταιρείες που επηρεάζονται

Παρακάτω εξετάζονται οι εταιρείες και οι τύποι των εταιριών που επηρεάζονται απο το νέο νόμο:

- Τηλεπικοινωνίες – Internet Services Providers
- Τράπεζες, Χρηματιστηριακές, Ασφαλιστικές
- Πάροχοι Υπηρεσιών Υγείας
- Πάροχοι ενέργειας
- Μεταφορικές Εταιρίες
- Εκπαιδευτικά Ιδρύματα
- Αλυσίδες λιανικής πώλησης(Retailers)
- Δικηγορικές Εταιρίες
- Συμβουλευτικές Εταιρίες
- Εταιρίες που διενεργούν συναλλαγές με Πιστωτικές, Χρεωστικές, κάρτες επιβράβευσης εμπιστοσύνης(Loyalty Cards)
- Όλες οι εταιρίες που θέλουν να προστατεύσουν το εταιρικό τους δίκτυο από τις χρηματοοικονομικές συνέπειες ενός περιστατικού άρνησης παροχής υπηρεσίας (DDoS).

Λίγο πολύ ο νέος νόμος επηρεάζει, για τα καλά, σχεδόν όλων των ειδών τις εταιρίες και ανοίγει στήν αγορά αρκετές ευκαιρίες για τος ασφαλιστικές εταιρείες λόγω της μεγάλης ζήτησης και ανάγκης που διαμορφώνεται. Πλέον δεν θα είναι θέμα επιλογής οι ασφάλειες έναντι κυβερνοεπιθέσεων, αλλά θέμα ανάγκης και επιβίωσης.

3.2.3 Ο Νόμος

Η ΕΕ επέκτεινε το δίχτυ κυβερνο-ασφάλειας των 28 κρατών-μελών, συμφωνώντας σε νέους κανόνες οι οποίοι υποχρεώνουν τις επιχειρήσεις να αυξήσουν την ασφάλεια κατά επιθέσεων του κυβερνοχώρου και επιβάλλουν σε εταιρίες όπως η Google και η Amazon να το δηλώνουν όταν δέχονται επίθεση.

Ο Νόμος, ο οποίος αναμένεται να επικυρωθεί επίσημα, θα υποχρεώσει όλες τις χώρες της ΕΕ να μοιραστούν περισσότερες πληροφορίες και θα επιβάλλει στις μηχανές αναζήτησης, στις υπηρεσίες cloud και σε καταστήματα λιανικής μέσω διαδικτύου να διασφαλίσουν πως η υποδομή τους είναι ασφαλής, σύμφωνα με τον Ευρωκοινοβούλιο.

«Οι σημαντικοί φορείς σε βιομηχανίες όπως η ενέργεια, η μεταφορά, η υγεία και η χρηματοοικονομία θα πρέπει να ανταπεξέλθουν σε ό,τι αφορά τα νέα μέτρα ασφαλείας και να ειδοποιούν σε περίπτωση επιθέσεων του κυβερνοχώρου» ανέφερε ο Andreas Schwab, επικεφαλής της ομάδας που

συνέταξε τη νομοθεσία. Η συμφωνία ακολουθεί την παρόμοια απόφαση των αρχών των ΗΠΑ να δώσουν πρόσβαση σε υπηρεσίες επιβολής του Νόμου, των κρυπτογραφημένων διαβιβάσεων, μετά από πρόσφατες τρομοκρατικές επιθέσεις. Οι εταιρίες όπως η Google, Apple και Yahoo! έχουν ήδη ενσωματώσει πιο στιβαρή κωδικοποίηση στα προϊόντα τους μετά από τις αποκαλύψεις του Edward Snowden το 2013. Οι νέοι κανόνες αυτοί αναμένουν την έγκριση του Ευρωκοινοβουλίου.

Ο πρώτος νόμος cybersecurity της Ευρώπης θα περιλαμβάνει κανόνες για την προστασία των υποδομών από τους χάκερ. Αεροδρόμια και σταθμοί ηλεκτρικού ρεύματος είναι πιθανοί στόχοι των χάκερ και η Ευρώπη θέλει να είναι προστατευμένη έναντι των απειλών. Η ντιρεκτίβα είναι η πρώτη κοινή προσέγγιση της Ευρώπης στην ασφάλεια των δικτύων, είτε αυτή απειλείται από ανθρώπινα λάθη, τεχνικά σφάλματά ή κακόβουλες επιθέσεις. Το Enisa [European Agency for Network and Information Security] υπολογίζει το κόστος των απωλειών από τους παραπάνω παράγοντες σε €260 με €340 δισ.

3.3 Ανάγκες των Ελληνικών εταιρειών

Με την βοήθεια μίας εκ των δύο (2) μεγαλύτερων ασφαλιστικών εταιριών στην Ελλάδα στις κυβερνοασφάλειες, μπορέσαμε να συλλέξουμε στοιχεία από κάποιους πελάτες της εταιρείας αυτής και παράλληλα έγινε έρευνα των αναγκών των εταιρειών που λειτουργούν και εδρεύουν στην Ελλάδα, για να δούμε κατά πόσο οι ανάγκες αυτές καλύπτονται από τα ήδη ισχύοντα ασφαλιστικά συμβόλαια και κατά πόσο αυτά σχετίζονται με τα ευρωπαϊκά κριτήρια.

3.3.1 Υπευθυνότητα στον κυβερνοχώρο

Η πληροφορική είναι ένα κρίσιμο μέρος των δραστηριοτήτων των επιχειρήσεων. Το σσημαντικότερο ως προς αυτό είναι το γεγονός ότι το χάσμα μεταξύ των ανθρώπων που χρησιμοποιούν την πληροφορική και των ανθρώπων που την καταλαβαίνουν είναι μεγάλο και αυξανόμενο. Η θετική πλευρά, η συνειδητοποίηση αυτού του κενού έχει οδηγήσει σε ένα μεγαλύτερο επίπεδο ενδιαφέροντος για την ευθύνη στον κυβερνοχώρο σε επίπεδο διοικητικού συμβουλίου και σε επίπεδο νομοθετών της ΕΕ έτσι ώστε να τίθονται περισσότεροι κανόνες και κανονισμοί προκειμένου να αντιμετωπιστεί η αυξανόμενη απειλή στον κυβερνοχώρο. Ωστόσο, πρέπει να γίνει διάκριση μεταξύ κινδύνων στον κυβερνοχώρο και κινδύνων

πληροφοριών. Η ποικιλία και το εύρος των απειλών στον κυβερνοχώρο έχει αυξηθεί πάρα πολύ τα τελευταία 10 χρόνια. Μια από της πιο ανησυχητικές τάσεις στον τομέα αυτό είναι το γεγονός ότι ο κυβερνοχώρος έχει γίνει ο επόμενο στόχος στον διεθνή πόλεμο.

3.3.1.1 Επιπτώσεις στις επιχειρήσεις

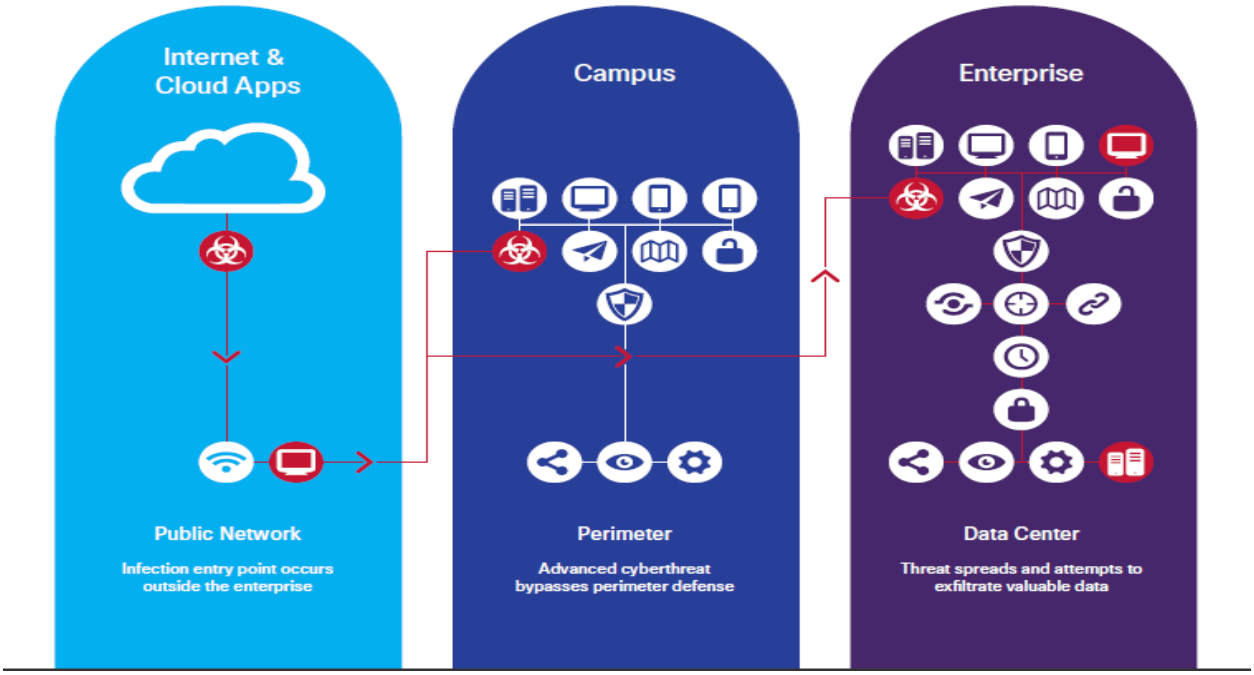
Για τις επιχειρήσεις, όλες αυτές οι εξελίξεις μπορούν να δημιουργήσουν τόσο άμεσες όσο και έμμεσες υποχρεώσεις και προβλήματα. Ο πρωταρχικός στόχος του ιού stuxnet, για παράδειγμα, ήταν να ματαιώσει τις πυρηνικές φιλοδοξίες της ιρανικής κυβέρνησης, αλλά είχε επίσης καταστροφικές συνέπειες για την Siemens και τους χρήστες των τεχνολογικών μηχανημάτων της. Στα πλαίσια αυτά, ένα άλλο παράδειγμα είναι η περίπτωση της Megaupload. Ο Vael τόνισε τη σημασία της ως μιας ψηφιακής πλατφόρμας αποθήκευσης που χρησιμοποιείται από εταιρείες που επιθυμούν να είναι πιο αποτελεσματικές στην αποθήκευση των δεδομένων τους. Ωστόσο, η Megaupload χρησιμοποιείται ακόμα και για την αποθήκευση πειρατικού λογισμικού και περιεχομένου. Σε συνέχεια αυτού, ο ιδρυτής της εταιρείας Kim Dotcom συνελήφθη και οι αρχές κατάσχεσαν όλα τα δεδομένα που είχε στην κατοχή του, αφήνοντας, όμως έτσι, μια σειρά από νόμιμες εταιρείες με χαμένα στοιχεία.

Ανάμεσα στην αναταραχή των νέων επιθέσεων στον κυβερνοχώρο και τα τρωτά σημεία της πληροφορικής, είναι εύκολο για τις επιχειρήσεις να ξεχάσουν τι επιπτώσεις μπορεί να έχει η έκθεσή τους στον κυβερνοχώρο και απαιτούν ασφάλεια σε αυτόν με το πάτημα ενός κουμπιού, αλλά μερικές φορές τα πράγματα είναι πιο περίπλοκα από τα θέλουμε. Υπάρχει επίσης μια τάση για τις εταιρείες να συνδέουν την ασφάλεια στον κυβερνοχώρο απλώς με το προσωπικό του τμήματος πληροφορικής τους, αντί να υιοθετούν μια πιο σφαιρική προσέγγιση. Οι άνθρωποι είναι ο πιο αδύναμος κρίκος. Δεν είναι η τεχνολογία, δεν είναι οι διαδικασίες, δεν είναι οι κανόνες, είναι οι άνθρωποι. Κατά συνέπεια το προσωπικό πρέπει να λαμβάνει υπόψη την ασφάλεια σε τακτική βάση και όχι μόνο στον πρώτο καιρό της πρόσληψής τους.

3.4 Παραβίαση εταιρικής ασφάλειας

Η πλειοψηφία των παραβιάσεων εταιρικής ασφάλειας συμβαίνει όταν οι χάκερ εκμεταλλεύονται τους εργαζόμενους μέσω κάποιας απάτης. Με την πρόοδο

της τεχνολογίας, οι χάκερ γίνονται όλο και πιο εξειδικευμένοι στο να εντοπίζουν τρύπες και ρωγμές στα εταιρικά συστήματα ασφαλείας ώστε να αποκτήσουν πρόσβαση σε προστατευμένα αρχεία και δεδομένα, κάτι το οποίο αποτελεί μια σημαντική απειλή για την ασφάλεια στον κυβερνοχώρο.



Τρόπος επίτευξης μιας κακόβουλης ενέργειας απο χάκερ

3.5 Ελληνική αγορά

Η έκταση που παίρνουν τα τελευταία χρόνια οι κυβερνοεπιθέσεις και η προβολή που τυγχάνουν από τα μέσα μαζικής ενημέρωσης έχουν αφυπνίσει, πλέον, και πολλές ελληνικές επιχειρήσεις. Παραδοσιακά, οι κλάδοι που διέπονται από αυστηρό ρυθμιστικό ή κανονιστικό πλαίσιο (π.χ. χρηματοπιστωτικά ιδρύματα, τηλεπικοινωνίες) έχουν κάνει σημαντικές επενδύσεις για την αντιμετώπιση του κυβερνοεγκλήματος. Σιγά σιγά όμως βλέπουμε και επιχειρήσεις από άλλους κλάδους να κάνουν βήματα για να προστατευθούν.

Το πρώτο βήμα είναι να προσδιοριστούν οι κίνδυνοι στους οποίους είναι εκτεθειμένη η επιχείρηση, καθώς και τι θέλει περισσότερο να προστατέψει, και στη συνέχεια να αξιολογήσει κατά πόσο οι υφιστάμενοι μηχανισμοί ασφάλειας προστατεύουν επαρκώς από τους κινδύνους αυτούς. Αυτό διαφοροποιείται σε εύρος και πολυπλοκότητα ανάλογα με το μέγεθος, τη

δραστηριότητα και το μοντέλο λειτουργίας της εταιρείας. Σε κάθε περίπτωση, είναι πολύ σημαντικό η στρατηγική της κυβερνοασφάλειας να αποτελεί θέμα στην ατζέντα της Διοίκησης και να μην θεωρείται ως ένα θέμα της διεύθυνσης πληροφορικής. Μόνο έτσι επιτυγχάνεται η εγρήγορση όλου του οργανισμού και η ασφάλεια έναντι των κυβερνοεπιθέσεων γίνεται μέρος της εταιρικής κουλτούρας.

3.6 Αξιολόγηση μηχανισμών ασφάλειας

Ένα σημαντικό κριτήριο αξιολόγησης αποτελούν οι επιτυχημένες παραβιάσεις ασφάλειας που έχουν εντοπιστεί. Όμως, οι οργανισμοί δεν πρέπει να επαναπαύονται σε αυτό το γεγονός. Σύμφωνα με το μοντέλο ευφυούς διαχείρισης των κινδύνων του κυβερνοχώρου, η επιτυχία των παραβιάσεων ασφάλειας βασίζεται στις εξής διαστάσεις: την τεχνογνωσία, τους πόρους, τα κίνητρα και τον χρόνο που διαθέτουν οι κυβερνοεγκληματίες. Οι διαστάσεις αυτές διαφοροποιούνται σε συνεχή βάση και επηρεάζονται σε μεγάλο βαθμό από το προφίλ του οργανισμού. Επίσης, ενδέχεται η καταγραφή αυτών των περιστατικών από τον οργανισμό να μην είναι πλήρης και αντικειμενική. Οι οργανισμοί θα πρέπει να εκτελούν σε τακτά χρονικά διαστήματα δοκιμές παρείσδυσης (penetration tests). Οι δοκιμές θα πρέπει να πραγματοποιούνται από ανεξάρτητες εταιρείες του χώρου, χωρίς την γνώση των στελεχών του οργανισμού, και να προσομοιώνουν το προφίλ των επιτιθέμενων για κάθε μια διάσταση (τεχνογνωσία, πόροι, κίνητρα και χρόνο).

3.7 Κοστος της προστασίας

Το κόστος μπορεί να εκτιμηθεί σε σημαντικό βαθμό μέσω αξιολόγησης των κινδύνων (IT risk assessment). Υπάρχουν συγκεκριμένες μεθοδολογίες που χρησιμοποιούμε για να εκτιμήσουμε τον κίνδυνο και τις επιπτώσεις του. Η αξιολόγηση αυτή, αν και βασίζεται σε πρότυπα, είναι συγκεκριμένη για κάθε επιχείρηση και προϋποθέτει την ενεργή συμμετοχή των στελεχών της, και είναι το πρώτο βήμα για την αντιμετώπιση επιθέσεων. Οι επενδύσεις στην κυβερνοασφάλεια κυμαίνονται μεταξύ 3% - 5% του ετήσιου προϋπολογισμού πληροφορικής. Όπως προαναναφέρθηκε, η αξιολόγηση κινδύνων πληροφοριών και των επιχειρηματικών επιπτώσεών τους αποτελεί βέλτιστη πρακτική για τον προσδιορισμό των απαιτούμενων επενδύσεων ασφάλειας.

Σε κάθε περίπτωση, οι επενδύσεις στην κυβερνοασφάλεια θα πρέπει να αναθεωρούνται σε ετήσια βάση. Επίσης, οι επενδύσεις δεν πρέπει να

περιορίζονται στην τεχνολογική διάσταση ή στην αντιμετώπιση προβλημάτων του παρελθόντος αλλά να αναλώνονται και στην ενσωμάτωση της ασφάλειας στα πληροφοριακά συστήματα που αναπτύσσονται (security by design). Αλλά η επένδυση σε ασφαλή τεχνολογία δεν αρκεί από μόνη της. Χωρίς σωστή διακυβέρνηση, αποτελεσματικές διαδικασίες και υιοθέτηση κατάλληλης κουλτούρας και συμπεριφορών, οι τεχνολογικές λύσεις δεν θα αξίζουν τα χρήματα που δαπανήθηκαν. Ας μην ξεχνάμε ότι τα προγράμματα εφαρμόζονται, οι διαδικασίες τηρούνται, οι τεχνολογίες υλοποιούνται, λειτουργούν και συντηρούνται από τα στελέχη των οργανισμών.

3.8 Συνοψίζοντας τις ανάγκες των εταιρειών

Όπως μπορούμε να προστατευτούμε απέναντι σε πιο γνωστές και παραδοσιακές μορφές επιθέσεων (π.χ. κλοπές), έτσι μπορούμε να θωρακιστούμε και απέναντι στις κυβερνοεπιθέσεις. Η ολοκληρωμένη προστασία καλύπτει τέσσερις άξονες: πρέπει να προετοιμαστούμε, να προστατευτούμε, να ανιχνεύουμε/εντοπίζουμε και να αντιμετωπίζουμε σωστά τις επιθέσεις όταν συμβαίνουν. Η προετοιμασία αφορά στο να γνωρίζει κάθε επιχείρηση σε τι είδους επιθέσεις είναι εκτεθειμένη και τι είναι πιο σημαντικό να προστατέψει. Η προστασία περιλαμβάνει μέτρα τεχνολογικά, διαδικασίες, οργάνωση αλλά και εγρήγορση, μέσω κατάλληλης και συνεχούς ενημέρωσης του ανθρώπινου δυναμικού. Η ανίχνευση αφορά στη συνεχή παρακολούθηση και έλεγχο για ενδείξεις πιθανών επιθέσεων και στον εντοπισμό τους το συντομότερο δυνατό, ενώ είναι ακόμη σε εξέλιξη. Τέλος, η αντιμετώπιση προϋποθέτει ένα σχέδιο δράσεων που θα βοηθήσει την επιχείρηση να ελαχιστοποιήσει τις επιπτώσεις μιας κυβερνοεπίθεσης όταν συμβεί.

4. Καλύψεις

Στο παρόν κεφάλαιο θα παρουσιάσουμε αναλυτικά τις καλύψεις τις οποίες προσφέρουν στην αγορά οι ασφαλιστικές εταιρίες, καθώς επίσης και θα αναλύσουμε, παράλληλα, ειδικές λεπτομέρειες των καλύψεων αυτών. Στο δεύτερο κομμάτι του κεφαλαίου θα αναφέρουμε τις πιο κοινές καλύψεις που προσφέρονται γενικά από κάθε εταιρία, η οποία δραστηριοποιείται στον τομέα των κυβερνοεπιθέσεων. (Επισημαίνεται ότι το πρώτο κομμάτι του κεφαλαίου βασίζεται καθαρά στα συμβόλαια της AIG και LLOYDS, τα οποία λογίζονται ως τα καλύτερα στην Ελληνική αγορά).

4.1 Κατηγορίες ασφάλισης

Οι κύριες κατηγορίες στις οποίες κινείται η αγορά ασφάλισης στον κυβερνοχώρο είναι οι παρακάτω:

Α. ΕΥΘΥΝΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Β. ΔΙΟΙΚΗΤΙΚΕΣ ΥΠΟΧΡΕΩΣΕΙΣ

Γ. ΕΞΟΔΑ ΑΠΟΚΑΤΑΣΤΑΣΗΣ ΤΗΣ ΦΗΜΗΣ ΚΑΙ ΤΗΣ ΥΠΟΛΗΨΗΣ

Δ.ΕΥΘΥΝΗ ΠΟΛΥΜΕΣΩΝ

Ε.ΕΚΒΙΑΣΜΟΣ ΑΠΟΚΑΛΥΨΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΣΤ. ΔΙΑΚΟΠΗ ΛΕΙΤΟΥΡΓΙΑΣ ΔΙΚΤΥΟΥ

4.1.1 Ευθύνη προστασίας δεδομένων

Α.1 Απώλεια Προσωπικών Πληροφοριών

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης, τα οποία απορρέουν από Απαίτηση από Υποκείμενο των Προσωπικών Δεδομένων κατά του Ασφαλισμένου όσον αφορά σε πραγματική ή κατ' ισχυρισμό Καλυπτόμενη Παράβαση Προσωπικών Πληροφοριών.

Α.2 Απώλεια Εταιρικών Πληροφοριών

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης, τα οποία απορρέουν από Απαίτηση από Τρίτο Μέρος κατά του Ασφαλισμένου όσον αφορά σε

πραγματική ή κατ' ισχυρισμό Καλυπτόμενη Παράβαση Εταιρικών Πληροφοριών.

Α.3 Ανάθεση Εργασιών σε Εξωτερικούς Συνεργάτες (Outsourcing)

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης τα οποία απορρέουν από Απαίτηση από Τρίτο Μέρος κατά Εξωτερικού Συνεργάτη (εφόσον η Εταιρεία έχει συμβατική υποχρέωση αποζημίωσης) και η οποία απορρέει από πραγματική ή κατ'ισχυρισμό παράβαση καθήκοντος από τον Εξωτερικό Συνεργάτη σχετικά με την επεξεργασία Προσωπικών Πληροφοριών και/ή Εταιρικών Πληροφοριών για λογαριασμό της Εταιρείας (για την οποία υπέχει ευθύνη η Εταιρεία).

Α.4 Ασφάλεια Δικτύου

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης τα οποία απορρέουν από Απαίτηση από Τρίτο Μέρος κατά του Ασφαλισμένου η οποία έχει ως αίτιο οιαδήποτε πράξη, αβλεψία ή παράλειψη από τον Ασφαλισμένο και έχει ως αποτέλεσμα:

(i) την εισαγωγή οποιουδήποτε μη εγκεκριμένου λογισμικού, κώδικα υπολογιστή ή ιού σε Προσωπικά Δεδομένα Τρίτου Μέρους μέσα στο Σύστημα Υπολογιστών της Εταιρείας τα οποία έχουν σχεδιαστεί ειδικά για να διαταράσσουν την λειτουργία ή να φθείρουν ή να καταστρέφουν οποιοδήποτε λογισμικό ή προσωπικά δεδομένα έχει αντιγραφεί στο Σύστημα Υπολογιστών της Εταιρείας,
(ii) την αφαίρεση από εξουσιοδοτημένο Τρίτο Μέρος της δυνατότητας πρόσβασης στα Προσωπικά Δεδομένα του,
(iii) την παράνομη ιδιοποίηση κωδικού πρόσβασης σε δίκτυο από την Εταιρεία,
(iv) την καταστροφή, τροποποίηση, αλλοίωση, φθορά ή διαγραφή των Προσωπικών Δεδομένων Τρίτου Μέρους που είναι αποθηκευμένα σε οποιοδήποτε Σύστημα Υπολογιστών,
(v) τη φυσική κλοπή των Στοιχείων Ενεργητικού της Εταιρείας από Τρίτο Μέρος, ή τη φυσική απώλειά τους ή
(vi) την αποκάλυψη Προσωπικών Δεδομένων Τρίτου Μέρους από υπάλληλο της Εταιρείας.

4.1.2 Διοικητικές υποχρεώσεις

Β.1 Διοικητική Έρευνα για Προσωπικά Δεδομένα

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) για νομικές συμβουλές και εκπροσώπηση σε σχέση με οποιαδήποτε Έρευνα Εποπτικής Αρχής.

Β.2 Διοικητικά Πρόστιμα για Προσωπικά Δεδομένα

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλα τα Διοικητικά Πρόστιμα για Προσωπικά Δεδομένα (τα οποία δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) που ο Ασφαλισμένος υποχρεούται νομικά να καταβάλει ύστερα από την ολοκλήρωση Έρευνας Εποπτικής Αρχής και τα οποία προκύπτουν από παράβαση της Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων.

4.1.3 Έξοδα αποκατάστασης της φήμης και της υπόληψης

Γ.1 Προληπτικές Ερευνητικές (forensic) Υπηρεσίες

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο στον Πίνακα Ασφάλισης) ειδικών σε ερευνητικές (forensic) υπηρεσίες για τον εντοπισμό και αντιμετώπιση ηλεκτρονικών και διαδικτυακών κινδύνων για το σκοπό της τεκμηρίωσης του κατά πόσο έχει συντελεστεί ή συντελείται Καλυπτόμενη Παράβαση Ασφάλειας Προσωπικών Δεδομένων και του εντοπισμού της αιτίας της παράβασης και της υποβολής συστάσεων ως προς τον τρόπο με τον οποίο αυτή μπορεί να αποσοβηθεί ή να μετριαστεί. Τέτοιες Επαγγελματικές Αμοιβές μπορούν να αναληφθούν μόνο από την ημερομηνία γνωστοποίησης προς τον Ασφαλιστή.

Γ.2 Αποκατάσταση της Φήμης της Εταιρείας

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) ανεξάρτητων συμβούλων (συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά μεταξύ άλλων των νομικών συμβουλών σχετικά με τη στρατηγική μέσων επικοινωνίας, των συμβουλευτικών υπηρεσιών για τη διαχείριση κρίσεων και

των ανεξάρτητων υπηρεσιών δημοσίων σχέσεων) για τη διαχείριση οποιασδήποτε ενέργειας που ευλόγως απαιτείται προκειμένου να αποσοβηθούν ή να μετριαστούν οι δυνητικές συνέπειες ενός Γεγονότος Ειδησεογραφικού Ενδιαφέροντος, συμπεριλαμβανομένων του σχεδιασμού και της διαχείρισης στρατηγικής επικοινωνίας. Τέτοιες Επαγγελματικές Αμοιβές μπορούν να αναληφθούν μόνο από την ημερομηνία γνωστοποίησης προς τον Ασφαλιστή μέχρι την ημερομηνία που επέρχεται 185 ημέρες μετά από αυτή τη γνωστοποίηση.

Γ.3 Αποκατάσταση της Ατομικής Υπόληψης

Ο Ασφαλιστής θα καταβάλλει σε κάθε Μέλος του Δ.Σ. Γενικό Διευθυντή, διευθυντή κανονιστικής συμμόρφωσης, Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ή Γενικό Νομικό Σύμβουλο Εταιρείας ή για λογαριασμό αυτών όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται Πίνακα Ασφάλισης) για συμβουλευτικές υπηρεσίες και υποστήριξη από ανεξάρτητο σύμβουλο δημοσίων σχέσεων προκειμένου να μετριαστεί ή να αποφευχθεί η βλάβη για την ατομική (προσωπική και επαγγελματική) υπόληψή τους εξαιτίας πραγματικής ή κατ'ισχυρισμό Καλυπτόμενης Παράβασης Ασφάλειας Προσωπικών Δεδομένων ή παράβασης της Νομοθεσίας περί Προστασίας Προσωπικών ΔεδομένωνΤέτοιες Επαγγελματικές Αμοιβές μπορούν να αναληφθούν μόνο από την ημερομηνία γνωστοποίησης προς τον ασφαλιστή μέχρι την ημερομηνία που επέρχεται 185 ημέρες μετά από αυτή τη γνωστοποίηση.

Γ.4 Γνωστοποίηση σε Υποκείμενα των Προσωπικών Δεδομένων

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) σε σχέση με την έρευνα, ταξινόμηση πληροφοριών, προετοιμασία και υποβολή γνωστοποίησης σε Υποκείμενα των Προσωπικών Δεδομένων και/ή σε κάθε αρμόδια Ρυθμιστική Αρχή για κάθε κατ'ισχυρισμό ή πραγματική Καλυπτόμενη Παράβαση Ασφάλειας Προσωπικών Δεδομένων ή παράβαση της Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων.

Γ.5 Παρακολούθηση

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) για υπηρεσίες

παρακολούθησης για πιθανή κατάχρηση Προσωπικών Πληροφοριών κατά τη διενέργεια ή απόπειρα διενέργειας χρηματοπιστωτικών συναλλαγών, ύστερα από πραγματική ή κατ'ισχυρισμό Καλυπτόμενη Παράβαση Ασφάλειας Προσωπικών Δεδομένων ή παράβαση της Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων.

Γ.6 Ηλεκτρονικά Προσωπικά Δεδομένα

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Επαγγελματικές Αμοιβές (οι οποίες δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) προκειμένου:

(i) να διαπιστωθεί κατά πόσο Προσωπικά Δεδομένα που τηρούνται από την Εταιρεία για λογαριασμό Τρίτου Μέρους μπορούν ή δεν μπορούν να επαναφερθούν, επανασυλλεχθούν ή αναδημιουργηθούν, και

(ii) να αναδημιουργηθούν ή να επανασυλλεχθούν Προσωπικά Δεδομένα που τηρούνται από την Εταιρεία για λογαριασμό Τρίτου Μέρους σε περίπτωση που τα συστήματα δημιουργίας εφεδρικών αντιγράφων δεν επιτύχουν να διασώσουν αυτά τα Προσωπικά Δεδομένα Τρίτου Μέρους ή αυτά αλλοιωθούν ή απολεσθούν εξαιτίας τεχνικής βλάβης ή εξαιτίας αμέλειας χειριστή ή άλλου προσώπου στο οποίο έχει ανατεθεί νόμιμα αυτή η ευθύνη.

4.1.4 Ευθύνη πολυμέσων

Δ.1 Ευθύνη Πολυμέσων

Έναντι του καταβαλλόμενου επασφάλιστρου, ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης (που δεν θα υπερβαίνουν το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) που απορρέουν από Απαίτηση Τρίτου Μέρους κατά της Εταιρείας αποκλειστικά στην εκτέλεση ή αδυναμία εκτέλεσης Δραστηριοτήτων Πολυμέσων που απορρέει από τις ακόλουθες πραγματικές ή υποτιθέμενες παράνομες πράξεις:

(i) δυσφήμηση, στην οποία περιλαμβάνονται ενδεικτικά και όχι περιοριστικά τα δυσφημιστικά δημοσιεύματα, η συκοφαντία, ή μείωση της επαγγελματικής φήμης ή του χαρακτήρα οποιουδήποτε προσώπου ή οργανισμού, ή πρόκληση ψυχικής ή συναισθηματικής οδύνης που προκύπτει από τα προαναφερόμενα,

(ii) η χωρίς πρόθεση παράβαση πνευματικών δικαιωμάτων (copyright), τίτλου, συνθήματος, εμπορικού σήματος, εμπορικής επωνυμίας, επαγγελματικής αμφίεσης, διακριτικού σήματος, σήματος υπηρεσίας, ονόματος υπηρεσίας ή ονόματος χώρου (domain name), είτε μέσω deep linking είτε μέσω framing ή με οποιονδήποτε άλλον τρόπο,

(iii) λογοκλοπία, πειρατεία ή υπεξαίρεση ή κλοπή ιδεών ή πληροφοριών,

(iv) εισβολή, καταστρατήγηση παράβαση ή προσβολή δικαιωμάτων της ιδιωτικής ζωής ή της δημοσιότητας, ψευδείς ισχυρισμοί, δημοσιοποίηση προσωπικών πληροφοριών, παρείσδυση και εμπορική ιδιοποίηση ονόματος, προσωπικότητας ή ομοιότητας,

(v) αθέμιτος ανταγωνισμός, αλλά μόνο αν φέρεται ότι συντελέστηκε σε συνδυασμό με οποιαδήποτε από τις πράξεις που αναφέρονται στα σημεία (i) – (iv) ανωτέρω, ή

(vi) ευθύνη που απορρέει από αμέλεια του Ασφαλισμένου σε σχέση με οποιοδήποτε περιεχόμενο ψηφιακών μέσων.

Δ.2 Ορισμοί

Δραστηριότητες Πολυμέσων

Νοείται η δημοσίευση ή μετάδοση οποιουδήποτε περιεχομένου ψηφιακών μέσων.

Δ.3 Εξαιρέσεις

Περιγραφές Προϊόντων

Αυτή η Επέκταση Κάλυψης δεν θα καλύπτει Ζημία που οφείλεται, βασίζεται ή αποδίδεται στην πραγματική ή κατ'ισχυρισμό ανακριβή, ανεπαρκή, ή ελλιπή περιγραφή της τιμής των αγαθών, προϊόντων ή υπηρεσιών και οποιωνδήποτε εγγυήσεων κόστους, δηλώσεων κόστους, ή εκτιμήσεων κόστους, στη γνησιότητα οποιωνδήποτε αγαθών, προϊόντων ή υπηρεσιών ή στη μη συμμόρφωση οποιωνδήποτε αγαθών ή υπηρεσιών με οποιαδήποτε δηλούμενη ποιότητα ή πρότυπα απόδοσης.

Οικονομικά Στοιχεία

Αυτή η Επέκταση Κάλυψης δεν θα καλύπτει Ζημία που οφείλεται, βασίζεται ή αποδίδεται σε ανακριβή οικονομικά στοιχεία τα οποία δημοσιοποιεί η

Εταιρεία, στα οποία περιλαμβάνονται ενδεικτικά και όχι περιοριστικά η ετήσια έκθεση και οι απολογισμοί της Εταιρείας και κάθε ανακοίνωση προς το χρηματιστήριο.

4.1.5 Εκβιασμός Αποκάλυψης Προσωπικών Δεδομένων στον Κυβερνοχώρο

Ε.1 Ευθύνη για Εκβιασμό Αποκάλυψης Προσωπικών Δεδομένων στον Κυβερνοχώρο

Έναντι του καταβαλλόμενου επασφάλιστρου, ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού κάθε Απώλεια από Εκβιασμό (που δεν θα υπερβαίνει το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) που υφίσταται ένας Ασφαλισμένος αποκλειστικά ως αποτέλεσμα Απειλής Εκβιασμού.

Ε.2 Ορισμοί

Απώλεια από Εκβιασμό νοούνται τα ακόλουθα:

(i) οποιαδήποτε χρηματικά ποσά που καταβάλλονται από έναν Ασφαλισμένο με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή προκειμένου να αποφευχθεί ή να τερματιστεί Απειλή Εκβιασμού, ή

(ii) οποιεσδήποτε Επαγγελματικές Αμοιβές για ανεξάρτητους συμβούλους για να διεξαγάγουν έρευνα προκειμένου να προσδιορίσουν την αιτία Απειλής Εκβιασμού.

Απειλή Εκβιασμού

Νοείται κάθε απειλή ή συνδεδεμένη σειρά απειλών, με σκοπό την απαίτηση χρηματικών ποσών, που γνωστοποιείται στον Ασφαλισμένο προκειμένου να αποτραπεί ή να τερματιστεί μια Απειλή για την Ασφάλεια.

Απειλή για την Ασφάλεια

Νοείται κάθε απειλή για το Σύστημα Υπολογιστών που μπορεί να έχει ως αποτέλεσμα μια πραγματική ή κατ'ισχυρισμό Καλυπτόμενη Παράβαση Ασφάλειας Προσωπικών Δεδομένων που προκαλεί οικονομική βλάβη στην Εταιρεία.

Ε.3 Εξαιρέσεις

Κρατικός Φορέας ή Δημόσια Αρχή

Αυτή η Επέκταση Κάλυψης δεν θα καλύπτει οποιαδήποτε Απώλεια από Εκβιασμό που οφείλεται, βασίζεται ή αποδίδεται σε οποιαδήποτε Απειλή Εκβιασμού που προέρχεται από οποιονδήποτε κυβερνητικό φορέα ή δημόσια αρχή.

Όροι

- Ο Ασφαλισμένος θα καταβάλλει πάντοτε κάθε δυνατή προσπάθεια προκειμένου να διασφαλίσει ότι η γνώση σχετικά με την ύπαρξη της ασφάλισης για την Απώλεια από Εκβιασμό που παρέχεται από το παρόν ασφαλιστήριο θα παραμείνει εμπιστευτική. Αν η ύπαρξη ασφάλισης για Απώλεια από Εκβιασμό που παρέχεται από το παρόν ασφαλιστήριο καταστεί κοινό κτήμα ή αποκαλυφθεί σε πρόσωπο που αποτελεί Απειλή για την Ασφάλεια χωρίς υπαιτιότητα του Ασφαλιστή, ο Ασφαλιστής θα έχει το δικαίωμα να διακόψει την ασφαλιστική κάλυψη που παρέχεται από το παρόν ασφαλιστήριο για Απώλεια από Εκβιασμό με άμεση ισχύ από την ημερομηνία κατά την οποία η γνώση αυτή θα καταστεί κοινό κτήμα ή θα αποκαλυφθεί σε οποιοδήποτε πρόσωπο που αποτελεί Απειλή για την Ασφάλεια.
- Ο Ασφαλισμένος θα επιτρέπει στον Ασφαλιστή (ή στους ορισθέντες αντιπροσώπους του Ασφαλιστή) να ενημερώνουν την αστυνομία ή άλλες αρμόδιες αρχές επιβολής του νόμου για οιαδήποτε Απειλή Εκβιασμού.

4.1.6 Διακοπή Λειτουργίας Δικτύου

ΣΤ.1 Ασφάλιση Διακοπής Λειτουργίας Δικτύου

Έναντι του καταβαλλόμενου επασφάλιστρου, ο Ασφαλιστής θα καταβάλλει στην Εταιρεία κάθε Ζημία λόγω Δικτύου (που δεν θα υπερβαίνει το Επιμέρους Ανώτατο Όριο που ορίζεται στον Πίνακα Ασφάλισης) σε σχέση με Ουσιώδη Διακοπή την οποία υφίσταται Ασφαλισμένος αφού εκπνεύσει η Περίοδος Ωρών Αναμονής και αποκλειστικά ως αποτέλεσμα Αδυναμία Ασφάλειας.

ΣΤ.2 Ορισμοί

Ουσιώδης Διακοπή

Νοείται οιαδήποτε ουσιώδης διακοπή η προσωρινή παύση της εξυπηρέτησης που παρέχεται από το Σύστημα Υπολογιστών η οποία προκαλείται άμεσα από Αδυναμία Ασφάλειας.

Ζημία λόγω Απώλειας Δικτύου

Νοείται η μείωση στο καθαρό κέρδος που αποκομίζει η Εταιρεία κατά την περίοδο από την εκπνοή της Περιόδου Ωρών Αναμονής μέχρι την αποκατάσταση της υπηρεσίας (αλλά σε κάθε περίπτωση όχι μεγαλύτερο διαστημάτων 120 ημερών μετά την έναρξη της Ουσιώδους Διακοπής) που, αν δεν υφίστατο η Ουσιώδης Διακοπή, θα αποκόμιζε η Εταιρεία (και που μπορεί να αποδοθεί σε απώλεια εσόδων) πριν από την πληρωμή φόρων εισοδήματος και μετά τον συνυπολογισμό εξοικονομήσεων και εύλογου μετριασμού. Η Ζημία λόγω Απώλειας Δικτύου σε αυτό το πλαίσιο δεν περιλαμβάνει ζημίες που απορρέουν από Απαιτήσεις που εγείρονται από Τρίτα Μέρη για οποιονδήποτε λόγο εκτός από τη μείωση στα έσοδα του Ασφαλισμένου λόγω συμβατικής μείωσης στις πληρωμές για τις υπηρεσίες ή στις πιστώσεις για τη χρήση υπηρεσιών που πληρώνονται από τον Ασφαλισμένο.

Αδυναμία Ασφάλειας

Νοείται κάθε σοβαρό πρόβλημα στη λειτουργία του Συστήματος Υπολογιστών ή παρείσδυση σε αυτό, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά εκείνων που έχουν ως αποτέλεσμα ή δεν καταφέρνουν να μετριάσουν μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη χρήση, επίθεση άρνησης εξυπηρέτησης (Denial of Service) ή λήψη ή αποστολή κακόβουλου κώδικα. Η Αδυναμία Ασφάλειας περιλαμβάνει κάθε τέτοια σοβαρό λειτουργικό πρόβλημα ή παρείσδυση που προκύπτει από την κλοπή κωδικού πρόσβασης ή κωδικού πρόσβασης δικτύου από τις εγκαταστάσεις Εταιρείας, από Σύστημα Υπολογιστών, ή από στέλεχος, διευθυντή ή υπάλληλο Εταιρείας με τη χρήση μη ηλεκτρονικών μέσων κατά παράβαση συγκεκριμένων έγγραφων πολιτικών ή διαδικασιών ασφαλείας της Εταιρείας.

Περίοδος Χρόνου Αναμονής

Νοείται ο αριθμός ωρών που προβλέπονται στον όρο 7 του Πίνακα Ασφάλισης οι οποίες πρέπει να παρέλθουν αφού αρχίσει μια Ουσιώδης Διακοπή προτού καταστεί δυνατό να αρχίσει να υφίσταται Ζημία λόγω Δικτύου.

ΣΤ.3 Εξαιρέσεις

Κρατικός Φορέας ή Δημόσια Αρχή

Αυτή η Επέκταση Κάλυψης δεν θα καλύπτει οιαδήποτε Ζημία λόγω Απώλειας Δικτύου που οφείλεται, βασίζεται ή αποδίδεται σε οιαδήποτε κατάσχεση, δήμευση , ή καταστροφή ενός Συστήματος Υπολογιστών με εντολή οποιουδήποτε κρατικού φορέα ή δημόσιας αρχής.

Ειδικοί Όροι που αφορούν στην Διακοπή Λειτουργίας Εταιρικού Δικτύου

Αυτή η Επέκταση Κάλυψης δεν θα καλύπτει οποιαδήποτε Ζημία λόγω Απώλειας Εταιρικού Δικτύου που οφείλεται, βασίζεται ή αποδίδεται σε οποιοδήποτε από τα ακόλουθα:

(i) διακοπή δικτύου ή συστημάτων που προκαλείται από απώλεια επικοινωνίας με το σύστημα υπολογιστών Τρίτου Μέρους, έχοντας ως αποτέλεσμα την αδυναμία της Εταιρείας να επικοινωνεί με τα συγκεκριμένα συστήματα,
(ii) νομικά έξοδα ή νομικές δαπάνες κάθε είδους,
(iii) ενημέρωση, αναβάθμιση, βελτίωση ή αντικατάσταση οποιουδήποτε Συστήματος Υπολογιστών σε επίπεδο πέραν αυτού που υφίστατο προτού προκύψει η Ζημία λόγω Απώλειας Δικτύου,
(iv) δυσμενείς επαγγελματικές συνθήκες, ή
(v) αφαίρεση σφαλμάτων ή τρωτών σημείων λογισμικών εφαρμογών.

ΣΤ.4 Γνωστοποίηση

Εκτός της απαίτησης για παροχή γνωστοποίησης στο πλαίσιο του παρόντος ασφαλιστηρίου, και προτού ισχύσει η κάλυψη, έκαστος Ασφαλισμένος πρέπει επίσης:

(i) να συμπληρώνει και να υπογράφει γραπτό, αναλυτικό και τεκμηριωμένο αποδεικτικό ζημίας εντός ενενήντα (90) ημερών μετά την διαπίστωση οποιαδήποτε Ζημίας λόγω Απώλειας Δικτύου (εκτός αν η περίοδος αυτή παραταθεί κατά άλλον τρόπο εγγράφως από τον Ασφαλιστή) το οποίο θα αναφέρει λεπτομερώς πλήρη περιγραφή της Ζημίας λόγω Απώλειας Δικτύου και τις περιστάσεις αυτής της Ζημίας λόγω Δικτύου. Το γραπτό αποδεικτικό πρέπει επίσης να περιλαμβάνει λεπτομερή υπολογισμό κάθε Ζημίας λόγω Απώλειας Δικτύου και όλα τα υποκείμενα έγγραφα που

σχετίζονται με την Ζημία λόγω Απώλειας Δικτύου ή συνιστούν μέρος των αποδεικτικών στοιχείων για αυτήν,

(ii) μετά από αίτημα του Ασφαλιστή, να υποβάλλονται σε εξέταση, και

(iii) να παραιτούνται από το επαγγελματικό απόρρητο και να παρέχουν στον Ασφαλιστή σε συνεχή βάση οποιαδήποτε συνεργασία και συνδρομή που ο Ασφαλιστής ενδέχεται να ζητήσει, συμπεριλαμβανομένης της βοήθειας προς τον Ασφαλιστή στα ακόλουθα:

a) κάθε διερεύνηση Αστοχίας Ασφάλειας ή Ζημίας λόγω Δικτύου,

b) επιβολή οιωνδήποτε νομίμων δικαιωμάτων της Εταιρείας ή του Ασφαλιστή κατά οποιουδήποτε ο οποίος ενδέχεται να υπέχει ευθύνη έναντι Ασφαλισμένου για Αστοχία Ασφάλειας,

c) επικύρωση οποιονδήποτε εγγράφων τα οποία ο Ασφαλιστής κρίνει απαραίτητα για τη διασφάλιση των δικαιωμάτων του στο πλαίσιο του παρόντος ασφαλιστηρίου, και

d) κάθε υπολογισμό ή εκτίμηση που πραγματοποιείται από τον Ασφαλιστή ή για λογαριασμό αυτού σύμφωνα με την Επέκταση Κάλυψης για Διακοπή Λειτουργίας Δικτύου.

μετά από:

(Α) την παρουσίαση επαρκών έγγραφων αποδεικτικών στοιχείων για την Ζημία λόγω Απώλειας Δικτύου όπως προβλέπεται στα σημεία (i), (ii), και (iii) ανωτέρω από τον Ασφαλισμένο, και

(Β) την επακόλουθη έγγραφη αποδοχή αυτών από τον Ασφαλιστή, όλες οι διακανονισθείσες απαιτήσεις είναι οφειλόμενες και πληρωτέες μετά από σαράντα πέντε (45) ημέρες. Τα έξοδα και οι δαπάνες για τη στοιχειοθέτηση ή απόδειξη της ζημίας ενός Ασφαλισμένου σύμφωνα με αυτή την Επέκταση Κάλυψης για Διακοπή Λειτουργίας Δικτύου, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά εκείνων που συνδέονται με την προετοιμασία των αποδεικτικών ζημίας, θα βαρύνουν τον Ασφαλισμένο και δεν καλύπτονται στο πλαίσιο του παρόντος ασφαλιστηρίου.

ΣΤ.5 Υπολογισμοί Καθαρού Κέρδους

Κατά τον προσδιορισμό της Ζημίας λόγω Απώλειας Δικτύου για το σκοπό της διακρίβωσης του ποσού που πρέπει να καταβληθεί σύμφωνα με την παρούσα Επέκταση Κάλυψης για Διακοπή Λειτουργίας Δικτύου, θα λαμβάνονται δεόντως υπόψη η προηγούμενη εμπειρία των επιχειρηματικών

δραστηριοτήτων της Εταιρείας πριν από την έναρξη της Αδυναμίας Ασφάλειας και οι πιθανές επιχειρηματικές δραστηριότητες που ένας Ασφαλισμένος θα μπορούσε να είχε επιτελέσει αν δεν είχε συμβεί η Αδυναμία Ασφάλειας. Οι υπολογισμοί της Ζημίας λόγω Δικτύου δεν θα περιλαμβάνουν, και το παρόν ασφαλιστήριο δεν θα καλύπτει, καθαρό εισόδημα το οποίο πιθανόν θα είχε αποκτηθεί ως αποτέλεσμα αύξησης του όγκου των εργασιών λόγω ευνοϊκών επιχειρηματικών συνθηκών που προκαλούνται από τον αντίκτυπο αστοχιών ασφάλειας σε άλλες επιχειρήσεις. Οι υπολογισμοί θα γίνονται σε ωριαία βάση και θα βασίζονται στην πραγματική απώλεια καθαρού κέρδους αυτού του Ασφαλισμένου που προκαλείται από μείωση εσόδων ή αύξηση εξόδων και δαπανών που είναι δυνατό να αποδοθεί άμεσα στην Ουσιώδη Διακοπή.

ΣΤ.6 Εκτίμηση

Αν η Εταιρεία και ο Ασφαλιστής διαφωνούν ως προς την έκταση Ζημίας λόγω Απώλειας Δικτύου, οποιοσδήποτε εκ των δύο δικαιούται να υποβάλει γραπτό αίτημα για εκτίμηση αυτής της Ζημίας λόγω Απώλειας Δικτύου. Αν υποβληθεί τέτοιο αίτημα, κάθε μέρος θα επιλέξει έναν ικανό και αμερόληπτο εκτιμητή. Οι εκτιμητές στη συνέχεια θα επιλέξουν από κοινού έναν εμπειρογνώμονα ο οποίος διαθέτει προϋπηρεσία τουλάχιστον δέκα (10) ετών και ο οποίος είναι εταίρος μεγάλου διεθνούς λογιστικού γραφείου, με εμπειρία στην εκτίμηση ζημιών. Κάθε εκτιμητής θα ορίσει ξεχωριστά την έκταση της Ζημίας λόγω Απώλειας Δικτύου. Αν δεν μπορέσουν να συμφωνήσουν, θα υποβάλουν τις διαφωνίες τους στον εμπειρογνώμονα. Οποιαδήποτε απόφαση από τον εμπειρογνώμονα θα είναι οριστική και δεσμευτική.

Η Εταιρεία και ο Ασφαλιστής (i) θα αποζημιώσουν έκαστος τον δικό του επιλεγέντα εκτιμητή και (ii) θα μοιραστούν εξ ίσου τα έξοδα του εμπειρογνώμονα. Σε περίπτωση που δεν επιτευχθεί συμφωνία Αφαλιστή και Εταιρείας ως προς το πρόσωπο του Εμπειρογνώμονα, η επιλογή θα γίνεται από τον Ασφαλιστή με βάση τα παραπάνω κριτήρια.

4.2 Ορισμοί Καλύψεων

1. Στοιχείο Ενεργητικού

Νοείται κάθε μέρος ή στοιχείο υλικού, λογισμικού ή εξοπλισμού που είναι ή μπορεί να χρησιμοποιηθεί για το σκοπό της δημιουργίας, της πρόσβασης, της

επεξεργασίας, της προστασίας, της παρακολούθησης, της αποθήκευσης, της ανάκτησης, της παρουσίασης ή της μετάδοσης ηλεκτρονικών δεδομένων οποιουδήποτε τύπου (συμπεριλαμβανομένης της φωνής).

2. Νόμος περί Γνωστοποίησης Παράβασης

Νοείται οποιαδήποτε Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων η οποία επιφέρει νομική υποχρέωση για την παροχή γνωστοποίησης όσον αφορά σε πραγματική ή δυνητική παράβαση.

3. Απαίτηση

Νοείται η λήψη από τον Ασφαλισμένο ή η επίδοση σε αυτόν ενός από τα ακόλουθα:

(i) Γνωστοποίησης Εφαρμογής,
(ii) γραπτού αιτήματος που ζητά νόμιμη αποκατάσταση,
(iii) αιτήματος ή γνωστοποίησης αστικής, ρυθμιστικής, διοικητικής ή ποινικής δίωξης που ζητά νόμιμη αποκατάσταση, συμμόρφωση ή άλλο μέτρο, ή
(iv) γραπτού αιτήματος από Εποπτική Αρχή σε σχέση με Έρευνα Διοικητικής Αρχής(μόνον όσον αφορά στην Ασφαλιστική κάλυψη Β (Διοικητικές Υποχρεώσεις)).

Η έννοια του όρου Απαίτηση δεν θα περιλαμβάνει (i) οποιοδήποτε Αίτημα Πρόσβασης Υποκειμένου των Προσωπικών Δεδομένων, ή (ii) οιονδήποτε ισχυρισμό που προβάλλεται από διευθυντή, προϊστάμενο, εταίρο, διευθυντή κανονιστικής συμμόρφωσης, Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ή Γενικό Νομικό Σύμβουλο της Εταιρείας ή για λογαριασμό αυτού.

4. Εταιρεία

Νοείται ο Λήπτης της Ασφάλισης και οιαδήποτε Θυγατρική.

5. Σύστημα Υπολογιστών

Νοούνται συστήματα πληροφορικής και επικοινωνιών, δίκτυα, υπηρεσίες και λύσεις (συμπεριλαμβανομένων όλων των Στοιχείων Ενεργητικού) που είτε (α) αποτελούν μέρος αυτών των συστημάτων και δικτύων είτε (β) χρησιμοποιούνται για την παροχή αυτών των υπηρεσιών και λύσεων, τα οποία είναι μισθωμένα από την Εταιρεία ή καθίστανται διαθέσιμα για αυτήν ή

προσβάσιμα από αυτήν ή τα οποία παρέχονται στην Εταιρεία για τη δική της αποκλειστική και ασφαλή χρήση για το σκοπό των εργασιών της.

6. Εταιρικές Πληροφορίες νοούνται:

(i) οποιεσδήποτε εμπιστευτικές πληροφορίες, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά των προϋπολογισμών, καταλόγων πελατών, προγραμμάτων μάρκετινγκ και άλλων πληροφοριών, η ανακοίνωση των οποίων θα ήταν επωφελής για ανταγωνιστή και οι οποίες δεν είναι διαθέσιμες κατά άλλον τρόπο σε τέτοιους ανταγωνιστές,

(ii) οποιεσδήποτε πληροφορίες οι οποίες είναι εμπιστευτικές ή υπόκεινται σε νόμιμα δικαιώματα επαγγελματικού απορρήτου Τρίτου Μέρους, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά οιωνδήποτε εμπιστευτικών πληροφοριών που παρέχονται σε δικηγόρο, λογιστή ή άλλον επαγγελματικό σύμβουλο στο πλαίσιο των επαγγελματικών καθηκόντων του, οι οποίες διαφορετικά δεν αποτελούν κοινό κτήμα, ή

(iii) οποιεσδήποτε πληροφορίες οι οποίες αποκαλύπτονται νόμιμα στην Εταιρεία και οι οποίες λαμβάνονται νόμιμα από την Εταιρεία σε περιστάσεις που επιβάλλουν νομική υποχρέωση να τηρηθούν οι πληροφορίες εμπιστευτικές ή οι οποίες παρέχονται στην Εταιρεία σύμφωνα με γραπτή εμπιστευτική συμφωνία, και οι οποίες έχουν συλλεχθεί και τηρούνται νόμιμα από την Εταιρεία ή για λογαριασμό αυτής.

7. Αποζημιώσεις νοούνται:

(α) οποιοδήποτε ποσό που ένας Ασφαλισμένος θα έχει τη νομική υποχρέωση να καταβάλει σε Τρίτο Μέρος σε σχέση με δικαστικές αποφάσεις ή επιδικάσεις διαιτησίας που εκδίδονται κατά ενός Ασφαλισμένου,

(β) χρηματικά ποσά που πρέπει να καταβληθούν από έναν Ασφαλισμένο σε Τρίτο Μέρος σύμφωνα με Συμφωνία Διακανονισμού την οποία έχει διαπραγματευθεί η Εταιρεία και η οποία έχει εγκριθεί από τον Ασφαλιστή, σύμφωνα με πράξη ή παράλειψη εκ μέρους ενός Ασφαλισμένου.

Αποζημιώσεις δεν θα νοούνται και το παρόν ασφαλιστήριο δεν θα καλύπτει οιοδήποτε από τα ακόλουθα:

(i) παραδειγματικές ή προσυμφωνημένες αποζημιώσεις,

(ii) πάσης φύσεως πρόστιμα πέραν των ρητώς δηλωθέντων στο παρόν ασφαλιστήριο ή χρηματικές ποινές,

(iii) τα έξοδα και τις δαπάνες για συμμόρφωση με οποιαδήποτε εντολή, χορήγηση ή συμφωνία παροχής ασφαλιστικών μέτρων ή άλλης μη χρηματικής επανόρθωσης,

(iv) έξοδα ή άλλα ποσά για τα οποία ευθύνεται ο Ασφαλισμένος στη βάση Συμφωνίας Εμπορικών Υπηρεσιών,

(v) αποθετικές ζημιές ή

(vi) εκπτώσεις, ευκολίες πληρωμής για τη χρήση υπηρεσιών, επιστροφές χρημάτων, μειώσεις τιμών, κουπόνια, δώρα, βραβεία ή άλλα συμβατικά ή μη συμβατικά κίνητρα, προωθητικές ενέργειες ή άλλες μορφές παρακίνησης που προσφέρονται στους πελάτες του Ασφαλισμένου.

8. Διοικητικά Πρόστιμα για Προσωπικά Δεδομένα

Νοούνται όλα τα νόμιμα ασφαλίσιμα πρόστιμα και οι ποινές που επιδικάζονται από Εποπτική Αρχή και που πρέπει να καταβληθούν από έναν Ασφαλισμένο για παράβαση Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων. Τα Διοικητικά Πρόστιμα για Προσωπικά Δεδομένα δεν θα περιλαμβάνουν οποιονδήποτε άλλο τύπο αστικών ή ποινικών προστίμων και ποινών.

9. Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων

Έχει την έννοια του Νόμου 2472/1997 περί Προστασίας Προσωπικών Δεδομένων και οποιασδήποτε μεταγενέστερης νομοθεσίας η οποία μεταβάλλει, καταργεί ή να αντικαθιστά αυτόν τον Νόμο και κάθε άλλον αντίστοιχο νόμο και κανονισμό που σχετίζεται με τη ρύθμιση και την επιβολή της προστασίας προσωπικών δεδομένων και της ιδιωτικής ζωής στην Ελλάδα και σε οποιαδήποτε χώρα.

10. Υπεύθυνος Προστασίας Προσωπικών Δεδομένων

Έχει την έννοια υπαλλήλου ο οποίος ορίζεται από την Εταιρεία ως το πρόσωπο που έχει την ευθύνη να υλοποιεί, να παρακολουθεί, να εποπτεύει, να εκθέτει και να δημοσιοποιεί τα πρότυπα ρυθμιστικής συμμόρφωσης της Εταιρείας όσον αφορά στη συλλογή προσωπικών δεδομένων, στην επεξεργασία προσωπικών δεδομένων και στην ανάθεση επεξεργασίας προσωπικών δεδομένων.

11. Υποκείμενο των Προσωπικών Δεδομένων

Έχει την έννοια κάθε φυσικού προσώπου, του οποίου Προσωπικές Πληροφορίες έχουν συλλεχθεί ή υποβληθεί σε επεξεργασία από την Εταιρεία ή για λογαριασμό αυτής.

12. Αίτημα Πρόσβασης Υποκειμένου των Προσωπικών Δεδομένων

Έχει την έννοια γραπτού αιτήματος από Υποκείμενο των Προσωπικών Δεδομένων προς την Εταιρεία σχετικά με την υποχρεωτική εμφάνιση:

(i) τηρουμένων Προσωπικών Πληροφοριών οι οποίες προσδιορίζουν την ταυτότητα του συγκεκριμένου ατόμου,
(ii) του λόγου για τον οποίο αυτές οι Προσωπικές Πληροφορίες έχουν συλλεχθεί ή υποβληθεί σε επεξεργασία,
(iii) των αποδεκτών ή κατηγοριών αποδεκτών στους οποίους έχουν αποκαλυφθεί ή ενδέχεται να αποκαλυφθούν οι συγκεκριμένες Προσωπικές Πληροφορίες, και
(iv) της προέλευσης αυτών των Προσωπικών Πληροφοριών.

13. Έξοδα Υπεράσπισης

Έχει την έννοια εύλογων και αναγκαίων νομικών αμοιβών, δαπανών και εξόδων στα οποία υποβάλλεται ο Ασφαλισμένος, με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή, σε σχέση με την έρευνα, την απάντηση, την υπεράσπιση, την προσφυγή και/ή τον διακανονισμό Απαίτησης που εγείρεται κατά του Ασφαλισμένου. Ως Έξοδα Υπεράσπισης δεν θα νοούνται οιαδήποτε εσωτερικά έξοδα του Ασφαλισμένου(π.χ. ημερομίσθια, μισθοί ή λοιπές αμοιβές).

14. Γνωστοποίηση Εφαρμογής

Νοείται ειδοποίηση από Εποπτική Αρχή που καλεί την Εταιρεία:

(i) να πιστοποιήσει τη συμμόρφωση με την ισχύουσα Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων,
(ii) να λάβει συγκεκριμένα μέτρα προκειμένου να συμμορφωθεί με την ισχύουσα Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων,
(iii) να απόσχει από την επεξεργασία οιωνδήποτε συγκεκριμένων Προσωπικών Πληροφοριών ή Προσωπικών Δεδομένων Τρίτου Μέρους,

εντός καθορισμένης χρονικής περιόδου.

15. Αρχή Προστασίας Προσωπικών Δεδομένων

Νοείται η Αρχή Προστασίας Προσωπικών Δεδομένων ή η Αρχή που αντικαθιστά αυτόν τον ρόλο σύμφωνα με τους νόμους και τους κανονισμούς που σχετίζονται με τη ρύθμιση και την επιβολή της προστασίας δεδομένων και της ιδιωτικής ζωής και κάθε αντίστοιχη θέση σε οποιαδήποτε άλλη δικαιοδοσία.

16. Ασφαλισμένος

Νοείται:

(i) η Εταιρεία,

(ii) κάθε φυσικό πρόσωπο που είναι ή έχει διατελέσει διευθυντής προϊστάμενος, εταίρος ή ανώτερο διοικητικό στέλεχος (συμπεριλαμβανομένων μεταξύ άλλων κάθε διευθυντή κανονιστικής συμμόρφωσης, Υπεύθυνου Προστασίας Προσωπικών Δεδομένων ή Γενικού Νομικού Συμβούλου) της Εταιρείας στο μέτρο που το πρόσωπο αυτό ενεργεί με αυτή την ιδιότητα,

(iii) κάθε υπάλληλος της Εταιρείας, και κάθε κληρονόμος ή νόμιμος αντιπρόσωπος οιουδήποτε Ασφαλισμένου που περιγράφεται στα σημεία (i), (ii) και (iii) αυτού του Ορισμού στο μέτρο που εγείρεται κατά αυτών απαίτηση σε σχέση με πράξη, σφάλμα ή παράλειψη αυτού του Ασφαλισμένου. 3.17 Ασφαλιστής Aig Europe Limited.

17. Όριο Ευθύνης

Νοείται το ποσό που ορίζεται στον Πίνακα Ασφάλισης.

18. Ζημία

Έχει την έννοια:

(i) Αποζημιώσεων, Εξόδων Υπεράσπισης, Επαγγελματικών Αμοιβών, Διοικητικών Προστίμων για Προσωπικά Δεδομένα, και

(ii) Απώλειας από Εκβιασμό (εφόσον επιλεγεί) και Ζημίας λόγω Απώλειας Δικτύου(εφόσον επιλεγεί).

Η έννοια του όρου Ζημία δεν θα περιλαμβάνει οποιαδήποτε αποζημίωση, εσωτερικά ή γενικά έξοδα οποιουδήποτε Ασφαλισμένου ή το κόστος του χρόνου οποιουδήποτε Ασφαλισμένου.

19. Γεγονός Ειδησεογραφικού Ενδιαφέροντος

Νοείται η πραγματική ή επαπειλούμενη δημόσια ανακοίνωση ή γνωστοποίηση σε οποιοδήποτε μέσο ενημέρωσης η οποία απορρέει άμεσα από πραγματική ή δυνητική ή κατ'ισχυρισμό παράβαση της Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων ή Καλυπτόμενη Παράβαση Ασφάλειας Δεδομένων η οποία είναι πιθανόν να φέρει την Εταιρεία σε κατάσταση ανυποληψίας ή να αμαυρώσει τη φήμη της ή να προκαλέσει βλάβη στην αξία της μέσα στην κοινότητα ανθρώπων ή επιχειρήσεων που αποτελούν τους πελάτες ή τους προμηθευτές της ή με τους οποίους η Εταιρεία συνήθως συναλλάσσεται στο πλαίσιο των δραστηριοτήτων της.

20. Εξωτερικός Συνεργάτης

Νοείται φυσικό ή νομικό πρόσωπο το οποίο συλλέγει ή επεξεργάζεται Προσωπικές Πληροφορίες ή Εταιρικές Πληροφορίες για λογαριασμό της Εταιρείας, είτε στη βάση ρητής συμβατικής συμφωνίας είτε σύμφωνα με νομική υποχρέωση.

21. Προσωπικές Πληροφορίες

Έχει την έννοια κάθε προσωπικής πληροφορίας σχετικά με Υποκείμενο των Προσωπικών Δεδομένων που έχει συλλεχθεί και τηρείται νόμιμα από την Εταιρεία ή για λογαριασμό αυτής.

22. Επαγγελματικές Αμοιβές

Έχει την έννοια των εύλογων και αναγκαίων αμοιβών, εξόδων και δαπανών για εμπειρογνώμονες οι οποίου προσλαμβάνονται από τον Ασφαλισμένο σύμφωνα με τους όρους του παρόντος ασφαλιστηρίου και με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή.

23. Λήπτης της Ασφάλισης

Νοείται το νομικό πρόσωπο που ορίζεται στον Πίνακα Ασφάλισης.

24. Καλυπτόμενη Παράβαση Εταιρικών Πληροφοριών

Νοείται η τυχαία ή εξ αμελείας αποκάλυψη Εταιρικών Πληροφοριών από έναν Ασφαλισμένο για την οποία ευθύνεται η Εταιρεία.

25. Καλυπτόμενη Παράβαση Ασφάλειας Δεδομένων

Νοείται η μη εξουσιοδοτημένη πρόσβαση από Τρίτο Μέρος στο Σύστημα Υπολογιστών της Εταιρείας ή η χρήση πρόσβασης στο Σύστημα Υπολογιστών

της Εταιρείας εκτός του πλαισίου της αρμοδιότητας που έχει χορηγηθεί από την Εταιρεία.

26. Καλυπτόμενη Παράβαση Προσωπικών Πληροφοριών

Νοείται η μη εξουσιοδοτημένη αποκάλυψη ή μεταβίβαση από έναν Ασφαλισμένο Προσωπικών Πληροφοριών για τις οποίες είναι υπεύθυνη η Εταιρεία είτε ως εκτελών την Επεξεργασία Δεδομένων είτε ως Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων όπως ορίζεται στο πλαίσιο οιασδήποτε ισχύουσας Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων.

27. Εποπτική Αρχή

Νοείται Επίτροπος Πληροφοριών ή νόμιμος φορέας που έχει συγκροτηθεί σύμφωνα με τη Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων σε οποιαδήποτε δικαιοδοσία και που έχει την αρμοδιότητα να επιβάλλει νόμιμες υποχρεώσεις σε σχέση με την επεξεργασία και τον έλεγχο Προσωπικών Πληροφοριών (ή ανάλογα με την περίπτωση, Εταιρικών Πληροφοριών).

28. Έρευνας Εποπτικής Αρχής

Νοείται κάθε τυπική ή επίσημη ενέργεια, έρευνα, ανάκριση ή έλεγχος από Εποπτική Αρχή σε βάρος Ασφαλισμένου που απορρέει από τη χρήση ή την κατ'ισχυρισμό κατάχρηση Προσωπικών Πληροφοριών ή οποιαδήποτε πλευρά του ελέγχου ή της επεξεργασίας Προσωπικών Πληροφοριών ή την ανάθεση επεξεργασίας δεδομένων σε Εξωτερικό Συνεργάτη η οποία ρυθμίζεται από τη Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων αλλά δεν θα συμπεριλαμβάνεται οιαδήποτε έρευνα ή ενέργεια η οποία καλύπτει ολόκληρο τον συγκεκριμένο επιχειρηματικό κλάδο ή δεν αφορά σε συγκεκριμένη εταιρεία.

29. Απαλλαγή

Νοείται το ποσό που ορίζεται επακριβώς στον Πίνακα Ασφάλισης.

30. Ημερομηνία Αναδρομικής Ισχύος

Νοείται η ημερομηνία που ορίζεται επακριβώς Πίνακα Ασφάλισης.

31. Συμφωνία Διακανονισμού

Νοείται οποιαδήποτε συμφωνία την οποία συνάπτει η Εταιρεία (με την προηγούμενη γραπτή συναίνεση του Ασφαλιστή) με Τρίτο Μέρος,

προκειμένου να αντιπαρέλθει μόνιμα οποιοδήποτε δυνητικό ή πραγματικό επίδικο θέμα ή διαφωνία

32. Θυγατρική

Νοείται κάθε επιχείρηση στην οποία ο Λήπτης της Ασφάλισης είτε άμεσα είτε έμμεσα μέσω άλλων εταιρειών:

(i) διαθέτει τον έλεγχο της σύνθεσης του διοικητικού συμβουλίου,
(ii) διαθέτει τον έλεγχο για παραπάνω από το ήμισυ των δικαιωμάτων ψήφου, ή
(iii) έχει στην κατοχή του περισσότερο από το ήμισυ των μετοχών που έχουν εκδοθεί ή του μετοχικού κεφαλαίου.

Για οιαδήποτε Θυγατρική ή οιονδήποτε Ασφαλισμένο αυτής, η κάλυψη σύμφωνα με το παρόν ασφαλιστήριο θα ισχύει μόνο για παράβαση Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων ή για πράξη, σφάλμα ή παράλειψη που έχει ως αποτέλεσμα Καλυπτόμενη Παράβαση Ασφάλειας Προσωπικών Δεδομένων η οποία διαπράττεται ενόσω το συγκεκριμένο νομικό πρόσωπο είναι Θυγατρική του Λήπτη της Ασφάλισης.

33. Τρίτο Μέρος

Νοείται οιοδήποτε φυσικό ή νομικό πρόσωπο το οποίο συναλλάσσεται σύμφωνα με την αρχή των ίσων αποστάσεων με τον Ασφαλισμένο και το οποίο ούτε ελέγχει τον Ασφαλισμένο ούτε ελέγχεται από αυτόν και το οποίο δεν είναι:

(i) Ασφαλισμένος, ή
(ii) οιοδήποτε άλλο φυσικό ή νομικό πρόσωπο το οποίο έχει σημαντική οικονομική επένδυση ή εκτελεστικό ρόλο στη λειτουργία ή στη διεύθυνση της Εταιρείας,
(iii) οιοδήποτε φυσικό ή νομικό πρόσωπο το οποίο μπορεί λόγω οιουδήποτε νόμικου, ηθικού ή εμπορικού δικαιώματος ή συμφέροντος να ελέγχει ή να επηρεάζει το διοικητικό συμβούλιο ή τη διεύθυνση της Εταιρείας ή το οποίο μπορεί να επηρεάζεται ή να ελέγχεται από την Εταιρεία κατά παρόμοιο τρόπο.

34. Προσωπικά Δεδομένα Τρίτου Μέρους

Νοούνται:

(i) Εταιρικές Πληροφορίες,

(ii) κάθε προσωπική πληροφορία σχετικά με φυσικό πρόσωπο που έχει συλλεχθεί και τηρείται νόμιμα από το τρίτο μέρος ή για λογαριασμό αυτού

(iii) κάθε άλλη πληροφορία εμπορικής, επιχειρηματικής ή λειτουργικής φύσης που ανήκει στο Τρίτο Μέρος,

και η οποία τηρείται από την Εταιρεία σύμφωνα με συμβατική υποχρέωση μεταξύ της Εταιρείας και του Τρίτου Μέρους στο πλαίσιο παροχής υπηρεσιών.

4.3 Εξαιρέσεις

Όταν μιλάμε για εξαιρέσεις εννοούνται τα γεγονότα για τα οποία ο Ασφαλιστής δεν θα ευθύνεται για ζημία που οφείλεται, βασίζεται ή αποδίδεται στα ακόλουθα:

1. Παράβαση Αντιμονοπωλιακής Πολιτικής

Οποιαδήποτε πραγματική ή κατ'ισχυρισμό πράξη παράβασης αντιμονοπωλιακής πολιτικής, περιορισμού του εμπορίου ή αθέμιτου ανταγωνισμού. Η εξαίρεση αυτή δεν θα ισχύει για τη ρήτρα της κάλυψης που αφορά Ευθύνη Πολυμέσων, εφόσον αυτή επιλεγεί.

2. Σωματικές Βλάβες και Περιουσιακές Ζημιές

Οποιαδήποτε:

(i) σωματική βλάβη, ασθένεια, νόσος ή θάνατος και, αν προκύπτει από τα προαναφερθέντα, νευρικός κλονισμός, συναισθηματική οδύνη, ψυχική οδύνη ή ψυχική βλάβη, εκτός από την ψυχική οδύνη ή την ψυχική βλάβη που προκύπτει από οιαδήποτε παράβαση της Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων εκ μέρους της Εταιρείας, ή

(ii) απώλεια ή καταστροφή ενσώματων αγαθών, εκτός από Προσωπικά Δεδομένα Τρίτου Μέρους, ή απώλεια χρήσης αυτών, ή φυσική κλοπή ή απώλεια Στοιχείων Ενεργητικού της Εταιρείας.

3. Συμβατική Ευθύνη

Οποιαδήποτε εγγύηση, συμβατική ρήτρα ή υποχρέωση που αναλαμβάνεται ή γίνεται αποδεκτή από έναν Ασφαλισμένο σύμφωνα με οποιοδήποτε συμβόλαιο ή συμφωνητικό (στα οποία συμπεριλαμβάνονται μεταξύ άλλων

ενδεικτικά και όχι περιοριστικά ευκολίες πληρωμής για τη χρήση υπηρεσιών, επιστροφές χρημάτων, μειώσεις τιμών, κουπόνια, δώρα, βραβεία ή άλλα συμβατικά ή μη συμβατικά κίνητρα, προωθητικές ενέργειες ή άλλες μορφές παρακίνησης που προσφέρονται στους πελάτες του Ασφαλισμένου) εξαιρουμένου του βαθμού στον οποίο η ευθύνη αυτή θα υπήρχε για τον Ασφαλισμένο σε περίπτωση που δεν υφίστατο τέτοιο συμβόλαιο ή συμφωνητικό.

4. Εγκληματικές Πράξεις

Κάθε πράξη, σφάλμα ή παράλειψη την οποία δικαστήριο, διαιτητικό δικαστήριο ή Εποπτική Αρχή κρίνει, ή την οποία ένας Ασφαλισμένος αναγνωρίζει, ως εγκληματική, απατηλή ή δόλια πράξη. Ο Ασφαλιστής θα συνεχίσει να καταβάλλει για λογαριασμό Ασφαλισμένου Έξοδα Υπεράσπισης σύμφωνα με το παρόν ασφαλιστήριο μέχρις ότου κριθεί από δικαστήριο, διαιτητικό δικαστήριο ή Εποπτική Αρχή ότι έχει τελεστεί εγκληματική, απατηλή ή δόλια πράξη από Ασφαλισμένο. Κατόπιν τέτοιας απόφασης ο Ασφαλιστής θα δικαιούται να απαιτήσει επιστροφή όλων των ποσών που έχουν καταβληθεί στον Ασφαλισμένο.

5. Συμπεριφορά

Κάθε εσκεμμένη αδιαφορία ή μη συμμόρφωση με απόφαση, οδηγία ή περιοριστική εντολή δικαστηρίου, διαιτητικού δικαστηρίου, διαιτητή ή Εποπτικής Αρχής εντός της δικαιοδοσίας και/ή σκόπιμη διάπραξη, υποβοήθηση, υποκίνηση, παράβλεψη ενός εκ των ακολούθων ή σύμπραξη σε αυτά:

(i) απατηλή, κακόβουλη ή δόλια πράξη, ή εγκληματική παράβαση νόμου ή κανονισμού, εφόσον διαπράττεται :

(a) από διευθυντές, προϊσταμένους, εταίρους, διευθυντή κανονιστικής συμμόρφωσης, Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ή Γενικό Νομικό Σύμβουλο της Εταιρείας που είτε ενεργούν μόνοι τους ή σε συνεργασία με άλλους, ή

(b) υπαλλήλους ή Εξωτερικούς Συνεργάτες της Εταιρείας που ενεργούν σε συνεργασία με διευθυντές, προϊσταμένους, εταίρους, διευθυντή κανονιστικής συμμόρφωσης, Υπεύθυνο Προστασίας Προσωπικών Δεδομένων ή Γενικό Νομικό Σύμβουλο της Εταιρείας.

6. Κίνδυνος Προσωπικών Δεδομένων

Οποιαδήποτε προσωπικά δεδομένα τα οποία διαφέρουν ουσιωδώς ως προς την ποιότητα, ευαισθησία ή αξία από εκείνα που αποκαλύπτονται σε οποιαδήποτε πρόταση, πληροφόρηση ή δήλωση που πραγματοποιείται ή παρέχεται από τον Ασφαλιστή πριν από την ημερομηνία έναρξης.

7. Πνευματική Ιδιοκτησία

Οποιαδήποτε παράβαση διπλωμάτων ευρεσιτεχνίας και απόρρητων επαγγελματικών πληροφοριών ή απώλεια δικαιωμάτων για την εξασφάλιση καταχώρισης διπλωμάτων ευρεσιτεχνίας λόγω μη εξουσιοδοτημένης αποκάλυψης.

8. Σκόπιμες Πράξεις

Οποιαδήποτε σκόπιμη ή ηθελημένη πράξη από οποιοδήποτε φυσικό πρόσωπο που είναι ή έχει διατελέσει διευθυντής, προϊστάμενος, εταίρος ή ανώτερο διοικητικό στέλεχος (συμπεριλαμβανομένων μεταξύ άλλων ενδεικτικά και όχι περιοριστικά κάθε διευθυντή κανονιστικής συμμόρφωσης, Υπεύθυνου Προστασίας Προσωπικών Δεδομένων ή Γενικού Νομικού Συμβούλου) της Εταιρείας που ευλόγως θα αναμενόταν να δώσει αφορμή για Απαίτηση κατά ενός Ασφαλισμένου.

9. Αμοιβές για Παραχώρηση Δικαιωμάτων Εκμετάλλευσης

Οποιαδήποτε πραγματική ή κατ'ισχυρισμό υποχρέωση για την καταβολή πληρωμών για χρήση δικαιωμάτων ή για παραχώρηση δικαιωμάτων εκμετάλλευσης, συμπεριλαμβανομένων ενδεικτικά και όχι περιοριστικά του ποσού ή της έγκαιρης καταβολής αυτών των πληρωμών.

10. Προηγούμενες Απαιτήσεις και Περιστάσεις

Ο Ασφαλιστής δεν υποχρεούται σε οποιαδήποτε πληρωμή βάσει του Ασφαλιστηρίου, αναφορικά με Ζημία που αφορά σε ό,τι προκύπτει από ή σχετίζεται με:

(i) Άδικη Πράξη η οποία τελέσθηκε πριν την Ημερομηνία Αναδρομικής Ισχύος κάλυψης

(ii) Πραγματικά περιστατικά που στοιχειοθετούν ή σχετίζονται με Άδικες Πράξεις, οι οποίες αναφέρονται σε ή σχετίζονται με Απαίτηση που έχει γνωστοποιηθεί στα πλαίσια άλλου ασφαλιστηρίου, συμπεριλαμβανομένου του ασφαλιστήριου, του οποίου το Ασφαλιστήριο αποτελεί ανανέωση ή αντικατάσταση, ή

(iii) Πραγματικά περιστατικά που στοιχειοθετούν ή σχετίζονται με Άδικες Πράξεις, οι οποίες αναφέρονται σε ή σχετίζονται με γεγονότα που εύλογα μπορούν να οδηγήσουν σε Απαίτηση και έχουν γνωστοποιηθεί στα πλαίσια άλλου ασφαλιστηρίου, συμπεριλαμβανομένου του ασφαλιστήριου, του οποίου το Ασφαλιστήριο αποτελεί ανανέωση ή αντικατάσταση. ή

(iv) Εκκρεμή διαδικασία πριν από την ημερομηνία έναρξης του Ασφαλιστηρίου. Διευκρινίζεται ότι η εξαίρεση εφαρμόζεται ακόμα και αν η εκκρεμής διαδικασία ξεκίνησε μετά την Ημερομηνία Αναδρομικής Ισχύος αλλά πριν την ημερομηνία έναρξης του Ασφαλιστηρίου ή

(v) Τα ίδια πραγματικά περιστατικά με αυτά της ανωτέρω εκκρεμούς διαδικασίας. Για τους σκοπούς των εξαιρέσεων (iv) και (v), ο όρος «διαδικασία» περιλαμβάνει ενδεικτικά, και όχι περιοριστικά, κάθε αστική, ποινική, διοικητική δίκη ή διαιτησία ή άλλη συναφή διαδικασία ή επίσημη ανάκριση, εξέταση, έρευνα από ελεγκτική ή εποπτική ή άλλη αρμόδια κρατική αρχή οποιασδήποτε δικαιοδοσίας

11. Απαιτήσεις Κινητών Αξιών

Οποιαδήποτε πραγματική ή κατ'ισχυρισμό παράβαση οποιουδήποτε νόμου, κανονισμού ή κανόνα (είτε του γραπτού νόμου είτε του εθιμικού δικαίου) σχετικά με την ιδιοκτησία, αγορά, πώληση ή προσφορά, ή την αίτηση για προσφορά για αγορά ή πώληση, χρεογράφων.

12. Τρομοκρατία / Πόλεμος

Οποιαδήποτε μορφή πολέμου, τρομοκρατίας ή εξέγερσης.

13. Απώλειες Συναλλαγών

Οποιεσδήποτε απώλειες συναλλαγών ή ευθύνες συναλλαγών, χρηματική αξία οποιωνδήποτε ηλεκτρονικών μεταφορών κεφαλαίων ή συναλλαγών από τον Ασφαλισμένο ή για λογαριασμό αυτού η οποία χάνεται, ελαττώνεται ή καταστρέφεται κατά τη μεταφορά από λογαριασμό, σε λογαριασμό ή μεταξύ λογαριασμών, ή η ονομαστική αξία κουπονιών, εκπτώσεων, δώρων, βραβείων ή οποιουδήποτε άλλου σημαντικής αξίας ανταλλάγματος που παρέχεται επιπροσθέτως του συνολικού συμφωνηθέντος ή αναμενόμενου ποσού.

14. Μη Εξουσιοδοτημένες Συναλλαγές

Κάθε πραγματική ή κατ'ισχυρισμό συναλλαγή από τον Ασφαλισμένο η οποία κατά το χρόνο στον οποίο πραγματοποιείται:

(i) υπερβαίνει τα επιτρεπόμενα οικονομικά όρια, ή
(ii) βρίσκεται εκτός των επιτρεπόμενων ομάδων προϊόντων.

15. Μη εξουσιοδοτημένα ή παρανόμως συλλεχθέντα προσωπικά δεδομένα

Η παράνομη ή μη εξουσιοδοτημένη συλλογή Προσωπικών Δεδομένων Τρίτου Μέρους από την Εταιρεία.

16. Αποστολή Ανεπιθύμητου Υλικού

Κάθε διανομή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, διαφημιστικών ταχυδρομικών επιστολών (direct mail) ή τηλεομοιοτυπικών μηνυμάτων, τηλεφωνική ή ηλεκτρονική υποκλοπή, καταγραφή ήχου ή εικόνας, ή τηλεπροώθηση πωλήσεων.

17. Μη Ασφαλίσιμη Ζημία

Οποιαδήποτε ζητήματα τα οποία ενδέχεται να κριθούν μη ασφαλίσιμα σύμφωνα με τη νομοθεσία που διέπει το παρόν ασφαλιστήριο ή με τη δικαιοδοσία στην οποία υποβάλλεται μια Απαίτηση ή εκεί όπου ενεργοποιείται οποιαδήποτε Ασφαλιστική ρήτρα ή Επέκταση Κάλυψης.

4.4 Καθορισμένο Πρότυπο καλύψεων, Μετα την κρίση

Ανεξαρτήτως του ότι η Ελλάδα δραστηριοποιείται σε μικρό βαθμό στον κλάδο σε σύγκριση με τις άλλες χώρες της Ευρώπης και γενικά σε παγκόσμια κλίμακα, μετά την οικονομική κρίση οι ασφαλιστικές εταιρείες, σε συγκριτική κλίμακα, μείωσαν τις καλύψεις για να τις κάνουν πιο προσιτές στις μικρομεσαίες εταιρείες. Το πρόβλημα εδώ είναι ότι οι μεγάλες εταιρείες, πλέον, αντιμετωπίζονται από τις ασφαλιστικές εταιρείες σαν μικρομεσαίες και αυτό, τις περισσότερες φορές, παραβλέπεται από τα διοικητικά στελέχη των εταιρειών αυτών. Γνωρίζοντας, όμως, ότι η ασφάλεια παίζει σημαντικό ρόλο στη λειτουργία μιας εταιρείας είναι δυσχερές για μεγάλες εταιρείες να επιλέγονται οι παρακάτω κυβερνοκαλύψεις.

4.4.1 Ασφαλιστικές καλύψεις

Όλες οι καλύψεις δυνάμει του Άρθρου περί Ασφαλιστικών Καλύψεων του Ασφαλιστηρίου αναλαμβάνονται σε πρωτεύουσα βάση και παρέχονται αποκλειστικά για απαιτήσεις που εγείρονται για πρώτη φορά κατά του Ασφαλισμένου και για άλλα Ασφαλιστικά Γεγονότα που επέρχονται για πρώτη φορά κατά την Περίοδο Ασφάλισης και γνωστοποιούνται στον Ασφαλιστή.

4.4.1.1 Διαχείριση γεγονότων

1. Πρώτη Αντίδραση

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής τις εύλογες και αναγκαίες αμοιβές και δαπάνες:

(i) του Συμβούλου Πρώτης Αντίδρασης για την παροχή των Νομικών Υπηρεσιών·

(ii) του Ειδικού ΙΤ για την παροχή των Υπηρεσιών ΙΤ Πρώτης Αντίδρασης·

(iii) του Συμβούλου Διαχείρισης Κρίσης, εάν ο διορισμός του κρίνεται αναγκαίος από τον Σύμβουλο ΠρώτηςΑντίδρασης ή τον Ασφαλιστή, αναφορικά με πραγματική ή εικαζόμενη Παραβίαση Προσωπικών Πληροφοριών, Αστοχία Ασφάλειας ή Αστοχία Συστήματος.

2. Νομικές Υπηρεσίες

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής τις εύλογες και αναγκαίες αμοιβές και δαπάνες του Συμβούλου Πρώτης Αντίδρασης για την παροχή των Νομικών Υπηρεσιών σε σχέση με Παραβίαση Προσωπικών Πληροφοριών, Αστοχία Ασφάλειας ή Αστοχία Συστήματος. Αυτές οι Νομικές Υπηρεσίες θα περιλαμβάνουν:

(i) (i) τη λήψη οδηγιών αναφορικά με τα πραγματικά περιστατικά της Παραβίασης Προσωπικών Πληροφοριών, της Αστοχίας Ασφάλειας ή της Αστοχίας Συστήματος και τον συντονισμό του Ειδικού ΙΤ ή των Συμβούλων

(ii) Διαχείρισης Κρίσης·

(iii) (ii) την παροχή συμβουλευτικής υποστήριξης ως προς την απαίτηση γνωστοποίησης κάθε αρμόδιας Ρυθμιστικής Αρχής, την ίδια τη γνωστοποίηση και την επικοινωνία με αυτήν·

(iv) (iii) την παροχή συμβουλευτικής υποστήριξης ως προς τις γνωστοποιήσεις προς Υποκείμενα των Δεδομένων·

(v) (iv) την παρακολούθηση αιτιάσεων που υποβάλλονται από Υποκείμενα των Δεδομένων και την παροχή συμβουλευτικής υποστήριξης προς τον Ασφαλισμένο στην απάντηση ερωτημάτων που υποβάλλουν τα

(vi) Υποκείμενα των Δεδομένων·

(vii) παροχή συμβουλευτικής υποστήριξης προς την Εταιρεία σε σχέση με την αντίδρασή της σε περίπτωση Παραβίασης Προσωπικών Πληροφοριών, Αστοχίας Ασφάλειας ή Αστοχίας Συστήματος.

3. Υπηρεσίες IT

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής τις εύλογες και αναγκαίες αμοιβές και δαπάνες του Ειδικού IT σε σχέση με Αστοχία Ασφάλειας ή Αστοχία Συστήματος, για τον σκοπό:

(i) (i) της διερεύνησης Αστοχίας Ασφάλειας ή Αστοχίας Συστήματος, συμπεριλαμβανομένης της παροχής των εξής υπηρεσιών:

(a) επιβεβαίωση της επέλευσης Αστοχίας Ασφάλειας ή Αστοχίας Συστήματος, και διαπίστωση του πώς επήλθε και του εάν συνεχίζει να ισχύει και

(b) διαπίστωση εάν η Αστοχία Ασφάλειας ή η Αστοχία Συστήματος έχει οδηγήσει σε Παραβίαση Προσωπικών Πληροφοριών, ή σε Παραβίαση Εταιρικών Πληροφοριών και προσδιορισμός του βαθμού παραβίασης των Προσωπικών Πληροφοριών ή των Εταιρικών Πληροφοριών·

(ii) (ii) του περιορισμού της Αστοχίας Ασφάλειας ή της Αστοχίας Συστήματος, συμπεριλαμβανομένης της αναχαίτισης

(iii) τυχόν επίθεσης άρνησης εξυπηρέτησης (denial of service)·

(iv) (iii) της αντιμετώπισης επιθέσεων άρνησης εξυπηρέτησης και της αφαίρεσης κακόβουλου λογισμικού, υπολογιστικού κώδικα ή ιού από το Σύστημα Υπολογιστών της Εταιρείας και/ή του εντοπισμού παραβιασμένων Δεδομένων και

(v) (iv) του ελέγχου του Συστήματος Υπολογιστών της Εταιρείας για τον προσδιορισμό των ενεργειών αποκατάστασης που απαιτούνται για τη συμμόρφωση με Γνωστοποίηση Εφαρμογής.

4. Επαναφορά Δεδομένων

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής τα εύλογα και αναγκαία έξοδα και δαπάνες που αναλαμβάνει ο Ασφαλισμένος, με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή, εξαιτίας Αστοχίας Ασφάλειας ή Αστοχίας Συστήματος, προκειμένου:

(i) να διαπιστωθεί κατά πόσο είναι ή δεν είναι εφικτή η επαναφορά ή αναδημιουργία Δεδομένων που τηρούνται από την Εταιρεία για λογαριασμό Τρίτου Μέρους

(ii) να αναδημιουργηθούν Δεδομένα που τηρούνται από την Εταιρεία, συμπεριλαμβανομένων των Δεδομένων που τηρούνται για λογαριασμό Τρίτου Μέρους, όταν τα εν λόγω δεδομένα δεν είναι αναγνώσιμα από μηχανή ή έχουν αλλοιωθεί·

(iii) να εγκατασταθεί και να παραμετροποιηθεί εκ νέου το λογισμικό που η Εταιρεία χρησιμοποιούσε με άδεια χρήσης κατά τον χρόνο της Αστοχίας Ασφάλειας ή της Αστοχίας Συστήματος, όταν το εν λόγω λογισμικό δεν είναι αναγνώσιμο από Η/Υ.

5. Προστασία της Φήμης

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή σε οποιοδήποτε Ασφαλισμένο Πρόσωπο ή για λογαριασμό αυτών, τις εύλογες και αναγκαίες αμοιβές και δαπάνες για την παροχή συμβουλευτικής υποστήριξης και συνδρομής από Σύμβουλο Διαχείρισης Κρίσης και από κάθε άλλον ανεξάρτητο σύμβουλο που εγκρίνεται από τον Ασφαλιστή πριν από τον διορισμό του (συμπεριλαμβανομένων μεταξύ άλλων των νομικών συμβουλών για τη στρατηγική μέσων επικοινωνίας και των ανεξάρτητων υπηρεσιών δημοσίων σχέσεων), προκειμένου να μετριαστούν ή να αποσοβηθούν οι δυνητικές αρνητικές συνέπειες ή η προσβολή της φήμης της Εταιρείας εξαιτίας Γεγονότος Ειδησεογραφικού Ενδιαφέροντος, συμπεριλαμβανομένου του σχεδιασμού και της διαχείρισης στρατηγικής επικοινωνίας.

6. Έξοδα Γνωστοποίησης

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής τις εύλογες και αναγκαίες αμοιβές, έξοδα και δαπάνες που αναλαμβάνει ο Ασφαλισμένος, συμπεριλαμβανομένων των εξόδων για την εγκατάσταση τηλεφωνικών

κέντρων, σε σχέση με την έρευνα, την ταξινόμηση πληροφοριών, την προετοιμασία και την υποβολή γνωστοποίησης προς Υποκείμενα των Δεδομένων και/ή προς κάθε αρμόδια Ρυθμιστική Αρχή, για κάθε πραγματική ή υποτιθέμενη

Παραβίαση Προσωπικών Πληροφοριών ή Παραβίαση Εταιρικών Πληροφοριών.

7. Παρακολούθηση Πίστωσης και Ταυτότητας

Κατόπιν γνωστοποίησης προς τα Υποκείμενα των Δεδομένων, ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής:

(i) τις εύλογες και αναγκαίες αμοιβές, έξοδα και δαπάνες που αναλαμβάνει ο Ασφαλισμένος, με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή, για υπηρεσίες παρακολούθησης της κλοπής πίστωσης ή ταυτότητας για τον εντοπισμό πιθανής κατάχρησης Προσωπικών Πληροφοριών, ως αποτέλεσμα πραγματικής ή υποτιθέμενης Παραβίασης Προσωπικών Πληροφοριών και/ή

(ii) το εύλογο και αναγκαίο ασφάλιστρο για τυχόν Ασφάλιση Κλοπής Ταυτότητας.

4.4.1.2 Υποχρεώσεις Προστασίας Προσωπικών Δεδομένων

1. Έρευνα Προστασίας Δεδομένων

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο όλα τα Έξοδα Υπεράσπισης στο πλαίσιο Έρευνας Ρυθμιστικής Αρχής.

2. Πρόστιμα Προστασίας Προσωπικών Δεδομένων

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία όλα τα Πρόστιμα Προστασίας Δεδομένων που νομίμως υποχρεούται να καταβάλει η Εταιρεία στο πλαίσιο Έρευνας Ρυθμιστικής Αρχής στο βαθμό που αυτό δε συντρέχει σχετική απαγόρευση από την εφαρμοστέα νομοθεσία.

4.4.1.3 Ευθύνη

1. Προσωπικές και Εταιρικές Πληροφορίες

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης τα οποία απορρέουν

από Απαίτηση κατά του Ασφαλισμένου, όσον αφορά σε πραγματική ή υποτιθέμενη Παραβίαση Προσωπικών Πληροφοριών, ή Παραβίαση Εταιρικών Πληροφοριών από Ασφαλισμένο.

2. Αστοχία Ασφάλειας

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης τα οποία απορρέουν από Απαίτηση από Τρίτο Μέρος κατά του Ασφαλισμένου όσον αφορά σε πραγματική ή υποτιθέμενη Αστοχία Ασφάλειας.

3. Παράλειψη Γνωστοποίησης

Ο Ασφαλιστής θα καταβάλλει στον Ασφαλισμένο ή για λογαριασμό αυτού όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης τα οποία απορρέουν από Απαίτηση κατά του Ασφαλισμένου, όσον αφορά σε παράλειψη της Εταιρείας να γνωστοποιήσει σε Υποκείμενο των Δεδομένων και/ή σε Ρυθμιστική Αρχή τυχόν Παραβίαση Προσωπικών Πληροφοριών, σύμφωνα με τη Νομοθεσία περί Προστασίας Δεδομένων.

4. Κάτοχος των Πληροφοριών (Προσωπικές και Εταιρικές Πληροφορίες)

Ο Ασφαλιστής θα καταβάλλει στην Εταιρεία ή για λογαριασμό αυτής όλες τις Αποζημιώσεις και τα Έξοδα Υπεράσπισης τα οποία απορρέουν από Απαίτηση από Τρίτο Μέρος κατά της Εταιρείας, για την οποία η Εταιρεία φέρεται να υπέχει ευθύνη και η οποία απορρέει από πραγματική ή υποτιθέμενη παράβαση υποχρέωσης από τον Κάτοχο των Πληροφοριών σχετικά με την επεξεργασία Προσωπικών Πληροφοριών, και/ή Εταιρικών Πληροφοριών για λογαριασμό της Εταιρείας (για την οποία υπέχει ευθύνη η Εταιρεία).

4.4.2 Ορισμοί Καλύψεων

1. Άρθρα Πρόσθετης Κάλυψης

Κάθε στοιχείο πρόσθετης κάλυψης που συνάπτει ο Λήπτης της Ασφάλισης

2. Παραβίαση Εταιρικών Πληροφοριών

Η μη εξουσιοδοτημένη αποκάλυψη ή διαβίβαση Εταιρικών Πληροφοριών, για την οποία ευθύνεται η Εταιρεία.

3. Παραβίαση Προσωπικών Πληροφοριών

Η μη εξουσιοδοτημένη αποκάλυψη ή διαβίβαση από Ασφαλισμένο Προσωπικών Πληροφοριών για τις οποίες είναι υπεύθυνη η Εταιρεία είτε ως Φορέας Επεξεργασίας Δεδομένων είτε ως Φορέας Ελέγχου Δεδομένων, όπως ορίζεται στο πλαίσιο οιασδήποτε εφαρμοστέας Νομοθεσίας περί Προστασίας Πληροφοριών.

4. Απαίτηση

Η λήψη από τον Ασφαλισμένο ή η επίδοση σε αυτόν ενός από τα ακόλουθα:

(i) γραπτού αιτήματος που ζητά νόμιμη αποκατάσταση ή
(ii) αστικής ή διοικητικής ή ποινικής δίωξης που ζητά νόμιμη αποκατάσταση, συμμόρφωση ή άλλο μέτρο.

5. Υπηρεσία Cloud

Κάθε κατ' αίτηση πρόσβαση σε φιλοξενούμενη υποδομή υπολογιστών ή σε πλατφόρμες υπολογιστών, συμπεριλαμβανομένων των υπηρεσιών Cloud που παρέχονται βάσει του προτύπου Υποδομής ως Υπηρεσίας (IaaS) ή Πλατφόρμας ως Υπηρεσίας (PaaS), η οποία παρέχεται από οποιοδήποτε φυσικό ή νομικό πρόσωπο που δεν τελεί υπό την κυριότητα, την εκμετάλλευση ή τον έλεγχο Ασφαλισμένου. Ο όρος Cloud (Υπηρεσία Νέφους) δεν περιλαμβάνει υπηρεσίες υπολογιστικού νέφους που παρέχονται αποκλειστικά βάσει του προτύπου Λογισμικού ως Υπηρεσίας (SaaS).

6. Εταιρεία

Ο Λήπτης της Ασφάλισης και οιαδήποτε Θυγατρική.

7. Σύστημα Υπολογιστών της Εταιρείας

Στοιχεία υλικού ή λογισμικού ή οποιαδήποτε μέρη τους που συνδέονται μεταξύ τους μέσω δικτύου δύο ή περισσότερων συσκευών, που είναι προσβάσιμες μέσω διαδικτύου ή εσωτερικού δικτύου, ή που συνδέονται μέσω συσκευών αποθήκευσης δεδομένων ή μέσω άλλων περιφερειακών συσκευών, τα οποία ανήκουν, λειτουργούν, ελέγχονται ή μισθώνονται από την Εταιρεία. Για τους σκοπούς όλων των Άρθρων πλην του Άρθρου Πρόσθετης Κάλυψης για Διακοπή Λειτουργίας Δικτύου (εάν συναφθεί) και του Άρθρου Πρόσθετης Κάλυψης για Περιστατικό Ηλεκτρονικών Δεδομένων (εάν συναφθεί), ο όρος «Σύστημα Υπολογιστών της Εταιρείας» περιλαμβάνει επίσης:

(i) κάθε υπολογιστή ή ηλεκτρονική συσκευή Τρίτου Μέρους (συμπεριλαμβανομένων των κινητών τηλεφώνων, των ταμπλετών

ή των υπολογιστών που ανήκουν ή ελέγχονται από υπάλληλο της Εταιρείας), που χρησιμοποιείται για την πρόσβαση σε Σύστημα Υπολογιστών της Εταιρείας ή στα Δεδομένα που περιέχει και

(ii) κάθε Υπηρεσία Cloud που χρησιμοποιεί η Εταιρεία.

8. Ημερομηνία Αναδρομικής Ισχύος

Η ημερομηνία που ορίζεται

9. Έλεγχος

Η προστασία των εργασιών ενός νομικού προσώπου μέσω:

(i) του ελέγχου της σύνθεσης του διοικητικού συμβουλίου του εν λόγω νομικού προσώπου,

(ii) του ελέγχου περισσότερου από το ήμισυ των δικαιωμάτων ψήφου των μετόχων του εν λόγω νομικού προσώπου ή

(iii) της κατοχής περισσότερου από το ήμισυ των μετοχών που έχουν εκδοθεί ή του μετοχικού κεφαλαίου του εν λόγω νομικού προσώπου.

10. Εταιρικές Πληροφορίες

Εμπορικά μυστικά, δεδομένα, σχέδια, προβλέψεις, τύποι, πρακτικές, διαδικασίες, αρχεία, εκθέσεις, έγγραφα Τρίτου Μέρους που προστατεύονται από το δικηγορικό απόρρητο και κάθε πληροφορία που δεν είναι διαθέσιμη στο κοινό.

11. Σύμβουλος Διαχείρισης Κρίσης

Κάθε σύμβουλος που διορίζεται από τον Ασφαλιστή ή από τον Σύμβουλο Πρώτης Αντίδρασης ή οποιοσδήποτε άλλος σύμβουλος που διορίζεται από την Εταιρεία και έχει εγκριθεί από τον Ασφαλιστή πριν από τον διορισμό του, για την παροχή υπηρεσιών δημοσίων σχέσεων ή υπηρεσιών επικοινωνίας κρίσης.

12. Τρομοκρατία στον Κυβερνοχώρο

Η προμελετημένη χρήση διασπαστικών δραστηριοτήτων κατά του Συστήματος Υπολογιστών της Εταιρείας, του Συστήματος Υπολογιστών Εξωτερικού Παρόχου Υπηρεσιών ή του δικτύου του Εξωτερικού Παρόχου Υπηρεσιών, ή η ρητή απειλή για τη χρήση τέτοιων δραστηριοτήτων, με πρόθεση την πρόκληση βλάβης και την προώθηση κοινωνικών, ιδεολογικών, θρησκευτικών, πολιτικών ή συναφών σκοπών ή ο εκφοβισμός προσώπων για την προώθηση αυτών των σκοπών. Ο όρος «Τρομοκρατία στον Κυβερνοχώρο»

σε καμία περίπτωση δεν περιλαμβάνει δραστηριότητες που αποτελούν τμήμα ή υποστηρίζουν στρατιωτικές ενέργειες, πόλεμο ή πολεμικές επιχειρήσεις.

13. Αποζημιώσεις

Νοούνται οποιαδήποτε χρηματικά ποσά πρέπει να καταβληθούν από τον Ασφαλισμένο:

(i) Δυνάμει δικαστικών ή διαιτητικών αποφάσεων που εκδίδονται κατά Ασφαλισμένου·
(ii) ως ποινικές ή παραδειγματικές αποζημιώσεις, εφόσον είναι ασφαλίσιμες κατά τον νόμο ή
(iii) σύμφωνα με συμφωνία συμβιβασμού την οποία έχει διαπραγματευθεί η Εταιρεία και η οποία έχει εγκριθεί από τον Ασφαλιστή, τα οποία έχει νόμιμη υποχρέωση να καταβάλει ο Ασφαλισμένος ως αποτέλεσμα Απαίτησης.

Αποζημιώσεις δεν θα νοούνται οιοδήποτε από τα ακόλουθα:

(i) μη αντισταθμιστικές αποζημιώσεις
(ii) πρόστιμα ή χρηματικές ποινές
(iii) τα έξοδα και οι δαπάνες για συμμόρφωση με οποιαδήποτε εντολή, χορήγηση ή συμφωνία παροχής ασφαλιστικών μέτρων ή άλλης μη
(iv) χρηματικής επανόρθωσης,
(v) έξοδα ή άλλα ποσά για τα οποία ευθύνεται ο Ασφαλισμένος στη βάση Συμφωνίας Εμπορικών Υπηρεσιών, εκτός εάν για τα εν λόγω ποσά ευθύνεται και ελλείψει συμφωνίας ή
(vi) εκπτώσεις, ευκολίες πληρωμής για τη χρήση υπηρεσιών, επιστροφές χρημάτων, μειώσεις τιμών, κουπόνια, δώρα, βραβεία ή άλλα συμβατικά ή μη συμβατικά κίνητρα, προωθητικές ενέργειες ή άλλες μορφές παρακίνησης που προσφέρονται στους πελάτες του Ασφαλισμένου.

14. Δεδομένα

Ψηφιακές ή ψηφιοποιημένες πληροφορίες ή μέσα που αποθηκεύονται ηλεκτρονικά.

15. Πρόστιμα Αρχής Προστασίας Προσωπικών Δεδομένων

Όλα τα ασφαλίσιμα πρόστιμα και/ή οι ποινές που επιδικάζονται από Ρυθμιστική Αρχή και που πρέπει να καταβληθούν από Εταιρεία για παραβίαση

Νομοθεσίας περί Προστασίας Προσωπικών Δεδομένων. Τα Πρόστιμα Προστασίας Προσωπικών Δεδομένων δεν θα περιλαμβάνουν κανέναν άλλο τύπο αστικών ή ποινικών προστίμων και ποινών.

16. Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων

Ο νόμος 2472/1997 (Νόμος περί προστασίας προσωπικών δεδομένων) και οιαδήποτε μεταγενέστερη νομοθεσία η οποία μεταβάλλει, καταργεί ή αντικαθιστά αυτόν τον νόμο και κάθε άλλον αντίστοιχο νόμο και κανονισμό που σχετίζεται με τη ρύθμιση και την επιβολή της προστασίας προσωπικών δεδομένων και του προσωπικού απόρρητου σε οποιαδήποτε χώρα.

17. Υπεύθυνος Προστασίας Προσωπικών Δεδομένων

Υπάλληλος ο οποίος ορίζεται από την Εταιρεία ως το πρόσωπο που έχει την ευθύνη να υλοποιεί, να παρακολουθεί, να εποπτεύει, να εκθέτει και να δημοσιοποιεί τα πρότυπα ρυθμιστικής συμμόρφωσης της Εταιρείας όσον αφορά στη συλλογή, στην επεξεργασία και στην ανάθεση επεξεργασίας προσωπικών δεδομένων.

18. Υποκείμενο των Δεδομένων

Κάθε φυσικό πρόσωπο, προσωπικές πληροφορίες του οποίου έχουν συλλεχθεί ή υποβληθεί σε επεξεργασία από την Εταιρεία ή για λογαριασμό αυτής.

19. Έξοδα Υπεράσπισης

Οι εύλογες και αναγκαίες νομικές αμοιβές, δαπάνες και έξοδα στα οποία υποβάλλεται ο Ασφαλισμένος, με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή, σε σχέση με την έρευνα, την απάντηση, την υπεράσπιση, την προσφυγή και/ή τον διακανονισμό για Απαίτηση ή Έρευνα Ρυθμιστικής Αρχής που εγείρεται ή πραγματοποιείται κατά του Ασφαλισμένου. Στα Έξοδα Υπεράσπισης δεν συμπεριλαμβάνονται οι αμοιβές προς Ασφαλισμένο, Εξωτερικό Πάροχο Υπηρεσιών ή Κάτοχο των Πληροφοριών, το κόστος του χρόνου απασχόλησής τους ή άλλες δαπάνες ή γενικά έξοδα του Ασφαλισμένου, του Εξωτερικού Παρόχου Υπηρεσιών ή του Κατόχου των Πληροφοριών.

20. Αριθμός Έκτακτης Ανάγκης

Ο τηλεφωνικός αριθμός που ορίζεται

21. Γνωστοποίηση Εφαρμογής

Η ειδοποίηση από Ρυθμιστική Αρχή που καλεί την Εταιρεία:

(i) να πιστοποιήσει τη συμμόρφωση με την ισχύουσα Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων,

(ii) να λάβει συγκεκριμένα μέτρα προκειμένου να συμμορφωθεί με την ισχύουσα Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων,

(iii) να απέχει από την επεξεργασία οιωνδήποτε συγκεκριμένων Προσωπικών Πληροφοριών ή Δεδομένων που κατέχει για λογαριασμό Τρίτου Μέρους, εντός συγκεκριμένης προθεσμίας, αλλά το αργότερο εντός πέντε (5) ετών από την ημερομηνία της γνωστοποίησης.

22. Υπηρεσίες IT Πρώτης Αντίδρασης

(i) επιβεβαίωση της επέλευσης Αστοχίας Ασφάλειας ή Αστοχίας Συστήματος, και διαπίστωση του πώς επήλθε και του εάν συνεχίζει να ισχύει.

(ii) διαπίστωση εάν η Αστοχία Ασφάλειας ή η Αστοχία Συστήματος έχει οδηγήσει σε Παραβίαση Προσωπικών Δεδομένων ή σε Παραβίαση Εταιρικών Πληροφοριών και προσδιορισμός του βαθμού παραβίασης των Προσωπικών Πληροφοριών ή των Εταιρικών Πληροφοριών ή

(iii) του περιορισμού της Αστοχίας Ασφάλειας ή της Αστοχίας Συστήματος, συμπεριλαμβανομένης της αναχαίτισης τυχόν επίθεσης άρνησης εξυπηρέτησης (denial of service).

23. Ασφάλιση Κλοπής Ταυτότητας

Ασφαλιστήριο κλοπής ταυτότητας που εκδίδεται από τον Ασφαλιστή ή από άλλον φορέα, με την προηγούμενη έγγραφη συναίνεση του Ασφαλιστή, και προσφέρεται στα Υποκείμενα των Δεδομένων, των οποίων οι Προσωπικές Πληροφορίες έχουν παραβιαστεί.

24. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα που λειτουργεί στην Ελλάδα ως ανεξάρτητη Αρχή.

25. Κάτοχος των Πληροφοριών

Τρίτο μέρος

(i) προς το οποίο Εταιρεία έχει παράσχει Εταιρικές Πληροφορίες ή Προσωπικές Πληροφορίες ή

(ii) που έχει λάβει Εταιρικές Πληροφορίες ή Προσωπικές Πληροφορίες για λογαριασμό της Εταιρείας, συμπεριλαμβανομένου του Εξωτερικού Παρόχου Υπηρεσιών.

26. Ασφαλισμένος

(i) η Εταιρεία·

(ii) οποιοδήποτε Ασφαλισμένο Πρόσωπο·

(iii) οποιοδήποτε φυσικό πρόσωπο που είναι ή έχει διατελέσει υπάλληλος της Εταιρείας·

(iv) ανεξάρτητος εργολάβος υπό τις οδηγίες και την εποπτεία του Λήπτη της Ασφάλισης, μόνο σε σχέση με τις υπηρεσίες που ο ανεξάρτητος εργολάβος παρέχει στον Λήπτη της Ασφάλισης και

(v) κάθε κληρονόμος ή νόμιμος αντιπρόσωπος οποιουδήποτε Ασφαλισμένου που περιγράφεται στα σημεία (i), (ii) και (iii) αυτού του ορισμού στο μέτρο που εγείρεται κατά αυτών Απαίτηση σε σχέση με πράξη, σφάλμα ή παράλειψη αυτού του Ασφαλισμένου.

27. Ασφαλισμένο Πρόσωπο

Κάθε φυσικό πρόσωπο που είναι ή έχει διατελέσει διευθυντής, προϊστάμενος, εταίρος ή ανώτερο διοικητικό στέλεχος (συμπεριλαμβανομένου του Αρμόδιου Στελέχους) της Εταιρείας, στο μέτρο που το πρόσωπο αυτό ενεργεί με αυτή την ιδιότητα.

28. Ασφαλιστής

Η ασφαλιστική εταιρεία

29. Ειδικοί ΙΤ

Η εταιρεία που αναφέρεται στο Πίνακα Ασφάλισης ή οποιαδήποτε άλλη εταιρεία που διορίζεται από την Εταιρεία και έχει εγκριθεί από τον Ασφαλιστή πριν από τον διορισμό της.

30. Νομικές Υπηρεσίες

(i) νομική συμβουλή και υποστήριξη που παρέχεται δυνάμει Συναφούς Συμφωνίας·

(ii) ο συντονισμός του Ειδικού ΙΤ και, εάν ο Σύμβουλος Πρώτης Αντίδρασης το κρίνει αναγκαίο, του Συμβούλου Διαχείρισης Κρίσης.

31. Όριο Ευθύνης

Το ποσό που ορίζεται στο Πίνακα Ασφάλισης.

32. Ζημία

(i) Αποζημιώσεις, Έξοδα Υπεράσπισης, Πρόστιμα Προστασίας Προσωπικών Δεδομένων που έχει νόμιμη υποχρέωση να καταβάλει ο Ασφαλισμένος και

(ii) Κάθε άλλο ποσό που καλύπτεται από τις Ασφαλιστικές Καλύψεις ή από τις Ενότητες Πρόσθετων Καλύψεων, αλλά μόνο στον βαθμό που ορίζεται στην εκάστοτε Ενότητα.

Στη Ζημία δεν συμπεριλαμβάνονται οι αμοιβές προς Ασφαλισμένο, Εξωτερικό Πάροχο Υπηρεσιών ή Κάτοχο των Πληροφοριών, το κόστος του χρόνου απασχόλησής τους ή άλλες δαπάνες ή γενικά έξοδα του Ασφαλισμένου, του Εξωτερικού Παρόχου Υπηρεσιών ή του Κατόχου των Πληροφοριών.

33. Γεγονότα Ειδησεογραφικού Ενδιαφέροντος

Η πραγματική ή επαπειλούμενη δημόσια ανακοίνωση ή γνωστοποίηση σε οποιοδήποτε μέσο ενημέρωσης, η οποία απορρέει άμεσα από πραγματική ή δυνητική ή υποτιθέμενη Παραβίαση Προσωπικών Πληροφοριών ή Παραβίαση Εταιρικών πληροφοριών, Αστοχία Ασφάλειας, Αστοχία Συστήματος ή Αστοχία Ασφάλειας Παρόχου Υπηρεσιών (εάν έχει συναφθεί το Άρθρο Πρόσθετης Κάλυψης του Εξωτερικού Παρόχου Υπηρεσιών) ή από Απειλή Εκβιασμού (εάν έχει συναφθεί το Άρθρο Πρόσθετης Κάλυψης για Εκβιασμό Αποκάλυψης Προσωπικών Δεδομένων στον Κυβερνοχώρο) ή από Περιστατικό Ηλεκτρονικών Δεδομένων (εάν έχει συναφθεί το Άρθρο Πρόσθετης Κάλυψης για Περιστατικό Ηλεκτρονικών Δεδομένων), η οποία είναι πιθανόν να φέρει την Εταιρεία ή οποιοδήποτε Ασφαλισμένο Πρόσωπο σε κατάσταση ανυποληψίας ή να αμαυρώσει τη φήμη της ή να προκαλέσει βλάβη στην αξία της μέσα στην κοινότητα ανθρώπων ή επιχειρήσεων που αποτελούν τους πελάτες ή τους προμηθευτές της ή με τους οποίους η Εταιρεία συνήθως συναλλάσσεται στο πλαίσιο των δραστηριοτήτων της.

34. Εξωτερικός Πάροχος Υπηρεσιών

Νομικό πρόσωπο που δεν τελεί υπό την κυριότητα, την εκμετάλλευση ή τον έλεγχο της Εταιρείας, το οποίο η Εταιρεία έχει διορίσει για την παροχή συγκεκριμένων υπηρεσιών (συμπεριλαμβανομένης της φιλοξενίας ιστοσελίδων, της επεξεργασίας πληρωμών και της συλλογής, επεξεργασίας, ανάθεσης της επεξεργασίας, αποθήκευσης και/ή διαγραφής ή καταστροφής δεδομένων ασφάλειας ΤΠ), οι οποίες διαφορετικά θα παρέχονταν εσωτερικά ή

βάσει ρητής συμβατικής συμφωνίας, αλλά μόνο στο βαθμό της παροχής των εν λόγω υπηρεσιών.

35. Προσωπικές Πληροφορίες

Κάθε πληροφορία που αφορά φυσικό πρόσωπο, από την οποία είναι δυνατή η ατομική ταυτοποίηση του φυσικού προσώπου. Οι Προσωπικές Πληροφορίες περιλαμβάνουν ενδεικτικά αλλά όχι περιοριστικά το ονοματεπώνυμο, τη διεύθυνση, τον τηλεφωνικό αριθμό και τα ιατρικά στοιχεία του φυσικού προσώπου.

36. Λήπτης της Ασφάλισης

Το νομικό πρόσωπο που ορίζεται στο Πίνακα Ασφάλισης.

37. Περίοδος Ασφάλισης

Η περίοδος από την ημερομηνία έναρξης έως την ημερομηνία λήξης .

38. Ρυθμιστική Αρχή

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή νόμιμος φορέας που έχει συγκροτηθεί σύμφωνα με τη Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων ή άλλη αρμόδια εποπτική αρχή σε οποιαδήποτε δικαιοδοσία που έχει την αρμοδιότητα να επιβάλλει νόμιμες υποχρεώσεις σε σχέση με την επεξεργασία και τον έλεγχο Προσωπικών Δεδομένων (ή ανάλογα με την περίπτωση, Εταιρικών Πληροφοριών).

39. Έρευνα Ρυθμιστικής Αρχής

Κάθε τυπική ή επίσημη ενέργεια, έρευνα, ανάκριση ή έλεγχος από Ρυθμιστική Αρχή σε βάρος Ασφαλισμένου, εφόσον η Ρυθμιστική Αρχή έχει προσδιορίσει εγγράφως τον Ασφαλισμένο, για χρήση ή υποτιθέμενη κατάχρηση.Προσωπικών Πληροφοριών ή οποιαδήποτε πλευρά του ελέγχου ή της επεξεργασίας Προσωπικών Πληροφοριών ή την ανάθεση επεξεργασίας δεδομένων σε Εξωτερικό Πάροχο Υπηρεσιών, η οποία ρυθμίζεται από τη Νομοθεσία περί Προστασίας Προσωπικών Δεδομένων, αλλά δεν θα συμπεριλαμβάνεται οποιαδήποτε έρευνα ή ενέργεια η οποία καλύπτει ολόκληρο τον συγκεκριμένο επιχειρηματικό κλάδο ή δεν αφορά σε συγκεκριμένη εταιρεία.

40. Συναφής Συμφωνία

Συμφωνία μεταξύ του Συμβούλου Πρώτης Αντίδρασης και της Εταιρείας, η οποία διέπει την παροχή της νομικής συμβουλής και υποστήριξης προς την Εταιρεία.

41. Σύμβουλος Πρώτης Αντίδρασης

Οι ανταποκρίτριες νομικές εταιρείες που λαμβάνουν εντολές από την εν λόγω νομική εταιρεία ή τυχόν αντικαταστάτρια εταιρεία που διορίζεται από τον Ασφαλιστή σε περίπτωση σύγκρουσης, με την οποία ο Λήπτης της Ασφάλισης θα συνάψει Συναφή Συμφωνία.

42. Αρμόδιο Στέλεχος

Κάθε Διευθύνων Σύμβουλος, Οικονομικός Διευθυντής, Διευθυντής Συμμόρφωσης, Διευθυντής Πληροφοριών, Υπεύθυνος Προστασίας Δεδομένων, Διευθυντής Διαχείρισης Κινδύνων ή Γενικός Νομικός Σύμβουλος (ή ισοδύναμες θέσεις).

43. Απαλλαγή

Τα ποσά που ορίζονται στο Πίνακα Ασφάλισης.

44. Αστοχία Ασφάλειας

(i) οποιαδήποτε παρείσδυση που οφείλεται σε αστοχία της ασφάλειας του Συστήματος Υπολογιστών της Εταιρείας, συμπεριλαμβανομένων εκείνων που έχουν ως αποτέλεσμα ή αποτυγχάνουν να μετριάσουν μη εξουσιοδοτημένη πρόσβαση, μη εξουσιοδοτημένη χρήση, επίθεση άρνησης εξυπηρέτησης (denial of service), άρνηση εξυπηρέτησης ή λήψη ή αποστολή κακόβουλου κώδικα, κακόβουλου λογισμικού η ιού, που προκαλεί καταστροφή, τροποποίηση, αλλοίωση, φθορά ή διαγραφή των Δεδομένων Τρίτου Μέρους που είναι αποθηκευμένα σε οποιοδήποτε Σύστημα Υπολογιστών της Εταιρείας·

(ii) η αποκάλυψη Δεδομένων:
(a) εξαιτίας υλικής κλοπής ή απώλειας υλικού που ελέγχεται από την Εταιρεία (ή στοιχείων του) ή
(b) από υπάλληλο της Εταιρείας.

(iii) η Αστοχία Ασφάλειας περιλαμβάνει επίσης κάθε τέτοια αστοχία ή παρείσδυση που προκύπτει από την κλοπή κωδικού πρόσβασης ή κωδικού πρόσβασης δικτύου από:
(a) εγκαταστάσεις της Εταιρείας.

(b) Σύστημα Υπολογιστών της Εταιρείας.
(c) στέλεχος, διευθυντή ή υπάλληλο Εταιρείας.

45. Αστοχία Συστήματος

Οποιαδήποτε εξ αμελείας πράξη ή παράλειψη υπαλλήλου της Εταιρείας, κατά τη λειτουργία, τη συντήρηση ή την αναβάθμιση του Συστήματος Υπολογιστών της Εταιρείας. Η Αστοχία Συστήματος δεν περιλαμβάνει εξ αμελείας πράξεις ή παραλείψεις υπαλλήλου της Εταιρείας, κατά τη λειτουργία, τη συντήρηση ή την αναβάθμιση Υπηρεσίας Cloud που χρησιμοποιείται από υπολογιστή ή ηλεκτρονική συσκευή της Εταιρείας ή Τρίτου Μέρους (συμπεριλαμβανομένων των κινητών τηλεφώνων, των ταμπλετών ή των υπολογιστών που ανήκουν ή ελέγχονται από υπάλληλο Εταιρείας) για την πρόσβαση σε Σύστημα Υπολογιστών της Εταιρείας ή στα Δεδομένα που περιέχει.

46. Ενιαία Απαίτηση

Μία ή περισσότερες Απαιτήσεις ή Ασφαλιστικά Γεγονότα, στον βαθμό που απορρέουν, βασίζονται, συνδέονται ή άλλως αποδίδονται στην ίδια αιτία ή πηγή και όλες αυτές οι Απαιτήσεις ή τα Ασφαλιστικά Γεγονότα θα θεωρούνται μία Ενιαία Απαίτηση, ανεξαρτήτως εάν αφορούν τους ίδιους ή διαφορετικούς ενάγοντες, Ασφαλισμένους ή αγωγές.

47. Θυγατρική

Κάθε επιχείρηση στην οποία ο Λήπτης της Ασφάλισης, είτε άμεσα είτε έμμεσα μέσω μίας ή περισσότερων άλλων Θυγατρικών του, έχει ή είχε τον Έλεγχο πριν από την ημερομηνία έναρξης του παρόντος Ασφαλιστηρίου. Ο όρος «Θυγατρική» περιλαμβάνει επίσης κάθε επιχείρηση της οποίας ο Λήπτης της Ασφάλισης αποκτά τον Έλεγχο, άμεσα ή έμμεσα μέσω μίας ή περισσότερων άλλων Θυγατρικών του κατά την Περίοδο Ασφάλισης, υπό τον όρο ότι η εν λόγω επιχείρηση:

(i) έχει συνολικά ακαθάριστα έσοδα που είναι λιγότερα από το 20% του συνόλου των ακαθάριστων εσόδων του Λήπτη της Ασφάλισης και
(ii) δεν έχει έσοδα από τις Ηνωμένες Πολιτείες της Αμερικής.

48. Τρίτο Μέρος

Κάθε νομικό ή φυσικό πρόσωπο, εκτός από:

(i) Ασφαλισμένο, Εξωτερικό Πάροχο Υπηρεσιών ή Κάτοχο των Πληροφοριών ή

(ii) οποιοδήποτε άλλο νομικό ή φυσικό πρόσωπο που έχει οικονομικό συμφέρον ή εκτελεστικό ρόλο στη λειτουργία της Εταιρείας.

49. Σύστημα Υπολογιστών Τρίτου Μέρους

Στοιχεία υλικού ή λογισμικού ή οποιαδήποτε μέρη τους που συνδέονται μεταξύ τους μέσω δικτύου δύο ή περισσότερων συσκευών, που είναι προσβάσιμες μέσω διαδικτύου ή εσωτερικού δικτύου, ή που συνδέονται μέσω συσκευών αποθήκευσης δεδομένων ή μέσω άλλων περιφερειακών συσκευών, τα οποία ανήκουν, λειτουργούν, ελέγχονται ή μισθώνονται από την Εταιρεία.

4.4.3 Εξαιρέσεις

Οι ασφαλιστικές εταιρείες δεν θα ευθύνονται για Ζημία που οφείλεται, βασίζεται ή αποδίδεται στα ακόλουθα:

1. Αντιμονοπωλιακή πολιτική

Οποιαδήποτε πραγματική ή υποτιθέμενη πράξη παραβίασης αντιμονοπωλιακής πολιτικής, περιορισμού του εμπορίου ή αθέμιτου ανταγωνισμού. Η παρούσα Εξαίρεση 1 – Αντιμονοπωλιακή πολιτική δεν ισχύει για Ζημία που οφείλεται, βασίζεται ή αποδίδεται σε πραγματικό ή υποτιθέμενο αθέμιτο ανταγωνισμό.

2. Σωματικές Βλάβες και Υλικές Ζημίες

Οποιαδήποτε:

(i) σωματική βλάβη, ασθένεια, νόσος ή θάνατος και, εάν προκύπτει από τα προαναφερθέντα, νευρικός κλονισμός, συναισθηματική οδύνη, ψυχική οδύνη ή

(ii) απώλεια ή καταστροφή ενσώματων αγαθών, εκτός από Δεδομένα.

3. Συμβατική Ευθύνη

Οποιαδήποτε εγγύηση, συμβατική ρήτρα ή υποχρέωση που αναλαμβάνεται ή γίνεται αποδεκτή από έναν Ασφαλισμένο σύμφωνα με οιοδήποτε συμβόλαιο ή συμφωνητικό εξαιρουμένου του βαθμού στον οποίο η ευθύνη αυτή θα υπήρχε για τον Ασφαλισμένο σε περίπτωση που δεν υφίστατο τέτοιο συμβόλαιο ή συμφωνητικό.

4. Συμπεριφορά

(i) κάθε εσκεμμένη αδιαφορία ή μη συμμόρφωση με απόφαση, οδηγία ή περιοριστική εντολή δικαστηρίου, διαιτητικού δικαστηρίου, διαιτητή ή Ρυθμιστικής Αρχής εντός της δικαιοδοσίας·

(ii) κάθε σκόπιμη, εκ προθέσεως ή εξ αμελείας διάπραξη, υποβοήθηση, υποκίνηση, παράβλεψη ή σύμπραξη σε εγκληματική, απατηλή ή δόλια πράξη ή εγκληματική παραβίαση νόμου ή κανονισμού ή

(iii) οποιαδήποτε σκόπιμη, εκ προθέσεως ή εξ αμελείας πράξη Ασφαλισμένου· εφόσον διαπράττεται:

(α) από διευθυντές, προϊσταμένους, εταίρους ή το Αρμόδιο Στέλεχος της Εταιρείας ή του Εξωτερικού Παρόχου Υπηρεσιών ή του Κατόχου των Πληροφοριών, που ενεργούν μόνοι τους ή σε συνεργασία με άλλους, ή

(β) από υπαλλήλους που ενεργούν σε συνεργασία με οποιουσδήποτε διευθυντές, προϊσταμένους, εταίρους ή το Αρμόδιο Στέλεχος της Εταιρείας ή του Εξωτερικού Παρόχου Υπηρεσιών ή του Κατόχου των Πληροφοριών.

Ο Ασφαλιστής θα συνεχίσει να καταβάλλει για λογαριασμό Ασφαλισμένου τα Έξοδα Υπεράσπισης σύμφωνα με το παρόν Ασφαλιστήριο μέχρις ότου κριθεί από δικαστήριο, διαιτητικό δικαστήριο ή Ρυθμιστική Αρχή ότι Ασφαλισμένος έχει διαπράξει οποιαδήποτε από τις πράξεις των σημείων (i) έως (iii) ανωτέρω. Κατόπιν τέτοιας απόφασης ο Ασφαλιστής θα δικαιούται να απαιτήσει επιστροφή όλων των ποσών που έχουν καταβληθεί στον Ασφαλισμένο.

5. Πνευματική Ιδιοκτησία

Οποιαδήποτε παραβίαση διπλωμάτων ευρεσιτεχνίας και απόρρητων επαγγελματικών πληροφοριών ή απώλεια δικαιωμάτων για την εξασφάλιση καταχώρισης διπλωμάτων ευρεσιτεχνίας λόγω μη εξουσιοδοτημένης αποκάλυψης. Η παρούσα Εξαίρεση 5 – Πνευματική Ιδιοκτησία δεν ισχύει για Ζημίες ή Έξοδα Υπεράσπισης που απορρέουν από Απαίτηση Τρίτου Μέρους κατά Ασφαλισμένου για Παραβίαση Εταιρικών Πληροφοριών.

6. Αμοιβή για Παραχώρηση Δικαιωμάτων Εκμετάλλευσης

Οποιαδήποτε πραγματική ή υποτιθέμενη υποχρέωση για την καταβολή πληρωμών για χρήση δικαιωμάτων ή για παραχώρηση δικαιωμάτων εκμετάλλευσης, συμπεριλαμβανομένου του ποσού ή του εμπρόθεσμου αυτών των πληρωμών.

7. Προηγούμενες Απαιτήσεις και Περιστάσεις

(i) κάθε περίσταση η οποία, από την ημερομηνία έναρξης του παρόντος Ασφαλιστηρίου, μπορεί ευλόγως να θεωρείται από οποιονδήποτε Ασφαλισμένο ότι μπορεί να δώσει αφορμή για Απαίτηση· ή οποιαδήποτε περίσταση, Απαίτηση ή Ασφαλιστικό Γεγονός που γνωστοποιείται δυνάμει ασφαλιστηρίου, το οποίο το παρόν Ασφαλιστήριο ανανεώνει, αντικαθιστά ή διαδέχεται ή

(ii) κάθε εκκρεμούσα ή προηγούμενη αστική, ποινική, διοικητική ή κανονιστική διαδικασία, έρευνα, διαιτησία, διαμεσολάβηση, άλλη διαδικασία επίλυσης διαφορών ή επιδίκαση για την οποία ο Ασφαλισμένος είχε λάβει γνώση κατά την Ημερομηνία Αναδρομικής Ισχύος, ή η οποία προβάλλει ή απορρέει από τα ίδια ή ουσιωδώς τα ίδια πραγματικά περιστατικά που προβάλλονται στις εν λόγω αγωγές ή

(iii) κάθε Απαίτηση ή Ασφαλιστικό Γεγονός που ειδάλλως θα αποτελούσε Ενιαία Απαίτηση με οποιαδήποτε απαίτηση ή άλλο ζήτημα που γνωστοποιείται.

8. Απαιτήσεις Κινητών Αξιών

Οποιαδήποτε πραγματική ή υποτιθέμενη παραβίαση οποιουδήποτε νόμου, κανονισμού ή κανόνα (είτε του γραπτού νόμου είτε του εθιμικού δικαίου) σχετικά με την ιδιοκτησία, αγορά, πώληση ή προσφορά, ή την αίτηση για προσφορά για αγορά ή πώληση, χρεογράφων.

9. Τρομοκρατία / Πόλεμος

Κάθε μορφής:

(i) πόλεμος, εισβολή, εχθρική ενέργεια ξένου κράτους, εχθροπραξία ή πολεμική επιχείρηση (ανεξαρτήτως εάν έχει κηρυχθεί πόλεμος ή όχι), εμφύλιος πόλεμος, στρατιωτική εξέγερση, στάση ή επανάσταση·

(ii) τρομοκρατία (εξαιρουμένης της Τρομοκρατίας στον Κυβερνοχώρο) ή

(iii) εξέγερση.

10. Χρηματική Αξία

Οποιεσδήποτε απώλειες κατά τη διενέργεια των συναλλαγών ή ευθύνες που προκύπτουν από διενεργηθείσες συναλλαγές· χρηματική αξία οποιωνδήποτε ηλεκτρονικών μεταφορών κεφαλαίων ή συναλλαγών από τον Ασφαλισμένο ή

για λογαριασμό αυτού η οποία χάνεται, ελαττώνεται ή βλάπτεται κατά τη μεταφορά από λογαριασμό, σε λογαριασμό ή μεταξύ λογαριασμών.

11. Υπερβολικό Ποσό Εξαγοράς

Κάθε ονομαστική αξία κουπονιών, εκπτώσεων, δώρων, βραβείων ή οποιουδήποτε άλλου σημαντικής αξίας ανταλλάγματος που παρέχεται επιπροσθέτως του συνολικού συμφωνηθέντος ή αναμενόμενο ποσού.

12. Μη Ασφαλίσιμη Ζημία

Κάθε ζήτημα για το οποίο ο Ασφαλιστής απαγορεύεται να προβεί σε πληρωμή, βάσει των κανόνων ή της δικαιοδοσίας στην οποία προβάλλεται Απαίτηση ή στην οποία προκύπτει για πρώτη φορά Ασφαλιστικό Γεγονός.

13. Ρύπανση

Οποιαδήποτε επίπτωση στον αέρα, το έδαφος ή το νερό που προκύπτει από εκκένωση, διασπορά, διαρροή, απελευθέρωση ή διαφυγή οποιουδήποτε στερεού, υγρού, αέριου, βιολογικού, ραδιενεργού ή θερμικού ερεθιστικού ή μολυσματικού στοιχείου, ανεξαρτήτως εάν συμβαίνει από φυσικά αίτια, όπως καπνός, ατμός, αιθάλη, ίνες, μικρόβια, μύκητες, ιοί, αναθυμιάσεις, οξέα, αλκάλια, χημικές ουσίες, απόβλητα και άλλες τοξικές ή επικίνδυνες ουσίες, ήχοι, θόρυβος, οσμές, δονήσεις, κύματα ή μεταβολές θερμοκρασίας.

14. Συστήματα

(i) κάθε ηλεκτρική ή μηχανική αστοχία υποδομής, πλην του Συστήματος Υπολογιστών της Εταιρείας, ανεξαρτήτως εάν τελεί υπό τον έλεγχο του Ασφαλισμένου, συμπεριλαμβανομένης κάθε διακοπής τροφοδοσίας, υπέρτασης, μερικής ή γενικής διακοπής ρεύματος.

(ii) κάθε αστοχία τηλεφωνικών γραμμών, γραμμών μεταφοράς δεδομένων, δορυφόρων ή άλλων υποδομών τηλεπικοινωνιών ή δικτύωσης που δεν τελούν υπό τον έλεγχο του Ασφαλισμένου ή Εξωτερικού Παρόχου Υπηρεσιών.

(iii) κάθε αστοχία δορυφόρου.

15. Παράλειψη Αποκατάστασης

Κάθε παράλειψη αποκατάστασης ελαττωματικών συστημάτων, διαδικασιών ή λογισμικού, όπου η ύπαρξη ελαττωμάτων, ελλείψεων ή ευπάθειας σε επίθεση ή παρείσδυση έχει επισημανθεί στο Αρμόδιο Στέλεχος αρκετά έγκαιρα πριν

από την επέλευση της Ζημίας, ώστε να αποφευχθεί ή να μειωθεί ο αντίκτυπός της.

16. Ελλείψεις Διόρθωσης

Αναμόρφωση, βελτίωση ή διόρθωση τυχόν ελλείψεων ή ελαττωμάτων στα συστήματα, τις διαδικασίες, το υλικό ή το λογισμικό λειτουργίας ή των ελέγχων για ιούς της Εταιρίας που προϋπήρχαν της Αστοχίας Ασφάλειας, της Αστοχίας Ασφάλειας Εξωτερικού Παρόχου Υπηρεσιών, ή της Αστοχίας Συστήματος, ανεξαρτήτως εάν η εν λόγω Αστοχία Ασφάλειας, Αστοχία Ασφάλειας Εξωτερικού Παρόχου Υπηρεσιών, ή Αστοχία Συστήματος οφειλόταν σε τέτοια έλλειψη ή ελάττωμα.

17. Παράνομη Συλλογή Πληροφοριών

Εταιρικές Πληροφορίες ή Προσωπικές Πληροφορίες που έχουν συλλεχθεί ή τηρούνται από Ασφαλισμένο εκ δόλου ή εξ αμελείας.

18. Παραβίαση Επιχειρησιακών Συνηθειών

Η εκ μέρους της Εταιρείας απασχόληση οποιουδήποτε φυσικού προσώπου ή οποιαδήποτε επιχειρησιακή συνήθεια της Εταιρείας (συμπεριλαμβανομένης της απαίτησης για παράνομη απόλυση ή καταγγελία της εργασιακής σχέσης, διακριτική μεταχείριση, παρενόχληση, αντίποινα ή άλλη απαίτηση που αφορά την απασχόληση).

19. Αμοιβές, Αποζημίωση ή Έξοδα Ασφαλισμένου για την Παροχή Υπηρεσιών

(i) η επιστροφή αμοιβής ή αποζημίωσης Ασφαλισμένου·

(ii) το κόστος του Ασφαλισμένου για την παροχή, τη διόρθωση, την επανεκτέλεση ή την ολοκλήρωση υπηρεσιών ή

(iii) τα ποσά για τα οποία ο Ασφαλισμένος δεν είναι οικονομικά υπεύθυνος ή για τα οποία δεν μπορεί να ασκηθούν νομικά μέσα κατά κανενός Ασφαλισμένου.

20. Φορολογία

Οι φόροι που επιβαρύνουν έναν Ασφαλισμένο.

4.4.4 Εταιρείες χωρίς κρίση επι της ποιότητας ασφαλίσεων

Στο κεφάλαιο αυτό αποδίδεται, ουσιαστικά, η γενική προσφορά των ασφαλιστικών εταιρειών που λειτουργούν στην Ελλάδα εξετάζοντας όλες τις προσφορές από τις 3 μεγαλύτερες εταιρείες που ασχολούνται με το χώρο των

κυβερνοασφαλίσεων. Φυσικά, μια ασφάλεια δεν είναι ποτέ εφικτή αν δεν υπάρχουν όροι και εξαιρέσεις, γι' αυτό και έχουμε συλλέξει και όλους τους δυνατούς όρους και εξαιρέσεις. Στο υποκεφάλαιο 3.4 είδαμε ότι μετά την κρίση οι εταιρείες διαλέγουν πλέον ένα πιο οικονομικό πλαίσιο καλύψεων έναντι κινδύνων σε κυβερνοεπιθέσεις καθώς πολλές ασφαλιστικές συμβιβάζονται στην πιο οικονομική και προσιτή λύση έτσι ώστε να ωφελούνται και αυτές αλλά και οι εταιρείες-πελάτες χωρίς πραγματική, όμως, κάλυψη. Στον παρακάτω πίνακα θα δούμε ποιές εταιρείες από αυτές που λειτουργούν στην Ελλάδα προσφέρουν ασφάλειες έναντι κυβερνοεπιθέσεων και, πέρα από αυτό, ποιές από αυτές δεν έχουν χαμηλώσει την ποιότητα τους λόγω της κρίσης.

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΠΡΟΣΦΟΡΑ ΚΥΒΕΡΝΟΑΣΦΑΛΙΣΗΣ	ΚΡΙΣΗ ΠΟΙΟΤΗΤΑΣ
AIG	Ναι	Οχι
ALLIANZ	Ναι	Οχι
ARAG	Οχι	-
ATRADIUS	Ναι	Ναι
AXA	Ναι	Ναι
CNP	Οχι	-
CREDIT AGRICOLE	Οχι	-
DAS	**Οχι**	**-**
ERGO	**Οχι**	**-**
EULER HERMES	**Οχι**	**-**
EURO INSURANCES	**Οχι**	**-**
EUROLIFE ERB	**Οχι**	**-**
EUROP ASSISTANCE	**Οχι**	**-**
GENWORTH	**Ναι**	**Ναι**
GROUPAMA	**Ναι**	**Οχι**
GENERALI	**Οχι**	**-**
HDI GERLING	**Ναι**	**Ναι**
INTERAMERICAN	**Οχι**	**-**
INTERASCO	**Οχι**	**-**
INTERLIFE	**Οχι**	**-**
INTER PARTNER	**Οχι**	**-**

ΑΣΦΑΛΙΣΤΙΚΗ ΕΤΑΙΡΙΑ	ΠΡΟΣΦΟΡΑ ΚΥΒΕΡΝΟΑΣΦΑΛΙΣΗΣ	ΚΡΙΣΗ ΠΟΙΟΤΗΤΑΣ
INTERNATIONAL LIFE	Οχι	-
MARSH	Ναι	Οχι
METLIFE	Οχι	-
MONDIAL ASSISTANCE	Οχι	-
MALAYAN	Ναι	Ναι
MAPFRE	Οχι	-
NP	Οχι	-
PRIME	Οχι	-
PERSONAL	Οχι	-
RSA	Ναι	Ναι
SOGECAP	Οχι	-
Α.Ε.Γ.Α	Οχι	-
AIGAION	Οχι	-
ΑΤΕ	Οχι	-
ΑΤΛΑΝΤΙΚΗ ΕΝΩΣΗ	Οχι	-
ΓΕΝΙΚΗ ΠΑΝΕΛΛΑΔΙΚΗ	Οχι	-
ΔΥΝΑΜΙΣ	Οχι	-
ΕΘΝΙΚΗ	Οχι	-
LLOYD'S	Ναι	Οχι
ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΙΣ(ΜΙΝΕΤΤΑ)	Οχι	-
ΕΥΡΩΠΑΙΚΗ ΠΙΣΤΗ	Οχι	-
ΕΥΡΩΠΗ	Οχι	-
ΙΝΤΕΡΣΑΛΟΝΙΚΑ	Οχι	-
NN	Ναι	Οχι
ΟΡΙΖΩΝ	Οχι	-
ΣΥΝΕΤΑΙΡΙΣΤΙΚΗ	Οχι	-
ΥΔΡΟΓΕΙΟΣ	Οχι	-

Πίνακας 4.1: Αλλοίωση ποιότητας ασφαλιστικών εταιρειών

Όπως βλέπουμε παραπάνω, η ποιότητα των συμβολαίων μένει αναλλοίωτη στις πολύ μεγάλες ασφαλιστικές εταιρείες, αλλά και σε αυτές οι οποίες προσέφεραν απλές και αρχικού σταδίου καλύψεις. Σε γενικότερο βαθμό όμως, μετά την κρίση η ποιότητα των καλύψεων έναντι κυβερνοεπιθέσεων υπέστη αλλοίωση.

5. Σύγκριση της Ελληνικής αγοράς με τη διεθνή

Στο κεφάλαιο αυτό θα δούμε την κατάσταση στην οποία βρίσκεται η Ελληνική αγορά σε σύγκριση με τη διεθνή αγορά. Είναι δεδομένο ότι η Ελληνική αγορά έχει πολύ χαμηλό βαθμό διείσδυσης στο χώρο σε σύγκριση με αυτό που θα μπορούσε να προσφέρει. Το πρόβλημα αυτό εντείνεται τα τελευταία χρόνια, κατά τα οποία η χώρα διέπεται από τη μεγαλύτερη οικονομική κρίση της ιστορίας της. Οι καλύψεις έναντι κυβερνοεπιθέσεων είναι κάτι που έχει εισέλθει δυναμικά στην αγορά μετά το 2010 καθώς η έννοια της ασφάλειας άρχισε να γίνεται αναγκαία στους ανθρώπους και στις επιχειρήσεις μετά το 2008. Η Ελλάδα, κατά τα χρόνια της ραγδαίας αυτής ανάπτυξης της ασφάλειας, πλήττεται από κρίση, πράγμα που την εμποδίζει να αναπτυχθεί σε αυτό το κομμάτι.

5.1 Οικονομική Κρίση

Το φαινόμενο της κρίσης είναι γνωστό σε όλους, ανεξάρτητα από το πόσο επηρεάζει την ζωή του καθενός, ενώ τα τελευταία χρόνια έχει φτάσει σε απελπιστική κατάσταση. Το έλλειμμα και το χρέος των ελληνικών δημοσιονομικών αυξάνεται και προβλέπεται να φτάσει σε ανησυχητικά επίπεδα. Μια από τις σημαντικότερες συνέπειες της κρίσης της οικονομίας είναι η αύξηση της ανεργίας, η οποία έχει φτάσει σε διψήφιο ποσοστό, ενώ ανάμεσα στους νέους το ποσοστό των ανέργων ξεπερνά το 25%. Στοιχεία των τελευταίων μηνών δείχνουν την ύπαρξη μιας διαρθρωτικής αδυναμίας της ελληνικής οικονομίας να δημιουργήσει νέες θέσεις εργασίας εντείνοντας την ανησυχία για το φαινόμενο. Μεγάλο μερίδιο της ευθύνης φέρει για αυτήν την κατάσταση η άθλια διαχείριση των οικονομικών, της ελληνικής δημοσιονομικής πολιτικής και του ασφαλιστικού αλλά και η παγκόσμια οικονομική κρίση. Στα μέσα του 2010, και μετά τις αποκαλύψεις ότι το δημοσιονομικό έλλειμμα της Ελλάδας έκλεισε για το 2009 σε επίπεδα πολύ πάνω από αυτά που θα καθιστούσαν το δημόσιο χρέος βιώσιμο, η ελληνική κυβέρνηση αδυνατούσε να δανειστεί με λογικά επιτόκια από τις αγορές για τη χρηματοδότηση του τρέχοντος δημοσιονομικού ελλείμματος και την αναχρηματοδότηση του χρέους. Αποτέλεσμα ήταν ο άμεσος κίνδυνος στάσης πληρωμών του Ελληνικού Δημοσίου. Η προσπάθεια της κυβέρνησης να ανακτήσει την αξιοπιστία της χώρας στις διεθνείς αγορές και να πετύχει μείωση των επιτοκίων οδήγησε σε λήψη μέτρων μείωσης των δαπανών, τα οποία δεν κατάφεραν να ανατρέψουν το αρνητικό κλίμα. Κατόπιν αυτών η

Ελλάδα κατέφυγε στη βοήθεια του Διεθνούς Νομισματικού Ταμείου, της Ευρωπαϊκής Επιτροπής και της Ευρωπαϊκής Κεντρικής Τράπεζας, (Θεσμούς του Ευρωπαϊκού και παγκοσμίου οικονομικού κατεστημένου) που συγκρότησαν από κοινού μηχανισμό για την Ελλάδα.

5.2 Καλύψεις και ασφάλεια έναντι κυβερνοεπιθέσεων στην Ελλάδα

Μετά τις Ηνωμένες Πολιτείες και η Ευρωπαϊκή Ένωση δείχνει αποφασισμένη να θέσει την κυβερνοασφάλεια αρκετά υψηλά στις προτεραιότητες της. Είναι χαρακτηριστικό ότι η Ευρωπαϊκή Επιτροπή ανακοίνωσε μία νέα σύμπραξη δημόσιου - ιδιωτικού τομέα για την κυβερνοασφάλεια, η οποία αναμένεται να προσελκύσει επενδύσεις ύψους 1,8 δισ. ευρώ έως το 2020! Η σύμπραξη αυτή, όπως επισημαίνεται στη σχετική ανακοίνωση, εντάσσεται στο πλαίσιο των νέων πρωτοβουλιών για καλύτερη θωράκιση της Ευρώπης έναντι των κυβερνοεπιθέσεων και ενίσχυση της ανταγωνιστικότητας του κλάδου της κυβερνοασφάλειας. Σύμφωνα με πρόσφατη έρευνα, τουλάχιστον το 80% των ευρωπαϊκών επιχειρήσεων έχουν καταγράψει ένα τουλάχιστον περιστατικό όσον αφορά την κυβερνοασφάλεια το τελευταίο έτος, ενώ ο αριθμός τέτοιων περιστατικών σε όλους τους κλάδους ανά τον κόσμο αυξήθηκε κατά 38% το 2015. Το γεγονός αυτό βλάπτει τις ευρωπαϊκές επιχειρήσεις, μεγάλες ή μικρές, και υπονομεύει την εμπιστοσύνη στην ψηφιακή οικονομία. Στο πλαίσιο της στρατηγικής για την Ψηφιακή Ενιαία Αγορά, η Ευρωπαϊκή Επιτροπή επιθυμεί να ενισχύσει τη διασυνοριακή συνεργασία όλων όσων δραστηριοποιούνται σε θέματα κυβερνοασφάλειας και να προωθήσει την ανάπτυξη καινοτόμων και ασφαλών τεχνολογιών, προϊόντων και υπηρεσιών σε όλη την ΕΕ. Η Ελλάδα, εξαιτίας της οικονομικής κρίσης που την διέπει, είναι, κατά την γνώμη μου, σχεδόν αδύνατο να ακολουθήσει την τάση της Ε.Ε. Οι επιχειρήσεις στην Ελλάδα παλεύουν να επιβιώσουν λόγω του οικονομικού πλαισίου που έχει επιβληθεί στη χώρα οπότε αυτό που προσπαθεί η Ε.Ε να προωθήσει είναι με βεβαιότητα σχεδόν αδύνατο να καθιερωθεί στην Ελλάδα.

5.3 Μελλοντικές ενέργειες της Ε.Ε.

Το σχέδιο δράσης που ανακοινώθηκε περιλαμβάνει τη δρομολόγηση της πρώτης ευρωπαϊκής σύμπραξης δημόσιου και ιδιωτικού τομέα στον τομέα της κυβερνοασφάλειας. Η ΕΕ θα επενδύσει 450 εκατομμύρια ευρώ στη σύμπραξη αυτή, στο πλαίσιο του προγράμματος έρευνας και καινοτομίας «Ορίζοντας

2020». Παράγοντες της αγοράς κυβερνοασφάλειας, εκπροσωπούμενοι από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια στον Κυβερνοχώρο (ECSO), αναμένεται να επενδύσουν τρεις φορές περισσότερο. Στη σύμπραξη αυτή θα μετέχουν επίσης μέλη εθνικών, περιφερειακών και τοπικών δημόσιων αρχών, ερευνητικών κέντρων και πανεπιστημίων. Στόχος είναι η ανάπτυξη στενότερης συνεργασίας στα αρχικά στάδια της διαδικασίας έρευνας και καινοτομίας και η εξεύρεση λύσεων για θέματα κυβερνοασφάλειας σε διάφορους τομείς, όπως η ενέργεια, η υγεία, οι μεταφορές και ο χρηματοπιστωτικός κλάδος. Η Ευρωπαϊκή Επιτροπή παρουσίασε, επίσης, διάφορα μέτρα για να αντιμετωπιστεί ο κατακερματισμός της ευρωπαϊκής αγοράς κυβερνοασφάλειας. Επί του παρόντος, μια εταιρεία πληροφορικής πρέπει να ακολουθεί διαφορετικές διαδικασίες πιστοποίησης για να μπορεί να πωλεί τα προϊόντα και τις υπηρεσίες της σε περισσότερες από μία χώρες της Ευρωπαϊκής Ένωσης. Γι' αυτό, η Ευρωπαϊκή Επιτροπή θα εξετάσει την πιθανότητα δημιουργίας ενός ευρωπαϊκού πλαισίου πιστοποίησης των προϊόντων ασφάλειας στον τομέα της πληροφορικής.

5.3.1 Τι σημαίνει κυβερνοασφάλεια για την Ε.Ε.

Μετά από μελέτη διάφορων ορισμών για τη Κυβερνοασφάλεια πιστεύω ότι ο πληρέστερος ορισμός και αυτός ο οποίος ανταποκρίνεται καλύτερα στις συνθήκες του σήμερα και της Ε.Ε είναι ο παρακάτω:

Κυβερνοασφάλεια είναι όλες οι οργανωμένες ενέργειες οι οποίες απαιτούνται για να εξασφαλιστούν οι πληροφορίες από κάθε κίνδυνο ή ρίσκο σε όλες τους τις μορφές (ηλεκτρονικές, φυσικές), καθώς και για να εξασφαλιστούν τα συστήματα και τα δίκτυα, μέσω των οποίων γίνεται η αποθήκευση, η ανάκτηση, η επεξεργασία και η μεταφορά τους, περιλαμβανομένων των ενεργειών οι οποίες πρέπει να γίνονται, ώστε να προφυλάσσονται από εγκληματικές ενέργειες, δολιοφθορές, κατασκοπεία, ατυχήματα, και αστοχίες. Στους κινδύνους για τη Κυβερνοασφάλεια πρέπει να συμπεριληφθούν κι αυτοί που αφορούν την μείωση της εμπιστοσύνης και αξιοπιστίας των παροχών προς τους πελάτες τους και οι οποίοι αν δεν αντιμετωπιστούν, είναι δυνατόν να επηρεάσουν αρνητικά τη σταθερότητα και περαιτέρω ανάπτυξη των πελατών τους, παραβιάζοντας την προστασία της ταυτότητας και ιδιωτικότητας των ίδιων των πελατών και των συνεργατών τους, αποδιοργανώνοντας την δυνατότητα ή επικοινωνίας ή διεξαγωγής επαγγελματικών συναλλαγών, επηρεάζοντας δυσμενώς την υγεία και

προκαλώντας απώλειες και επηρεάζοντας δυσμενώς τις επιχειρήσεις της εθνικής κρίσιμης υποδομής.

5.3.2 Νέα οδηγία

Παράλληλα, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε τη νέα οδηγία για την ασφάλεια δικτύων και πληροφοριών, η οποία δημιουργεί ένα δίκτυο ομάδων παρέμβασης για περιστατικά που αφορούν την ασφάλεια των υπολογιστών σε ολόκληρη την ΕΕ, με στόχο την ταχεία αντίδραση στις απειλές και τα περιστατικά στον κυβερνοχώρο. Επίσης, θεσπίζει μια «Ομάδα Συνεργασίας» μεταξύ των κρατών μελών, με σκοπό την υποστήριξη και διευκόλυνση της στρατηγικής συνεργασίας καθώς και της ανταλλαγής πληροφοριών, και την καλλιέργεια πνεύματος αξιοπιστίας και εμπιστοσύνης.

5.3.3 Νέοι μηχανισμοί

Παράλληλα, η Ευρωπαϊκή Επιτροπή καλεί τα κράτη μέλη να αξιοποιήσουν στο έπακρο τους νέους αυτούς μηχανισμούς και να ενισχύσουν τον μεταξύ τους συντονισμό όταν και όπου αυτό είναι δυνατό. Θα προτείνει επίσης τρόπους βελτίωσης της διασυνοριακής συνεργασίας σε περίπτωση σοβαρών περιστατικών στον κυβερνοχώρο. Δεδομένης της ταχύτητας με την οποία αλλάζει το τοπίο στα θέματα κυβερνοασφάλειας, η Ευρωπαϊκή Επιτροπή σκοπεύει να προβεί σε αξιολόγηση του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), προκειμένου να εξακριβώσει κατά πόσον η εντολή και η ικανότητα του ENISA εξακολουθούν να επαρκούν ώστε να μπορέσει να ανταποκριθεί στην αποστολή του για στήριξη των κρατών μελών στις προσπάθειες αύξησης της ανθεκτικότητάς τους έναντι των κυβερνοεπιθέσεων. Η Ευρωπαϊκή Επιτροπή εξετάζει επίσης τρόπους ενίσχυσης και εξορθολογισμού της συνεργασίας για την κυβερνοασφάλεια σε διάφορους τομείς της οικονομίας, περιλαμβανομένης της εκπαίδευσης και της κατάρτισης στην κυβερνοασφάλεια.

5.4 Διαστάσεις κυβερνοασφάλειας στήν Ε.Ε.

Η Ευρωπαϊκή Ένωση, επίσης, κάνει προσπάθειες για να εξασφαλίσει τα δίκτυα και τις πληροφορίες της. Η EU θεωρεί ότι τα συστήματα επικοινωνίας και πληροφοριών είναι σημαντικοί παράγοντες στην εξέλιξη της οικονομίας και κοινωνίας. Για την εξασφάλιση της Κυβερνοασφάλειας η Ε.Ε ίδρυσε τον ENISA, ο οποίος δημιουργήθηκε για να ενδυναμώσει τη δυνατότητα της Ευρωπαϊκής

Ένωσης, των Κρατών μελών της Ε.Ε. και της επαγγελματικής κοινότητας να αποφεύγει, να διευθύνει και να ανταποκρίνεται σε προβλήματα που αφορούν την ασφάλεια των δικτύων και πληροφοριών. Ο ENISA αποτελεί ένα κέντρο εμπειρογνωμοσύνης σε θέματα Ασφάλειας των Δικτύων και Πληροφοριών και προωθεί τη συνεργασία ανάμεσα στο δημόσιο και ιδιωτικό τομέα. Προκειμένου να διασφαλίσει την εκπλήρωση των στόχων, οι δράσεις του Οργανισμού επικεντρώνονται στα εξής:

- Την παροχή συμβουλών και βοήθειας στην Επιτροπή και τα Κράτη μέλη.
- Τη συλλογή και ανάλυση δεδομένων για τα περιστατικά ασφαλείας στην Ευρώπη και τους πιθανούς κινδύνους
- Την προώθηση μεθόδων διαχείρισης κρίσεων
- Την αύξηση της γνώσης και της συνεργασίας ανάμεσα στους διαφορετικούς παράγοντες στο πεδίο της ασφάλειας των πληροφοριών.

5.5 Διαστάσεις κυβερνοασφάλειας στήν Ελλάδα

Στην Ελλάδα, σήμερα υπάρχει μια πανσπερμία δημόσιων υπηρεσιών, ανεξάρτητων αρχών, οργανισμών και φορέων οι οποίες έχουν αρμοδιότητες οι οποίες σχετίζονται με τη Κυβερνοασφάλεια. Οι κυριότερες απ' αυτές είναι:

(1) Το Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ), που έχει επιτελικό ρόλο σε εθνικό επίπεδο και είναι αρμόδιο για την έκδοση το Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ) σε συνεργασία με την Εθνική Υπηρεσία Πληροφοριών. Ο ΕΚΑ έχει εφαρμογή σε όλη τη Δημόσια Διοίκηση.
(2) Η ΕΥΠ, που αποτελεί Αρχή Ασφάλειας Πληροφοριών (INFOSEC), είναι υπεύθυνη για το εθνικό Computer Emergency and Response Team (CERT) και αποτελεί την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων.
(3) Η Διεύθυνση Πολιτικού Σχεδιασμού Έκτακτης Ανάγκης (ΠΣΕΑ) και η Υπηρεσία Ανάπτυξης Πληροφορικής (ΥΑΠ) του Υπουργείου Εσωτερικών (ΥΠΕΣ).
(4) Η Ελληνική Αστυνομία (ΕΛΑΣ), ως υπαγόμενη στο ΥΠΕΣ, που εμπλέκεται κυρίως μέσω της Διεύθυνσης Χειρισμού Κρίσεων, της Διεύθυνσης Εγκληματολογικών Υπηρεσιών της Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος, του Τομέα Εξέτασης Ψηφιακών Πειστηρίων κλπ.
(5) Το Υπουργείο Μεταφορών και Επικοινωνιών (ΥΜΕ), που είναι αρμόδιο για τη χάραξη πολιτικής για την ασφάλεια των δημόσιων δικτύων και των υπρεσιών ηλεκτρονικών επικοινωνιών.

(6) Ανεξάρτητες αρχές, όπως η Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ), η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), οι οποίες παρεμβαίνουν σε θέματα της αρμοδιότητάς τους.

(7) Η Τράπεζα της Ελλάδας (ΤτΕ), που εμπλέκεται στην πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος για τη νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες και τη χρηματοδότηση ειδικών εγκλημάτων βίας.

(8) Η Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας του Εθνικού Δικτύου Έρευνας και Τεχνολογίας (ΕΔΕΤ-CERT, GRNET-CERT), που είναι αρμόδια να ανταποκρίνεται σε περιστατικά ανασφάλειας στον ελληνικό δικτυακό χώρο (.gr).

(9) Φορείς και υπηρεσίες, όπως ο Ελληνικός Φορέας Πρόληψης της Ηλεκτρονικής Απάτης (ΕΦΤΑ), ο Σύνδεσμος Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδας (ΣΕΠΕ), ο ελληνικός κόμβος ασφαλούς διαδικτύου SafeNetHomePlus, η υπηρεσία SafeLine, καθώς και ιδιαιτέρως, λόγω της ιδιαίτερης δυναμικής που μπορεί να επιδείξει, η Ομάδα Δράσης για την Ψηφιακή Ασφάλεια (Digital Awareness and Response to Threats, DART).

(10) Η Δνση Κυβερνοάμυνας (ΔΙΚΥΒ) του ΓΕΕΘΑ με αρμοδιότητες, τη προστασία της Πληροφοριακής Υποδομής των Ε.Δ σε ειρήνη, κρίση και πόλεμο, τη συνδρομή στη προστασία κρίσιμων Πληροφοριακών Υποδομών της Χώρας σε περίοδο ειρήνης, η υλοποίηση υποχρεώσεων οι οποίες προκύπτουν στον τομέα του Κυβερνοχώρου στο πλαίσιο του ΝΑΤΟ και ΕΕ, τη διοργάνωση και διεξαγωγή ασκήσεων Κυβερνοάμυνας σε Εθνικό επίπεδο.

Όπως γίνεται αντιληπτό το θέμα της Κυβερνοασφάλειας είναι θέμα το οποίο απασχολεί την Ελληνική Δημόσια Διοίκηση. Ο βαθμός επιτυχίας της στον τομέα της Κυβερνοασφάλειας είναι, παρά ταύτα, πολύ χαμηλός. Ως βασικός λόγος πρέπει να θεωρηθεί η έλλειψη κοινής πολιτικής κυβερνοασφάλειας και συντονιστικού φορέα. Με τον τομέα της κυβερνοασφάλειας να είναι σε χαμηλή προτεραιότητα, την ίδια λογική ακολουθούν και οι Ελληνικές ασφαλιστικές εταιρείες με τα συμβόλαια έναντι κυβερνοεπιθέσεων που προσφέρουν.

5.6 Σημαντική διαφόρα της Ελλάδας με την Ε.Ε στο Πλαίσιο της κυβερνοασφάλισης

Σημαντικό προκειμένου να καθορίσουμε τις διαστάσεις της Κυβερνοασφάλειας είναι να κοιτάξουμε ποιες είναι οι τάσεις για τη χρήση του ίντερνετ στο εγγύς και στο απώτερο μέλλον. Στο διαδίκτυο ήδη σήμερα στηρίζονται συστήματα τα οποία είναι κρίσιμα για τη λειτουργία και ευημερία ενός κράτους: τραπεζικά, φορολογικά, δίκτυα κοινής ωφελείας, υγειονομικά κ.λπ. Η ανάγκη μείωσης του κόστους λειτουργίας των συστημάτων είναι ένα πάγιο ζητούμενο για όλους. Το γεγονός αυτό σύντομα, κι όταν η τεχνολογία το επιτρέψει, θα οδηγήσει τα συστήματα υψηλής διαβάθμισης να εγκαταλείψουν τη αποκλειστική υποδομή και να χρησιμοποιούν την κοινόχρηστη υποδομή, το κόστος της οποίας είναι υποπολλαπλάσιο της αποκλειστικής ενώ η διαθέσιμη χωρητικότητα πολλαπλάσια. Οι τεχνολογίες οι οποίες επιτρέπουν τη μείωση του κόστους λειτουργίας ενός συστήματος, χρησιμοποιώντας κεντρική φιλοσοφία με αποκεντρωμένους πόρους, ήδη υφίσταται, αυτό που απομένει είναι να εξασφαλιστούν τεχνολογίες που θα εξασφαλίζουν την ασφαλή λειτουργία τους στο περιβάλλον του ίντερνετ.

5.7 Μεγάλα κενά της Ελλάδας στο κλάδο

Υπάρχουν συγκεκριμένοι τρόποι ασφάλισης, οι ασφαλιστές και οι μεσίτες θα μπορούσαν να θέσουν στον κυβερνοχώρο ασφάλιση με μια πιο βιώσιμη πορεία και να επωφεληθούν από τις ευκαιρίες για κερδοφόρα ανάπτυξη:

5.7.1 Αποτίμηση της μέγιστης απώλειας

Η τιμολόγηση θα συνεχίσει να είναι τόσο μια τέχνη όσο και επιστήμη με την απουσία ισχυρών αναλογιστικών δεδομένων. Αλλά μπορεί να είναι δυνατό να αναπτυχθεί μια πολύ σαφέστερη εικόνα της συνολικής μέγιστης απώλειας που να είναι δυνατόν να ταιριάξει με την ικανότητα ανοχής του κινδύνου. Όσο μεγαλύτερη είναι η ανοχή στον κίνδυνο τόσο μεγαλύτερη είναι η σύνθεση ενός χαρτοφυλακίου με μετοχές υψηλού κινδύνου, χρεόγραφα και ξένα νομίσματα.

Η αντιστάθμιση κινδύνου (hedging) είναι μια τεχνική κάλυψης απέναντι στις απώλειες κεφαλαίων που μπορεί να προκύψουν ως αποτέλεσμα απρόσμενων κινήσεων της αγοράς, με χαρακτηριστικότερη την προστασία έναντι του συναλλαγματικού, του επιτοκιακού ή του συστημικού κινδύνου. Νομοθετικός κίνδυνος είναι το ρίσκο που παίρνει μια επιχείρηση είτε να εισαχθεί μια νέα

νομοθεσία, είτε να αλλάξει μια παλαιότερη, με αποτέλεσμα να επηρεαστούν αρνητικά οι επενδύσεις της. Νομικός κίνδυνος είναι ο κίνδυνος που αντιμετωπίζουν επιχειρήσεις και επενδυτές να απολέσουν κεφάλαια ή κέρδη λόγω της έκδοσης αντίθετων δικαστικών αποφάσεων σε διαφορετικές χώρες στις οποίες δραστηριοποιούνται.

5.7.2 Κίνδυνος βάσει συνθηκών

Πολλοί ασφαλιστές επιβάλλουν τώρα ένα πλαίσιο όρων και προϋποθέσεων. Μια πιο αποτελεσματική προσέγγιση θα ήταν να γίνει η κάλυψη εξαρτώμενη από μια πληρέστερη και πιο συχνή αξιολόγηση των τρωτών σημείων του ασφαλιζόμενου και να ακολουθήσει η συμφωνία. Αυτό θα μπορούσε να περιλαμβάνει ένα έλεγχο των διαδικασιών, των ευθυνών και της διακυβέρνησης μέσα στην επιχείρηση του πελάτη. Θα μπορούσε επίσης να περιλαμβάνει αξιολογήσεις απειλών οι οποίες θα αντληθούν από τις αξιολογήσεις των απειλών για τις βιομηχανίες και / ή συγκεκριμένων επιχειρήσεων, που παρέχονται από κυβερνητικές υπηρεσίες και άλλες αξιόπιστες πηγές. Θα μπορούσε επίσης να συμπεριληφθούν ασκήσεις που μιμούνται τις επιθέσεις για να ελεγχθούν οι αδυναμίες και τα σχέδια για την απάντηση. Ως προϋπόθεση της κάλυψης, θα μπορούσε στη συνέχεια, να καθοριστεί η εφαρμογή των κατάλληλων τεχνολογιών για την πρόληψη και τον εντοπισμό των διαδικασιών.

Η επιχείρηση θα ωφεληθεί από μια καλύτερη κατανόηση και έλεγχο. Οι κίνδυνοι που θα επιλέξει να αποδεχθεί η εταιρεία φέρνουν, ως εκ τούτου, μείωση των χρηματοδοτικών ανοιγμάτων, και την ικανότητα να προσφέρει τιμολόγηση με μεγαλύτερο ενθουσιασμό. Αυτές οι αξιολογήσεις θα μπορούσαν επίσης να βοηθήσουν να εδραιωθεί μια στενότερη σχέση με τους πελάτες και να παρέχει τα θεμέλια για την αμοιβή με βάση τις παρεχόμενες συμβουλευτικές υπηρεσίες.

5.7.3 Διευκόλυνση των κινδύνων

Λόγω της γενικευμένης παρουσίας των δικτύων επικοινωνίας και των συστημάτων πληροφοριών, το ζήτημα της ασφάλειάς τους έχει καταστεί θέμα που δημιουργεί ολοένα και μεγαλύτερες ανησυχίες στην κοινωνία. Για να διασφαλιστεί στους χρήστες ο πλέον υψηλός βαθμός ασφάλειας, η Ευρωπαϊκή Ένωση (ΕΕ) αποφάσισε να δημιουργήσει έναν ευρωπαϊκό οργανισμό επιφορτισμένο με την ασφάλεια δικτύων και πληροφοριών (ENISA), ο οποίος θα έχει συμβουλευτικό και συντονιστικό ρόλο προς την Επιτροπή και τις

χώρες της ΕΕ ως προς τα μέτρα που λαμβάνουν για να καταστήσουν ασφαλή τα δίκτυα και τα συστήματα πληροφοριών τους. Σκοπός της Ευρωπαϊκής Ένωσης, των χωρών της ΕΕ και του κλάδου των επιχειρήσεων είναι να προλαμβάνουν, αντιδρούν και να διαχειρίζονται προβλήματα που συνδέονται με την ασφάλεια δικτύων και πληροφοριών. Επιπλέον, ο ENISA παρέχει βοήθεια και συμβουλές στην Επιτροπή και στις χώρες της ΕΕ. Μπορεί επίσης να του ζητηθεί να συνδράμει την Επιτροπή στις τεχνικές προπαρασκευαστικές εργασίες ενημέρωσης και ανάπτυξης της νομοθεσίας της ΕΕ. Εξάλλου, ο ENISA πρέπει να διευκολύνει και να ενθαρρύνει τη συνεργασία μεταξύ των φορέων του δημόσιου και του ιδιωτικού τομέα και, με τον τρόπο αυτό, να καταστήσει δυνατή την επίτευξη αρκετά υψηλού επιπέδου ασφάλειας στις χώρες της ΕΕ.

Καθήκοντα

Για την επίτευξη των στόχων που παρουσιάζονται ανωτέρω, ο ENISA εκτελεί τα ακόλουθα καθήκοντα:

- συλλογή των αναγκαίων πληροφοριών για την ανάλυση των σημερινών και των μελλοντικών κινδύνων, και διαβίβαση των αποτελεσμάτων στις χώρες της ΕΕ και στην Επιτροπή·
- παροχή συμβουλών καθώς και, κατά περίπτωση, παροχή συνδρομής στο Ευρωπαϊκό Κοινοβούλιο, στην Επιτροπή και στους αρμόδιους ευρωπαϊκούς και εθνικούς οργανισμούς·
- ενίσχυση της συνεργασίας μεταξύ των διαφόρων φορέων του τομέα (π.χ. μέσω διαβουλεύσεων και δικτύωσης)·
- διευκόλυνση της συνεργασίας μεταξύ της Επιτροπής και των χωρών της ΕΕ για την εκπόνηση κοινών μεθοδολογιών για την πρόληψη των προβλημάτων ασφάλειας·
- συμβολή στην ευαισθητοποίηση των χρηστών και στην ταχεία διάθεση στους χρήστες αντικειμενικών και διεξοδικών πληροφοριών για την ασφάλεια των δικτύων πληροφοριών (π.χ. μέσω της προώθησης της ανταλλαγής των βέλτιστων πρακτικών, συμπεριλαμβανομένων των μεθόδων προειδοποίησης των χρηστών, και της αναζήτησης περιπτώσεων συνέργειας μεταξύ του δημόσιου και του ιδιωτικού τομέα)·
- παροχή συνδρομής στην Επιτροπή και στις χώρες της ΕΕ κατά το διάλογο που διεξάγουν με τις επιχειρήσεις με σκοπό τη διαχείριση των προβλημάτων ασφάλειας που θέτουν το υλισμικό και το λογισμικό·

- παρακολούθηση της εξέλιξης των προτύπων για προϊόντα και υπηρεσίες που αφορούν την ασφάλεια και προώθηση των δραστηριοτήτων εκτίμησης κινδύνων και τη διαχείριση κινδύνων·
- συμβολή στις πρωτοβουλίες σε επίπεδο ΕΕ με σκοπό τη συνεργασία με τρίτες χώρες και με διεθνείς οργανισμούς για τη διαμόρφωση σφαιρικής προσέγγισης του θέματος της ασφάλειας·
- παρουσίαση των συμπερασμάτων, προσανατολισμών και συμβουλών του.

5.8 Υπόλοιπος κόσμος

Η αντιμετώπιση των απειλών για επιθέσεις στον κυβερνοχώρο με την εμπλοκή ξένων κυβερνήσεων, αποτέλεσε πραγματικό "πονοκέφαλο" για την κυβέρνηση του Μπαράκ Ομπάμα, κατά την οκταετία άσκησης των προεδρικών καθηκόντων του στις ΗΠΑ. Τα τελευταία οκτώ χρόνια οι ΗΠΑ έχουν γίνει στόχος επιθέσεων στο διαδίκτυο, με έμφαση σε υπηρεσίες της αμερικανικής κυβέρνησης, αλλά και ιδιωτικές εταιρίες, με τις κυβερνοεπιθέσεις αυτές να αποδίδονται στην Κίνα, τη Βόρεια Κορέα, το Ιράν, αλλά και τη Ρωσία. Στις υποθέσεις ηλεκτρονικών υποκλοπών που έγιναν γνωστές, οι Αμερικανοί αξιωματούχοι αποφάσισαν να κατηγορήσουν δημόσια τη Βόρεια Κορέα, αλλά και να στραφούν δημοσίως κατά Κινέζων αξιωματούχων, στοχεύοντας στη αρνητικές επιπτώσεις από τη δημοσιοποίηση του ονόματός τους. Ωστόσο, το ζήτημα που έχει προκύψει με τη Ρωσία κι αναφορικά με τις εκτιμήσεις των αμερικανικών υπηρεσιών ασφάλειας για την εμπλοκή της, στις προεκλογικές υποκλοπές ηλεκτρονικών μηνυμάτων σε βάρος του Δημοκρατικού Κόμματος είναι ουσιαστικά πιο πολύπλοκο από τις προηγούμενες υποθέσεις. Σε πρώτο επίπεδο, οι ρωσικές δυνατότητες για τη διεξαγωγή επιχειρήσεων στον κυβερνοχώρο είναι τεχνολογικά πιο αναπτυγμένες, ώστε να είναι δύσκολος ο εντοπισμός των ηλεκτρονικών ιχνών εντοπισμού της πηγής που προκάλεσε την παρεμβολή. Σε δεύτερο επίπεδο, στην Ουάσιγκτον εκφράζονται φόβοι για το ενδεχόμενο καλλιέργειας γεωπολιτικής αστάθειας σε ανοιχτά πολεμικά μέτωπα, όπως ο εμφύλιος πόλεμος στη Συρία. Ο Λευκός Οίκος αναμένεται ν' ανακοινώσει σειρά μέτρων κατά της Ρωσίας στον απόηχο των εκτιμήσεων και καταγγελιών για την εμπλοκή της Μόσχας στις προεκλογικές υποκλοπές κατά του Δημοκρατικού Κόμματος, ενεργοποιώντας ειδικό προεδρικό διάταγμα που είχε υπογράψει ο πρόεδρος Ομπάμα τον Απρίλιο του 2015.

5.9 Απολογισμός επιθέσεων του 2016 σε Παγκόσμια κλίμακα

Το 2016 αποτελεί μία από τις χειρότερες χρονιές σε ό,τι αφορά τις κυβερνο-επιθέσεις που έλαβαν χώρα παγκοσμίως, καθώς αυτές πολλαπλασιάστηκαν φέτος σε σχέση με προηγούμενες χρονιές. Το τελευταίο έτος, οι επιθέσεις είναι πιο εξελιγμένες και στην πλειονότητα των περιπτώσεων έχουν πραγματοποιηθεί σε μεγάλη κλίμακα. Το γεγονός αυτό αποτελεί μια ανατριχιαστική προειδοποίηση, καθώς οι επιθέσεις DDoS (κατανεμημένη επίθεση άρνησης υπηρεσιών) γίνονται ολοένα και πιο πολλές και σε τέτοια κλίμακα που λίγοι πίστευαν ότι θα ήταν εφικτό. Οι επιθέσεις αυτές -όπου τεράστιες ποσότητες δεδομένων διανέμονται σε διαδικτυακά συστήματα, ώστε αυτά να μην μπορούν πλέον να ανταποκρίνονται στα νόμιμα αιτήματα- εξελίχθηκαν σε μεγάλο βαθμό μέσα στο τρέχον έτος, καθώς οι χάκερς «συνειδητοποίησαν» ότι μπορούν να εκμεταλλεύονται ευάλωτες συσκευές, οι οποίες αποτελούν κομμάτι του λεγόμενου Ίντερνετ των Πραγμάτων (IoT - Internet of Things). Αναμφισβήτητο είναι το γεγονός ότι το IoT υπόσχεται πολλά. Έχουμε πλέον τη δυνατότητα να δημιουργήσουμε δίκτυα, όπου μια ολόκληρη νέα γενιά «έξυπνων» συσκευών θα μπορεί να είναι συνδεδεμένες σε αυτά. Από ψυγεία και βραστήρες, μέχρι συστήματα που θερμαίνουν τα σπίτια μας και συσκευές που ταΐζουν τα κατοικίδιά μας κατά την απουσία μας.

Η χρησιμότητα του να μπορούμε να ελέγχουμε αυτές τις συσκευές από απόσταση είναι προφανής και νέες, τέτοιου είδους, «ευκολίες» θα εμφανίζονται ολοένα και πιο συχνά στο μέλλον, καθώς οι άνθρωποι σκέφτονται νέους τρόπους με τους οποίους μπορεί να χρησιμοποιηθεί η τεχνολογία. Ωστόσο, οι τεχνολογίες αυτές, που επιτρέπουν στις συσκευές να είναι «έξυπνες», τους παρέχουν παράλληλα τη δυνατότητα να γίνονται και επικίνδυνες, αποτελώντας απειλή για την ασφάλεια των προσωπικών μας δεδομένων.

Κανένας ειδικός δεν υποστηρίζει ότι οι χάκερς θα θελήσουν να «εισβάλουν» σε κάποιο κλιματιστικό προκειμένου να κλέψουν προσωπικά δεδομένα, ωστόσο ορισμένες IoT συσκευές αποθηκεύουν στοιχεία που έχουν αξία την οποία ίσως ακόμα δεν μπορούμε να κατανοήσουμε. Έτσι, οι λευκές μας συσκευές θα μπορούσαν να χρησιμοποιηθούν από χάκερς σε συντονισμένες επιθέσεις, στις οποίες ο ρόλος των προϊόντων θα είναι να αποστέλλουν τεράστιο όγκο άχρηστων δεδομένων με σκοπό να κατακλύζουν άλλα συστήματα, καθιστώντας τα άχρηστα για μικρά ή μεγάλα χρονικά διαστήματα. Οι επιθέσεις που έλαβαν χώρα μέσα στο 2016 πραγματοποιήθηκαν με τη χρήση «ζόμπι έξυπνων συσκευών» (συσκευές που εκμεταλλεύονται οι χάκερς για τις επιθέσεις τους), οι οποίες, σε συνδυασμό, δημιουργούν έναν «στρατό IoT

συσκευών» ή αλλιώς ένα botnet (ένα δίκτυο υπολογιστών που ελέγχεται εξ αποστάσεως χωρίς τη γνώση ή την έγκριση του νόμιμου χρήστη). Όσες περισσότερες συσκευές «καταταγούν» σε αυτά τα botnets, τόσο μεγαλύτερος ο όγκος άχρηστων δεδομένων που μπορεί να διανεμηθεί. Η μεγαλύτερη επίθεση που έλαβε χώρα το 2016 περιλάμβανε εκατοντάδες χιλιάδες συσκευές να χρησιμοποιούνται ταυτόχρονα στην επίθεση όπου «πρωταγωνίστησε» το Mirai botnet. Το τρομακτικό γεγονός με τη συγκεκριμένη υπόθεση ήταν ότι η επίθεση ήταν σχετικά απλή. Ένα βασικό μάθημα, που θα πρέπει να λάβουμε όλοι μας υπόψη από το Mirai, είναι ότι πρέπει ανά τακτά διαστήματα να αλλάζουμε τους κωδικούς πρόσβασης, τόσο στις IoT συσκευές, όσο και στις ιστοσελίδες τις οποίες επισκεπτόμαστε. Οι ειδικοί επιμένουν ότι δεν πρέπει να βασιζόμαστε στον εργοστασιακό κωδικό πρόσβασης μιας συσκευής, όπως π.χ. ένα ρούτερ, αλλά θα πρέπει να αλλάζουμε τα passwords ώστε να διασφαλίζουμε τα προσωπικά μας δεδομένα. Το μέλλον θα δείξει εάν τελικά οι άνθρωποι θα μπορούν να χρησιμοποιούν με ασφάλεια τις καθημερινές τους συσκευές ή εάν αυτές θα χρησιμοποιούνται ως όπλο στα χέρια κακόβουλων.

Συμπεράσματα

Ζούμε σε μια εποχή που η σύγχρονη τεχνολογία πλέον έχει εισχωρήσει στη ζωή όλων μας. Η εξέλιξη αυτή έχει αλλάξει τα δεδομένα και πλέον οι απαιτήσεις έχουν διαφοροποιηθεί. Είναι μια εποχή πρωτοφανών κυβερνοεπιθέσεων όπου οι κακόβουλες εκστρατείες, τόσο σε προσωπικό επίπεδο χρήστη υπολογιστών όσο και σε κυβερνητικούς στόχους, πραγματοποιούνται από φορητούς υπολογιστές και από ασύρματα δίκτυα. Ακόμα κι αν κάποιος δεν είναι τεχνικά καταρτισμένος, ημέρα με την ημέρα σίγουρα θα έχει ακούσει κάποια ιστορία σχετική με hacking, είτε λογίζεται ως τέτοια είτε όχι. Η Ελλάδα είναι μια από της κορυφαίες χώρες στην Ευρώπη σε τεχνογνωσία έναντι τέτοιων κινδύνων. Παρ' όλα αυτά η Ελλάδα χωλαίνει σε μεγάλο βαθμό στους πόρους. Η παρούσα έρευνα αποδεικνύει ότι η Ελλάδα σαν χώρα προτιμάει την πιο οικονομική και βραχυπρόθεσμη λύση που απευθύνεται στις εταιρείες της και όχι την μακροπρόθεσμη, πλήρη και ασφαλέστερη κάλυψη έναντι τέτοιων επιθέσεων. Το αποτέλεσμα αυτής της πράξης αναμένεται να φέρει στις εταιρείες μεγαλύτερη ζημία σε βάθος χρόνου.

Οι ασφαλιστικές εταιρείες που εντοπίστηκαν να προσφέρουν ιδανικές καλύψεις έναντι κυβερνοεπιθέσεων είναι δύο. Παρόλο το εύρος των ασφαλιστικών παροχών που προσφέρουν αυτές οι ασφαλιστικές εταιρείες, οι πελάτες τους προτιμούν μια απλή κάλυψη που θα τους εξασφαλίσει μια καλύτερη φήμη παρά μία ουσιαστική κάλυψη που θα μπορέσει να τους προστατέψει ολοκληρωτικά. Ένα μεγάλο ελαφρυντικό για το γεγονός αυτό είναι ότι η Ελλάδα βρίσκεται ακόμα σε οικονομική κρίση που πλήττει την χώρα τα τελευταία χρόνια και δεν την αφήνει να αναπτυχθεί και να ανασάνει. Παρόλα αυτά κλείνω με το συμπέρασμα ότι στην Ασφάλεια έναντι κυβερνοεπιθέσεων δεν μπορεί να ευσταθεί κανένα ελαφρυντικό γιατί αποτελεί ένα μείζων θέμα το οποίο, σε μεταγενέστερο χρόνο, αναμένεται να εξελιχθεί σε θέμα ζωής και θανάτου για τη λειτουργία μιας επιχείρησης αλλά και της χώρας εν γένει.

Πίνακες

Βιβλιογραφία

1. AIG Cyberedge file:CYBEREDGE_PLAYBOOK_tcm3877-524819.pdf
2. http://www.aig.com.gr/Specialized-products-CyberEdge_3877_523666.html
3. http://www.nextdeal.gr/%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CE%AD%CF%82-%CE%B5%CF%84%CE%B1%CE%B9%CF%81%CE%AF%CE%B5%CF%82.html?start=40
4. AIG Cyberedge file: CYBEREDGE_BROCHURE_tcm3877-524820.pdf
5. AIG Cyberedge file: CYBEREDGE_RISK_tcm3877-524825.pdf
6. AIG Cyberedge file: CYBEREDGE_STUDY_tcm3877-524826.pdf
7. AIG Cyberedge file: INSIDE CYBER - A broader view_tcm3877-616109.pdf Στατιστικά
8. https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/
9. http://www.slideshare.net/ContinuumManagedServices/12-mustknow-cybersecurity-stats-of-2014
10. [http://www.itgovernance.co.uk/blog/6-truly-shocking-cyber-security-statistics/
11. http://www.hackmageddon.com/category/security/cyber-attacks-statistics/
12. https://www.insurancedaily.gr/neos-kanonismos-gia-ta-prosopika-dedomena-kai-cyber-secure-solution/
13. http://www.cromar.gr/uploads/files/932966a2143877863d20a120681de140909bb7394310.pdf
14. http://www.cromar.gr/pages.php?p_id=163
15. http://www.cromar.gr/uploads/files/932966a2143877863d20a120681de140909bb7394310.pdf
16. http://www.newmoney.gr/bloomberg/262243-ee-nea-nomothesia-gia-tin-enisxisi-tis-kiberno-asfaleias-pros-oles-tis-etairies
17. http://gr.pcmag.com/ee-cyber-security/19189/news/o-protos-nomos-tes-ee-enantion-ton-khaker
18. http://www.geetha.mil.gr/media/1.vima-ell-strat-skepsis/kybernoasfaleia.pdf
19. http://www.apenantioxthi.com/2015/08/h-empistosynh-ws-aksi-xrhsimopoiontas-to-diadiktyo-gia-tis-koinwnikes-mas-epafes.html
20. https://home.kpmg.com/gr/el/home/insights/2016/07/cyber-security-the-end-of-innocence.html
21. http://www.imerisia.gr/article.asp?catid=27200&subid=2&pubid=114055028
22. http://eur-lex.europa.eu/legal-content/EL/ALL/?uri=URISERV:l24153
23. http://www.newsbomb.gr/bombplus/texnologia/story/756477/2016-enas-xronos-gematos-kyverno-epitheseis
24. http://www.cyberinsurancegreece.com/ereynes/psifiaki-asfaleia/

25. Smart grid cybersecurity for Europe Ivan L.G.Pearson
26. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing
27. Whitman ME, Mattord HJ. Principles of information security 3rd ed. Thompson Course Technology; 2009
28. Mitnick K, Simon W. The art of deception: controlling the human element of security. Wiley Publishing, 2002
29. Wood CC. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security, 2004
30. Martin N, Rice J. Cybercrime: understanding and addressing the concerns of stakeholders. Computers & Security2011
31. Jime´nez M, Sa´nchez P, Rosique F, A´ lvarez B, Iborra A. A tool for facilitating the teaching of smart home applications. Computing Applications in Engineering Education 2011
32. Ariely D. The (honest) truth about dishonesty: how we lie to everyone e especially ourselves. HarperCollins, 2012
33. Stephenson, Debbie. "Spear Phishing: Who's Getting Caught?". Firmex. Retrieved 27 July 2014
34. Hoofnagle, Chris Jay, Identity Theft: Making the Known Unknowns Known. Harvard Journal of Law and Technology, Vol. 21, Fall 2007
35. It All Depends, Lori M. Kaufman, chief technology officer at BAE Systems, July/August 2009, Copublished by the IEEE Computer and Reliability Sicieties 114
36. Akdeniz, Yaman (2008). Internet child pornography and the law: national and international responses
37. ENISA - Cooperative models for effective public private partnership - Good practice guide
38. ENISA - Report on the Second International Conference on Cyber-crisis Cooperation and Exercises, October 2013
39. EC3 – EUROPOL: First year report
40. Cisco 2014 - Annual Security Report
41. Motion for a resolution to wind up the debate on the statement by the Commission pursuant to Rule 110(2) of the Rules of Procedure on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)) , 6-9-13
42. Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 22ας Νοεμβρίου 2012 σχετικά με την ασφάλεια και την άμυνα στον κυβερνοχώρο (2012/2096(INI))
43. Πρόταση Ψηφίσματος του Ευρωπαϊκού Κοινοβουλίου της 14ης Μαΐου 2013, σχετικά με τον ρόλο της ΕΕ στην προώθηση μιας ευρύτερης διατλαντικής εταιρικής σχέσης 2012/2287(INI)
44. Απόφαση του Ευρωπαϊκού Συμβουλίου της 3ης Δεκεμβρίου 2013 για τον καθορισμό του ειδικού προγράμματος υλοποίησης του προγράμματος Ορίζων 2020 – Πρόγραμμα-πλαίσιο για την έρευνα και την καινοτομία (2014

– 2020) και για την κατάργηση των αποφάσεων 2006/971/ΕΚ, 2006/972/ΕΚ, 2006/973/ΕΚ, 2006/974/ΕΚ και 2006/975/ΕΚ

45. Ευρωπαϊκή Επιτροπή, HORIZON 2020 εν συντομία, Το Πρόγραμμα Πλαίσιο της ΕΕ για την Έρευνα και την Καινοτομία, Γενική Διεύθυνση Έρευνας και Καινοτομίας 2014).
46. Minister for the Cabinet Office and Paymaster General. The UK cyber security strategy: protecting and promoting the UK in a digital world. Cited 12 February 2012. Retrieved from: http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_UK_Cyber_Security_Strategy.pdf; 2011
47. Preimesberger, Chris (May 28, 2014). "DDoS Attack Volume Escalates as New Methods Emerge". eWeek
48. Chenda Ngak, 'Are Facebook, Twitter, Apple, New York Times, NBC hacks a sign of things to come?' (22 February 2012) - http://www.cbsnews.com/8301-205_162-57570805/are-facebook-twitter-apple-new-york-times-nbc-hacks-a-sign-of-things-to-come/

Επιστημονικο Λεξιλόγιο

Adware (Διαφημιστικό λογισμικό): Adware μπορεί να σημαίνει το λογισμικό που δημιουργεί αυτόματα διαφημίσεις σε ένα πρόγραμμα που κατά τα άλλα είναι δωρεάν, όπως ένα online video game. Αλλά σε αυτό το πλαίσιο, πιο συχνά σημαίνει ένα είδος spyware (κατασκοπευτικό λογισμικό) που παρακολουθεί τις συνήθειες σου στην περιήγηση στο διαδίκτυο συγκεκαλυμμένα, για να δημιουργήσει στοχευμένες διαφημίσεις.

Anonymous (Ανώνυμοι): Ως μη-ιεραρχική hacktivist (όρος που προέρχεται από τις λέξεις hacker και activist, δηλ. Ένας χάκερ ακτιβιστής) συλλογικότητα, οι Anonymous χρησιμοποιούν τις hacking (και, αναμφισβήτητα, τις cracking) τεχνικές για να καταγράψουν την πολιτική τους διαμαρτυρία σε εκστρατείες γνωστές ως "#ops". Περισσότερο γνωστοί για τις κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών (distributed denial of services, DDoS), στις παλαιότερες δραστηριότητες τους έχουν συμπεριλάβει επιθέσεις εναντίον της Εκκλησίας της Σαηεντολογίας, στην Visa, στο Paypal, και σε άλλους, οι οποίοι απέσυραν τις παροχή των υπηρεσιών τους από το WikiLeaks του Julian Assange, μετά από την κίνησή του τελευταίου να δημοσιοποιήσει απόρρητα/διαβαθμισμένα έγγραφα πολέμου στο site Wikileaks, την πρόσκληση στην εκστρατεία τους #OpTunisia για την υποστήριξη της Αραβικής Άνοιξης (Arab Spring), και μια εκστρατεία που έριξε την ιστοσελίδα της Westboro Baptist Church. Οι #Ops τους συνήθως "μαρκάρονται" με την κυκλοφορία ενός βίντεο-προκήρυξης όπου ένας παρουσιαστής φορώντας την μάσκα του Guy Fawkes αναφέρει κείμενο χρησιμοποιώντας έναν υπολογιστή για να παραλλάξει την φωνή του. Στις ομάδες παρακλάδια τους περιλαμβάνονται οι AntiSec και οι LulzSec.

AntiSec: Μια Anonymous ξεχωριστή ομάδα, οι AntiSec είναι γνωστοί από το hack στην επιχείρηση ασφαλείας Stratfor, κοινοποίησαν τους αριθμούς πιστωτικών καρτών και τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που πήραν από το site της εταιρείας. Ο Jeremy Hammond συνελήφθη με την κατηγορία ότι εκτελεούσε Anti-Sec δραστηριότητες κάτω από το ψευδώνυμο sup_g.

Back door (κερκόπορτα): Μια back door (πίσω πόρτα/κερκόπορτα), ή trap door (καταπακτή), είναι μια κρυφή είσοδος σε μια υπολογιστική συσκευή ή στο λογισμικό, που παρακάμπτει τα μέτρα ασφαλείας, όπως τα logins και την προστασία με κωδικό πρόσβασης. Κάποιοι έχουν ισχυριστεί ότι οι κατασκευαστές (λογισμικού/υλισμικού) έχουν συνεργαστεί με τις υπηρεσίες πληροφοριών της κυβέρνησης (των ΗΠΑ και άλλων χωρών) για την κατασκευή κερκόπορτων στα προϊόντα τους. Τα Malware σχεδιάζονται, συχνά, για να εκμεταλλευτούν αυτές τις πίσω πόρτες ή τις ευπάθειες στα συστήματα Η/Υ.

Black hat (Μαύρο καπέλο): Οι μαύρο καπέλο hackers είναι εκείνοι που επιδίδονται στο hacking για παράνομους σκοπούς, συχνά για ίδιο οικονομικό κέρδος, αλλά και για την φήμη. Τα hacks τους (και τα crack τους) έχουν ως αποτέλεσμα αναστάτωση και απώλεια τόσο για τους ιδιοκτήτες των συστημάτων που χτυπήθηκαν, όσο και για τους χρήστες αυτών των συστημάτων.

Bot (ρομπότ σε σύντμηση, ro-bot): Ένα πρόγραμμα που αυτοματοποιεί συνήθως μια απλή ενέργεια, έτσι ώστε να μπορεί να γίνει κατ' επανάληψη σε ένα πολύ υψηλότερο ποσοστό και για μια πιο παρατεταμένη περίοδο από ότι θα έκανε ή θα μπορούσε να κάνει ένας άνθρωπος χειριστής. Όπως τα περισσότερα πράγματα στον κόσμο του hacking, τα bots είναι, από μόνα τους, καλοήθη και χρησιμοποιούνται για μια σειρά από νόμιμους σκοπούς, όπως την online διανομή περιεχομένου. Ωστόσο, συχνά χρησιμοποιούνται σε συνδυασμό με το cracking, και από αυτή την χρήση τους είναι που προέρχεται η δημόσια κακή τους φήμη. Τα Bots μπορεί να χρησιμοποιηθούν, για παράδειγμα, για να γίνουν κλήσεις περιεχομένου που συνθέτουν επιθέσεις άρνησης παροχής υπηρεσίας (denial of service, DoS). Το Bot είναι επίσης ένας όρος που χρησιμοποιείται για να δηλώσει το hacking μεμονωμένων υπολογιστών που συνθέτουν ένα botnet (δίκτυο από bots).

Botnet (δίκτυο από bots): Ένα botnet είναι μια ομάδα υπολογιστών που ελέγχονται εν αγνοία των ιδιοκτητών τους και χρησιμοποιούνται για την αποστολή spam ή για να κάνουν επιθέσεις άρνησης παροχής υπηρεσίας. Χρησιμοποιείται malware για να χακαριστούν οι μεμονωμένοι υπολογιστές, επίσης γνωστοί και ως "zombies" (ζόμπι), για να στέλνονται οι κατευθύνσεις μέσα από αυτά. Είναι περισσότερο γνωστό από τα μεγάλα δίκτυα spam, που συχνά εδρεύουν στην πρώην Σοβιετική Ένωση.

Brute force attack (επίθεση ωμής βίας): Επίσης γνωστή ως μια εξαντλητική αναζήτηση κλειδιού, μια επίθεση ωμής βίας είναι μια αυτοματοποιημένη αναζήτηση για κάθε δυνατό κωδικό πρόσβασης σε ένα σύστημα. Είναι μια αναποτελεσματική μέθοδος hacking σε σύγκριση με τις άλλες μεθόδους, όπως πχ. το phishing. Χρησιμοποιείται συνήθως όταν δεν υπάρχει άλλη εναλλακτική λύση. Η διαδικασία μπορεί να γίνει μικρότερη σε διάρκεια, από την επικέντρωση της επίθεσης σε στοιχεία κωδικού που ενδέχεται να χρησιμοποιούνται από ένα συγκεκριμένο σύστημα.

Clone phishing (κλώνος ψάρεμα): Το clone phishing είναι η τροποποίηση του υφιστάμενου, νόμιμου ηλεκτρονικού ταχυδρομείου με έναν ψεύτικο σύνδεσμο για να εξαπατήσει τον παραλήπτη του και να παρέχει έτσι προσωπικές πληροφορίες, νομίζοντας ότι απαντά σε κάποιον έγκυρο αποστολέα (πχ. στην τράπεζά του).

Code: Το code (κώδικας) είναι οι αναγνώσιμες εντολές από την μηχανή, που συνήθως βασίζονται σε ένα κείμενο οδηγιών που διέπουν μια συσκευή ή ένα πρόγραμμα. Η αλλαγή του κώδικα μπορεί να αλλάξει τη συμπεριφορά της συσκευής ή του προγράμματος.

Compiler: Ένας compiler (μεταγλωττιστής) είναι ένα πρόγραμμα που μεταφράζει τη γλώσσα υψηλού επιπέδου (πηγαίος κώδικας σε μια γλώσσα προγραμματισμού) σε εκτελέσιμη γλώσσα μηχανής. Οι compilers μερικές φορές ξαναγράφονται για να δημιουργήσουν μια πίσω πόρτα χωρίς να αλλάξουν τον κατά τα άλλα καλοήθη πηγαίο κώδικα ενός προγράμματος.

Cookie (μπισκοτάκι ή τρίμμα/ψίχουλο, θυμίζει λίγο τα ψίχουλα που άφηνε ο κοντορεβυθούλης στο δρόμο του μέσα στο δάσος για μπορέσει να ξαναβρεί τον δρόμο της επιστροφής πίσω στο σπίτι του): Τα cookies είναι αρχεία κειμένου που αποστέλλονται από το πρόγραμμα περιήγησης στο web σε έναν διακομιστή, συνήθως για να προσαρμοστούν οι πληροφορίες από μια ιστοσελίδα. Τα cookies παράγονται από τις ιστοσελίδες για να μπορούν να σε "θυμηθούν" όταν ξανασπιστρέψεις να τις επισκεφτείς κάποια στιγμή στο μέλλον. Χρησιμοποιούνται αρκετές φορές ως φορείς malware αλλά με πολύ περιορισμένες δυνατότητες (είναι απλά αρχεία κειμένου με σχετικά μικρό μέγεθος και εύκολα γίνεται αντιληπτό αν έχει "κολλήσει" κάτι ξένο πάνω τους. Παρόλλα αυτά είναι ένα είδος οικειοθελούς παρακολούθησης.

Cracking (ρηγμάτωση/σπάσιμο): Διαδικασία για να crack (να "σπάσεις" ή να παραβιάσεις και να μπεις μέσα σε) ένα ασφαλές σύστημα ηλεκτρονικού υπολογιστή, συχνά για να κάνεις ζημιά ή να κερδίσεις οικονομικές απολαβές, αν και μερικές φορές μπορεί να είναι απλά για μια πολιτική διαμαρτυρία.
* **Password cracking**

* **Software cracking**

Denial of service attack (DoS): Το DoS (επίθεση για την άρνηση παροχής υπηρεσίας) χρησιμοποιείται εναντίον ενός website ή ενός δικτύου υπολογιστών για να γίνουν προσωρινά άχρηστα (να μην απαντούν). Αυτό συχνά επιτυγχάνεται με την αποστολή τόσο πολλών αιτημάτων για την εμφάνιση περιεχομένου από μια ιστοσελίδα που έχει ως συνέπεια την υπερφόρτωση του server και το πάγωμα του (λόγω υπερφόρτωσης με εργασίες). Τα αιτήματα περιεχομένου είναι οι οδηγίες που αποστέλλονται, για παράδειγμα από τον browser σας, σε μια ιστοσελίδα για να σας επιτραπεί να δείτε την εν λόγω ιστοσελίδα. Κάποιοι έχουν περιγράψει τέτοιες επιθέσεις ως το ισοδύναμο για το internet, όπως γίνεται στις διαδηλώσεις στους δρόμους (σταματά η κυκλοφορία, δεν λειτουργούν τα καταστήματα, κτλ.) και ορισμένες ομάδες, όπως οι Anonymous, τις χρησιμοποιούν συχνά ως ένα εργαλείο διαμαρτυρίας.

Distributed denial of service attack (κατανεμημένη επίθεση άρνησης υπηρεσίας), DDoS: Είναι μια DoS επίθεση χρησιμοποιώντας μια σειρά από διαφορετικές μηχανές. Αυτό μπορεί να επιτευχθεί με την σπορά σε διαφορετικές μηχανές (υπολογιστές) ενός Trojan και τη δημιουργία ενός botnet, ή όπως είναι και η περίπτωση σε μια σειρά από επιθέσεις των Anonymous, χρησιμοποιώντας τους υπολογιστές εθελοντών.

Doxing (φακέλωμα/ξεσκέπασμα): Ανακαλύπτοντας και δημοσιεύοντας την ταυτότητα ενός κατά τα άλλα ανώνυμου χρήστη του διαδικτύου με τον εντοπισμό των online δημόσια διαθέσιμων λογαριασμών του, των μεταδεδομένων και των εγγράφων του, όπως λογαριασμούς ηλεκτρονικού ταχυδρομείου, καθώς και από hacking, stalking (καταδίωξη) και harassing (παρενόχληση).

Firewall (τοίχος φωτιάς/προστασίας): ένα σύστημα που χρησιμοποιεί το υλισμικό, το λογισμικό, ή και τα δύο, για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα ή σε ένα μηχάνημα.

Gray hat (Γκρι καπέλο): Ακριβώς όπως γίνεται γενικά στην ζωή, το hacking είναι συχνά όλο και λιγότερο μαύρο ή άσπρο, τις περισσότερες φορές είναι γκρι. Ο όρος gray hat hacker αντανακλά αυτή την πραγματικότητα. Ένας gray hat hacker θα παραβεί τον νόμο για την επιδίωξη ενός hack, αλλά δεν το κάνει κακόβουλα ή για προσωπικό κέρδος. Θα λέγαμε ότι είναι κάτι σαν το "ο καλός σκοπός αγιάζει τα μέσα". Πολλοί θα υποστήριζαν ότι οι Anonymous είναι gray hats.

Hacking (χακάρισμα): Hacking είναι η "δημιουργική χειραγώγηση" του κώδικα, διακρίνεται, έστω και άμορφα, από τον προγραμματισμό, με επίκεντρο τη χειραγώγηση του υπάρχοντος κώδικα στις συσκευές ή στο λογισμικό για τα οποία ο κώδικας έχει ήδη γραφτεί. Μεταφορικά επεκτείνετε στην πολιτική μηχανική για την χειραγώγηση του κώδικα για να επηρεαστεί με αλλαγές. Πολλοί προτιμούν να χρησιμοποιούν τον όρο craking για να περιγράψουν το hacking σε μια μηχανή ή σε ένα πρόγραμμα χωρίς άδεια. Οι hackers, μερικές φορές, χωρίζονται σε white hat, black hat και gray hat hackers, με τα όρια ανάμεσα σε αυτούς τους διαχωρισμούς πολλές φορές να είναι ασαφή.

Hacktivist (από το hacker και το acrivist): Ένας hacker, που οι στόχοι του είναι κοινωνικοί ή πολιτικοί. Για παράδειγμα, από την υποβολή αναφορών-καταγγελιών στο διαδίκτυο ανώνυμα για μια χώρα που προσβάλλει την ελευθερία του λόγου, έως το να ξεκινήσει μια καμπάνια με DDoS επιθέσεις σε μια εταιρεία της οποίας πχ. ο Διευθύνων Σύμβουλος έχει δημοσιεύσει απαράδεκτες δηλώσεις. Δεν πρέπει να συγχέεται με το slacktivism (ακτιβισμός του καναπέ), το οποίο αναφέρεται σε ακτιβισμό με το "πληκτρολόγιο", όπου ο υποστηρικτής/ακτιβιστής δεν κάνει τίποτα για την επίτευξη των στόχων μιας

κοινωνικής ή πολιτικής εκστρατείας, παρά μόνο δηλώνει την υποστήριξή του online, για παράδειγμα, με ένα like σε μια σελίδα στο Facebook.

Hash: Το hash είναι ένας αριθμός που δημιουργείται από έναν αλγόριθμο με μια ακολουθία χαρακτήρων σε ένα μήνυμα ή σε κάποια άλλη συμβολοσειρά. Σε ένα σύστημα επικοινωνιών που χρησιμοποιούνται hashes, ο αποστολέας ενός μηνύματος ή αρχείου μπορεί να δημιουργήσει ένα hash, να κρυπτογραφήσει με αυτό το μήνυμα ή το αρχείο, και να το στείλει σε έναν παραλήπτη. Ο παραλήπτης με την σειρά του, παράγει ένα άλλο hash και αν το παραγόμενο hash είναι ίδιο με το hash του αποστολέα μπορεί με αυτό να αποκρυπτογραφήσει το μήνυμα ή το αρχείο που παρέλαβε. Αν το hash που έφτιαξε ο παραλήπτης είναι ίδιο με το hash που έβαλε ο αποστολέας μαζί με το μήνυμα ή το αρχείο, είναι σχεδόν βέβαιο ότι δεν έχει γίνει αλλοίωση στο μήνυμα ή στο αρχείο κατά την μεταφορά του από τον έναν στον άλλον.

IP: διεύθυνση πρωτοκόλλου Internet. Είναι το διακριτικό μοναδικό αριθμητικό αποτύπωμα που κάθε συσκευή έχει όταν είναι συνδεδεμένη με ένα δίκτυο και χρησιμοποιεί το πρωτόκολλο του διαδικτύου. Αν έχετε την IP μιας συσκευής μπορείτε να αναγνωρίσετε συχνά και το άτομο που την χρησιμοποιεί (ταυτοποίηση), και να παρακολουθεί έτσι τη δραστηριότητά του, και να ανακαλύψετε και την θέση του (γεωγραφική ή μέσα στο δίκτυο). Οι διευθύνσεις αυτές κατανέμονται από τα περιφερειακά μητρώα του ίντερνετ της IANA (**the Internet Assigned Numbers Authority(link is external)**) . Οι crackers χρησιμοποιούν τις IP διευθύνσεις για να ανακαλύψουν την ταυτότητα/θέση μιας συσκευής, παρακολουθώντας την κυκλοφορία των δεδομένων που γίνεται μέσω αυτών.

IRC: Ιντερνετικό Πρωτόκολλο Συνομιλίας, είναι ένα πρωτόκολλο που χρησιμοποιείται και από τους δύο συμμετέχοντες για μια one-on-one (ή και άλλοι συνδυασμοί) συνομιλία. Συχνά χρησιμοποιείται από τους χάκερ για να επικοινωνούν ή να μοιράζονται αρχεία μεταξύ τους. Επειδή είναι συνήθως χωρίς κρυπτογράφηση, οι hackers χρησιμοποιούν μερικές φορές sniffers πακέτων για να κλέψουν προσωπικά δεδομένα από τέτοιες συνομιλίες.

Keystroke logging (καταγραφή πληκτρολόγησης): η καταγραφή της πληκτρολόγησης είναι η παρακολούθηση των πλήκτρων που πιέζονται σε έναν υπολογιστή (ή των σημείων επαφής σε οθόνες αφής touchscreen) από τον χρήστη. Είναι, απλά, η καταγραφή της πληκτρολόγησης από έναν άνθρωπο σε μια συσκευή. Χρησιμοποιείται από gray ή black hat hackers για να καταγράψουν τα αναγνωριστικά πρόσβασης (login username) και τους κωδικούς πρόσβασης (password). Τα keyloggers συνήθως τοποθετούνται σε μια συσκευή μέσω κάποιου Trojan που εισβάλουν με κάποιο phishing email.

Logic bomb (Λογική βόμβα): Είναι ένας ιός που μπαίνει σε ένα σύστημα και που ενεργοποιεί μια κακόβουλη ενέργεια, όταν πληρούνται ορισμένες προϋποθέσεις. Η πιο κοινή εκδοχή είναι η time bomb (ωρολογιακή βόμβα).

LulzSec: Οι LulzSec είναι ένα παρακλάδι των Anonymous. Από τις πιο γνωστές τους ενέργειες, ήταν το hacking σε πληροφορίες χρηστών από την ιστοσελίδα της Sony Pictures και για το μη-επιβεβαιωμένο κλείσιμο της ιστοσελίδας της CIA με επίθεση DDoS. Ο πιο γνωστός LulzSec είναι, ο Hector Xavier Monsegur, γνωστός και ως "Sabu", ένας χάκερ που έγινε πληροφοριοδότης του FBI, του οποίου οι πληροφορίες οδήγησαν στη σύλληψη τεσσάρων άλλων μελών των LulzSec. Αντιμετωπίζει το ενδεχόμενο μιας μακράς φυλάκισης, παρά τη συνεργασία του με τις αρχές.

Malware (από malicious και το software): Ένα πρόγραμμα σχεδιασμένο ως λογισμικό για να παραβιάσει, να προκαλέσει βλάβη ή για να κλαπούν πληροφορίες από μια συσκευή ή ένα σύστημα. Παραδείγματα malware είναι τα spyware, τα adware, τα rootkits, οι ιοί, τα keyloggers, και άλλα πολλά. Το λογισμικό μπορεί να εισβάλει με μια σειρά από τρόπους, από ιστοσελίδες-δόλωμα και spam μέχρι και USB drives, κά.

Master: Ο υπολογιστής που ελέγχει ένα δίκτυο botnet, αλλά δεν ελέγχεται από άλλες συσκευές του δικτύου. Είναι επίσης ο υπολογιστής στον οποίο όλες οι άλλες συσκευές, αναφέρουν και αποστέλλουν πληροφορίες, όπως πχ. αριθμοί πιστωτικών καρτών, για περαιτέρω επεξεργασία. Ο έλεγχος της master συσκευής από τον χρήστη του γίνεται συνήθως μέσω IRC.

NSA: Η Εθνική Υπηρεσία Ασφαλείας των ΗΠΑ, είναι η ομάδα των αμερικανικών μυστικών υπηρεσιών που είναι αφιερωμένη και αφοσιωμένη στην υποκλοπή και την ανάλυση δεδομένων, συγκεκριμένα ψηφιακών δεδομένων. Αν και δεν είναι η μόνη υπηρεσία πληροφοριών των ΗΠΑ και του υπόλοιπου κόσμου, εκτελεί μαζική παρακολούθηση στις επικοινωνίες και χάρη στον πρώην εργαζόμενο, αναλυτής σε ανάδοχη εταιρία, στην NSA, τον Edward Snowden που έκανε διαρροή διαβαθμισμένων εγγράφων, η υπηρεσία έχει γίνει η πιο διάσημη και πλέον στιγματισμένη.

Payload (Ωφέλιμο φορτίο): Το φορτίο της μετάδοσης δεδομένων καλείται ωφέλιμο φορτίο. Σε κάποιο black hat hacking, αναφέρεται στο τμήμα του ιού που θα καταφέρει να πετύχει με την δράση του, την καταστροφή δεδομένων, τη συλλογή πληροφοριών ή την παραβίαση του υπολογιστή.

Packet sniffer (αφουγκραστής/υποκλοπέας πακέτων): Τα sniffers είναι προγράμματα που έχουν σχεδιαστεί για τον εντοπισμό και τη σύλληψη ορισμένων τύπων δεδομένων. Τα sniffers πακέτων σχεδιάζονται για την ανίχνευση πακέτων που ταξιδεύουν online στο διαδίκτυο. Τα πακέτα αυτά είναι πακέτα πληροφοριών που ταξιδεύουν στο διαδίκτυο και περιέχουν τη διεύθυνση προορισμού μαζί με το περιεχόμενο. Μπορούν να χρησιμοποιηθούν για να γίνει υποκλοπή των στοιχείων σύνδεσης και των κωδικών πρόσβασης για μια συσκευή ή ένα δίκτυο υπολογιστών.

Phishing (ψάρεμα): η εξαπάτηση κάποιου για να δώσει τα προσωπικά του στοιχεία, και στοιχεία όπως αυτά της σύνδεσης και των κωδικών πρόσβασης, τους αριθμούς πιστωτικών καρτών, και ούτω καθεξής, με τη μίμηση σε νόμιμες εταιρείες, οργανισμούς ή και άτομα online. Το phishing συχνά γίνεται μέσω πλαστών ηλεκτρονικών μηνυμάτων ή συνδέσμους σε παραπλανητικές/παραλλαγμένες ιστοσελίδες (που ο χρήστης νομίζει ότι είναι οι κανονικές).

Remote access (Απομακρυσμένη πρόσβαση): Η απομακρυσμένη πρόσβαση είναι η διαδικασία του να καταφέρετε να πάρετε τον έλεγχο σε έναν άλλο υπολογιστή-στόχο, από τον δικό σας υπολογιστή μέσω ενός δικτύου ή/και του διαδικτύου και να τον χειριστείτε σαν να είσαστε μπροστά του, σαν την λειτουργία της τηλεόρασης με ένα τηλεχειριστήριο. Αποκτώντας απομακρυσμένη πρόσβαση σε έναν υπολογιστή-στόχο μπορείτε να τον χειριστείτε σαν να ήταν δικός σας, σας επιτρέπει επίσης να εκτελέσετε μεταφορά αρχείων μεταξύ των δύο υπολογιστών (στόχος και θύτης).

Rootkit: Ένα rootkit είναι ένα σύνολο προγραμμάτων λογισμικού που χρησιμοποιείται για να αποκτηθεί πρόσβαση σε επίπεδο διαχειριστή (admin) σε ένα σύστημα για την εγκατάσταση malware, ενώ ταυτόχρονα γίνεται και πλήρης απόκρυψη (καμουφλάρισμα) της παραβίασης.

Script kiddie: Ένας υποτιμητικός όρος για τους επίδοξους crakers χωρίς τεχνικές δεξιότητες. Οι script kiddies χρησιμοποιούν προκατασκευασμένα cracking εργαλεία για να επιτεθούν σε συστήματα για να τα παραμορφώσουν, συχνά σε μια προσπάθεια να κερδίσουν πόντους φήμης από τους συνομηλίκους τους.

Social engineering (Κοινωνική μηχανική): Ένας θεματοφύλακας είναι όπως ένας επιστάτης ενώ ένας social engineering είναι όπως ένας απατεώνας. Πολιτική μηχανική είναι για να εξαπατά τους ανθρώπους για να δώσουν τις εμπιστευτικές πληροφορίες τους, όπως τους κωδικούς πρόσβασης στους λογαριασμούς τους. Αν λάβουμε υπόψη τη δυσκολία του να σπάσει μια κρυπτογράφηση των 128-bit με επίθεση brute force, για παράδειγμα, η πολιτική μηχανική αποτελεί ένα αναπόσπαστο στοιχείο του cracking. Τα παραδείγματα τέτοιου τύπου περιλαμβάνουν το phishing και το spear-phishing.

Spam: ανεπιθύμητα και ενοχλητικά (διαφημιστικά συνήθως) μηνύματα ηλεκτρονικού ταχυδρομείου και άλλα ηλεκτρονικά μηνύματα που προσπαθούν να πείσουν τον δέκτη τους για να αγοράσει είτε ένα προϊόν είτε μια υπηρεσία, ή χρησιμοποιούνται με την προοπτική να εξαπατήσουν τον παραλήπτη τους. Οι μεγαλύτερες και πιο κερδοφόρες οργανώσεις spamming συχνά χρησιμοποιούν botnets για να αυξήσουν την ποσότητα των spam που στέλνουν (και ως εκ τούτου και το ποσό των χρημάτων που αυτά θα αποφέρουν).

Spear-phishing: Ένα πιο επικεντρωμένο είδος/τύπος phishing, στοχεύει σε μια μικρότερη ομάδα στόχων, από ένα τμήμα σε μια εταιρεία ή οργανισμό έως και έναν μεμονωμένο άνθρωπο (αν το σκέτο phishing είναι ψάρεμα με δίχτυ, το spear-phishing είναι ψάρεμα με ψαροντούφεκο). [*δες στο: phishing, πιο πάνω*]

Spoofing: Το spoofing σε email, μεταβάλλει την επικεφαλίδα (header) ενός μηνύματος ηλεκτρονικού ταχυδρομείου, έτσι ώστε να φαίνεται ότι προέρχεται από κάπου αλλού. Ένας black hat hacker, για παράδειγμα, θα μπορούσε να μεταβάλει την επικεφαλίδα του ηλεκτρονικού ταχυδρομείου του, ώστε να φαίνεται ότι προέρχεται από την τράπεζά σας. Το IP spoofing είναι η παραλλαγή του spoofing για υπολογιστές, με αυτό τον τρόπο, στέλνεται ένα πακέτο σε έναν υπολογιστή με την IP διεύθυνση να έχει τροποποιηθεί για να μιμηθεί μια άλλη αξιόπιστη IP, με την ελπίδα ότι το πακέτο θα γίνει αποδεκτό και θα επιτρέψει την πρόσβαση από τον αποστολέα στο μηχάνημα-στόχο.

Spyware (από το spy και το software): Το spyware είναι ένα είδος κακόβουλου λογισμικού που έχει προγραμματιστεί για να κρυφτεί μέσα σε έναν υπολογιστή ή σε έναν διακομιστή-στόχο και να στέλνει πληροφορίες πίσω σε έναν κεντρικό διακομιστή, οι πληροφορίες αυτές περιλαμβάνουν στοιχεία όπως όνομα χρήστη και κωδικό πρόσβασης, στοιχεία τραπεζικού λογαριασμού, καθώς και αριθμούς πιστωτικών καρτών.

Syrian Electronic Army (Συριακός Ηλεκτρονικός Στρατός): Ο SEA είναι μια φιλοκυβερνητική ομάδα hacking, είναι πιο γνωστός για την παραμόρφωσή σε υψηλού προφίλ δημοσιεύσεις όπως στο New York Times και στο National Public Radio (και στο The Daily Dot). Πρόσφατα, ο Vice και ο Krebs της Ασφάλειας, έχουν αποκαλύψει πολλά από τα φερόμενα ως μέλη της ομάδας. Επίσης, κάποιοι τους έχουν κατηγορήσει/λοιδορήσει ότι είναι λιγότερο hackers ακόμα και από τα script kiddies.

Time bomb (Ωρολογιακή βόμβα): Ιοί τους οποίους το ωφέλιμο φορτίο (payload) έχει επιτευχθεί μέσα σε ή μετά από, ένα ορισμένο χρονικό διάστημα.

Trojan (Δούρειος Ίππος): Ένα Trojan είναι ένα είδος κακόβουλου λογισμικού που μεταμφιέζεται ως ένα επιθυμητό κομμάτι λογισμικού. Στο πλαίσιο αυτού του καμουφλάζ, θα παρέχει το ωφέλιμο φορτίο του και συνήθως εγκαθιστά μια πίσω πόρτα στο μολυσμένο μηχάνημα.

Virus (Ιός): Αυτοαναπαραγόμενο malware που τοποθετεί αντίγραφα του εαυτού του στο μολυσμένο μηχάνημα. Ένας ιός μπορεί να καταστρέψει ένα σκληρό δίσκο, να υποκλέψει (για λογαριασμό του κατασκευαστή του) πληροφορίες, να κάνει καταγραφή πληκτρολογήσεων, καθώς και πολλές άλλες κακόβουλες δραστηριότητες.

Vulnerability (Ευπάθεια): Ένα αδύναμο σημείο σε λογισμικό ή/και υλισμικό που οι hackers μπορούν να εκμεταλλευτούν για να αποκτήσουν πρόσβαση σε ένα μηχάνημα.

Whaling (Φαλαινοθηρία): Ένα spear-phishing που στοχεύει στην ανώτερη διοίκηση κερδοφόρων εταιρειών (φάλαινες), προφανώς με την ελπίδα ότι η υψηλότερη αξία τους (διασημότητα, πολλά χρήματα) θα έχει ως αποτέλεσμα περισσότερο κέρδος, αν ο cracker είναι στο κυνήγι για το οικονομικό κέρδος ή επειδή θα υπάρξει μεγαλύτερη προβολή που θα εξασφαλίσει σε gray hat hackers περισσότερη δημοσιότητα για αυτά που θέλουν να πετύχουν.

White hat (Λευκό καπέλο): Ένας ηθικός hacker, ο οποίος χρησιμοποιεί τις ικανότητές του στην υπηρεσία του κοινωνικού καλού. Ο όρος μπορεί επίσης να εφαρμοστεί και σε έναν χάκερ ο οποίος βοηθάει μια εταιρεία ή έναν οργανισμό ή γενικά τους χρήστες, εκθέτοντας τρωτά σημεία σε συστήματα, πριν τα αντιληφθούν/εντοπίσουν οι black hat hackers.

Worm (σκουλίκι): Αυτό-αναπαραγώμενο αυτόνομο malware. Ως αυτόνομο δεν αποστέλλει πίσω σε κάποιον master πληροφορίες, και σε αντίθεση με έναν ιό, δεν χρειάζεται να συνδεθεί με ένα υπάρχον πρόγραμμα. Συχνά δεν κάνει κάτι άλλο από βλάβες ή να καταστρέψει τους υπολογιστές που μεταδίδεται. Αλλά μερικές φορές είναι εξοπλισμένο με ωφέλιμο φορτίο, συνήθως αυτό που εγκαθιστά πίσω πόρτες στα μολυσμένα μηχανήματα για να τα κάνει zombies και μέρος κάποιου botnet.

Zero day exploit (Ημέρα μηδέν εκμετάλλευση): Μια επίθεση zero day είναι μια προηγουμένως άγνωστη ευπάθεια σε ένα σύστημα. Η zero day επίθεση είναι η πρώτη χρήση που θα εκμεταλλευτεί κάποια άγνωστη ευπάθεια, από crackers, και αφού δεν ήταν γνωστή, η ευπάθεια από πριν, για να παρθούν τα κατάλληλα μέτρα, η επίθεση έχει και μεγαλύτερο αντίκτυπο/συνέπειες. Πολλές εταιρίες λογισμικού πληρώνουν αμοιβή σε όποιον βρει κάποια ευπάθεια στα συστήματά τους και τους την αναφέρει ώστε να κάνουν τις απαραίτητες διορθώσεις πριν εκδηλωθεί κάποια επίθεση που θα μπορούσε να την εκμεταλλευτεί, με τις όποιες συνέπειες θα είχε κάτι τέτοιο.

Ακεραιότητα (integrity): ονομάζεται η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας.

Ανάνηψη (recovery): ονομάζεται η αποκατάσταση ενός πληροφοριακού συστήματος σε μια συγκεκριμένη φάση της λειτουργίας του, η οποία διακόπηκε εξαιτίας κάποιου γεγονότος

Ασφάλεια (security): ονομάζεται η προστασία της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας.

Ασφάλεια πληροφορίας (information security): ονομάζεται ο συνδυασμός εμπιστευτικότητας, συνέπειας, ακεραιότητας και διαθεσιμότητας μιας πληροφορίας.

Αυθεντικότητα (authenticity): ονομάζεται η αποφυγή κάποιας ατελούς ή ανακριβούς τροποποίησης μιας πληροφορίας από ένα εξουσιοδοτημένο χρήστη.

Αυθεντικοποίηση χρήστη (user authentication): ονομάζεται η διαδικασία που αποσκοπεί στην επιβεβαίωση της ταυτότητας ενός χρήστη.

Διαθεσιμότητα (availability): ονομάζεται η αποφυγή της αδικαιολόγητης καθυστέρησης ενός εξουσιοδοτημένου χρήστη να αποκτήσει προσπέλαση σε πληροφορίες ή υπολογιστικούς πόρους.

Διαθεσιμότητα πληροφορίας (information availability): ονομάζεται η αποφυγή της προσωρινής ή μόνιμης παρακράτησης μιας πληροφορίας από τους χρήστες που έχουν δικαίωμα να τη χρησιμοποιούν.

Εγκυρότητα (validity): ονομάζεται η εξασφάλιση πλήρους ακρίβειας και πληρότητας μιας πληροφορίας.

Εμπιστευτικότητα (confidentiality): ονομάζεται η αποφυγή της αποκάλυψης μιας πληροφορίας χωρίς την άδεια του ιδιοκτήτη της.

Εφαρμογή (application): ονομάζεται ένα σύνολο πληροφοριών, λογισμικού και διαδικασιών, σχεδιασμένων προκειμένου να εκπληρώσουν ένα συγκεκριμένο σύνολο στόχων.

Εφεδρικό αντίγραφο πληροφοριών (information backup): ονομάζεται ένα αντίγραφο των πληροφοριών που μπορεί να χρησιμοποιηθεί – μεταξύ άλλων – και για λόγους ανάνηψης.

Παραβίαση (violation): ονομάζεται ένα γεγονός κατά τη διάρκεια του οποίου έχει παραβιαστεί το χαρακτηριστικό της αυθεντικότητας ή της διαθεσιμότητας ή της εμπιστευτικότητας ή της ακεραιότητας ή της συνέπειας.

Πληροφοριακό Σύστημα (information system): ένα υπολογιστικό σύστημα μαζί με τις πληροφορίες τις οποίες επεξεργάζεται

Προσπέλαση (access): ονομάζεται η δυνατότητα χρήσης πληροφοριών ή υπολογιστικών πόρων ενός πληροφοριακού συστήματος.

Προσπέλαση πληροφορίας (information access): ονομάζεται η δυνατότητα χρήσης συγκεκριμένων πληροφοριών από ένα πληροφοριακό σύστημα.

Ρήγμα ασφάλειας (breach of security): ονομάζεται η αποκάλυψη, μετατροπή ή παρακράτηση μιας πληροφορίας χωρίς εξουσιοδότηση.

Συνθηματικό (password): ονομάζεται μια μυστική συμβολοσειρά που χρησιμοποιείται για την αυθεντικοποίηση ενός χρήστη.

Ταυτοποίηση χρήστη (user identification): ονομάζεται η διαδικασία με την οποία ένα υπολογιστικό σύστημα αναγνωρίζει ένα χρήστη

Υπηρεσία (service): ονομάζεται κάθε σύνολο λειτουργιών (functionalities) που παρέχονται σε κάποιο χρήστη από ένα υπολογιστικό σύστημα.

Υπολογιστικό συγκρότημα (IT assembly): ονομάζεται ένα σύνολο λογισμικού και υλικού ή τηλεπικοινωνιακού ή άλλου σχετικού εξοπλισμού, το οποίο χρησιμοποιείται προκειμένου να επεξεργασθεί πληροφορίες

Υπολογιστικό σύστημα (IT system): ονομάζεται ένα συγκεκριμένο υπολογιστικό συγκρότημα, το οποίο είναι εγκατεστημένο σε συγκεκριμένες τοποθεσίες, πλαισιώνεται από συγκεκριμένο επιχειρησιακό περιβάλλον και αποβλέπει στην εκπλήρωση συγκεκριμένων στόχων

Χρήστης (user): ονομάζεται μια οντότητα η οποία αξιοποιεί ένα μέρος ή το σύνολο ενός Πληροφοριακού Συστήματος.