ΟΔΗΓΟΣ ΑΣΦΑΛΙΣΗΣ CYBER

BETA

ΕΝΩΣΗ ΑΣΦΑΛΙΣΤΙΚΩΝ ΕΤΑΙΡΙΩΝ ΕΛΛΑΔΟΣ

Αποποίηση ευθυνών – Disclaimer

Οι πληροφορίες που περιέχονται στο παρόν και οι δηλώσεις που εκφράζονται είναι γενικής φύσης και δεν προορίζονται να αντιμετωπίσουν τις περιστάσεις οποιουδήποτε συγκεκριμένου ατόμου ή οντότητας. Παρόλο που προσπαθούμε να παρέχουμε ακριβείς και έγκαιρες πληροφορίες και να χρησιμοποιούμε πηγές που θεωρούμε αξιόπιστες, δεν υπάρχει εγγύηση ότι αυτές οι πληροφορίες είναι ακριβείς κατά την ημερομηνία παραλαβής τους ή ότι θα συνεχίσουν να είναι ακριβείς στο μέλλον. Κανείς δεν πρέπει να ενεργεί βάσει αυτών των πληροφοριών χωρίς κατάλληλη επαγγελματική συμβουλή μετά από ενδελεχή εξέταση της συγκεκριμένης κατάστασης.

Όλες οι περιγραφές & οι περιλήψεις που αφορούν ασφαλιστικές καλύψεις προορίζονται μόνο για γενικούς ενημερωτικούς σκοπούς και δεν τροποποιούν ή επηρεάζουν τους όρους / προϋποθέσεις/ εξαιρέσεις οποιουδήποτε ασφαλιστηρίου συμβολαίου. Οι ασφαλιστικές καλύψεις διέπονται αποκλειστικά και μόνο από τους όρους / προϋποθέσεις/ εξαιρέσεις της εκάστοτε συναφθείσας μεταξύ ασφαλιστή και ασφαλισμένου ασφαλιστικής σύμβασης.

Περιεχόμενα

ΠΡΟΛΟΓΟΣ

CYBER RISKS: Πρόκληση και Ευκαιρία για την Ασφαλιστική Αγορά

1. Το 2020 αποτέλεσε χρονιά σταθμό για τον ψηφιακό μετασχηματισμό κρατών, δημόσιων οργανισμών και επιχειρήσεων. Η εμφάνιση της πανδημίας του κορονοϊού COVID-19 επιτάχυνε ραγδαία τις εξελίξεις σε παγκόσμιο επίπεδο στον εδώ και καιρό δυναμικά αναπτυσσόμενο τομέα της ψηφιακής τεχνολογίας. Σε όλο τον κόσμο δημόσιοι οργανισμοί, επιχειρήσεις, μικρές και μεγάλες, συμπεριλαμβανομένων των ασφαλιστικών επιχειρήσεων, αναγκάστηκαν να υιοθετήσουν ταχύτατα την απομακρυσμένη εργασία σε μια προσπάθεια να συνδράμουν στην επιβράδυνση της εξάπλωσης του COVID-19 και να προστατεύσουν τους εργαζόμενους και τους πελάτες τους βασιζόμενοι σχεδόν αποκλειστικά σε ψηφιακές τεχνολογίες προκειμένου να παραμείνουν σε επαφή και να συνεχίσουν τη λειτουργία τους.

Η αυξανόμενη εξάρτηση από τις ψηφιακές τεχνολογίες οδήγησε αναπόφευκτα σε αυξανόμενους κινδύνους ψηφιακής ασφάλειας και σε ανάλογη αύξηση του ηλεκτρονικού εγκλήματος.

2. Στις 20 Οκτωβρίου 2020, ο ENISA, ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια στον Κυβερνοχώρο (www.enisa.europa.eu) δημοσίευσε την Έκθεση «Cyber Espionage - Threat Landscape 2020», όπου περιγράφει τις πιο πρόσφατες τάσεις που σχετίζονται με επιθέσεις κατασκοπείας στον κυβερνοχώρο και παρέχει ολοκληρωμένη ανάλυση των 15 κορυφαίων κυβερνοαπειλών που αντιμετωπίστηκαν σε παγκόσμιο επίπεδο μεταξύ Ιανουαρίου 2019 και Απριλίου 2020. Η Έκθεση προσδιορίζει την επίθεση με κακόβουλο λογισμικό ως την νούμερο ένα απειλή στον κυβερνοχώρο για την Ευρωπαϊκή Ένωση, ενώ αυξανόμενη τάση παρουσιάζουν το ηλεκτρονικό ψάρεμα, η κλοπή ταυτότητας και το ransomware. Το κορυφαίο κίνητρο των εγκληματιών του κυβερνοχώρου παραμένει η απόκτηση παράνομων εσόδων. Η Έκθεση διαπιστώνει επίσης ότι το περιβάλλον COVID-19 τροφοδοτεί επιθέσεις σε σπίτια, επιχειρήσεις, κυβερνήσεις και κρίσιμες υποδομές. Η ψηφιοποίηση όλων των διαδικασιών και η αποδυνάμωση των υπαρχόντων μέτρων ασφάλειας στον κυβερνοχώρο μέσω αλλαγών στα πρότυπα εργασίας και υποδομής που προκαλούνται από την πανδημία COVID-19 δημιουργεί ευκαιρίες για εξατομικευμένες επιθέσεις στους ιδιαίτερα «έξυπνους» εγκληματίες του κυβερνοχώρου με τη χρήση προηγμένων μεθόδων και τεχνικών. Η Έκθεση προειδοποιεί ότι υπάρχει μακρύς δρόμος για την επίτευξη ενός πιο ασφαλούς ψηφιακού περιβάλλοντος.

Κανείς δεν πρέπει να θεωρεί τον εαυτό του ασφαλή. Η καλύτερη αντίδραση είναι η συνειδητοποίηση του κινδύνου και η έγκαιρη διαχείρισή του.

3. Όλα αυτά εμφανίζονται σε μία εποχή που η ασφαλιστική αγορά και οι υπεύθυνοι χάραξης της ευρωπαϊκής πολιτικής είχαν ήδη εντείνει τις προσπάθειές τους για να αντλήσουν οφέλη από την αύξηση της ψηφιοποίησης, περιορίζοντας κατά το δυνατόν τους αναδυόμενους νέους κινδύνους.

Οι υπεύθυνοι χάραξης πολιτικής της Ευρωπαϊκής Ένωσης έχουν δεσμευτεί να συνθέσουν και να ενισχύσουν τους διάσπαρτους νομοθετικούς κανόνες που ισχύουν στην Ευρωπαϊκή

Ένωση για την ασφάλεια στον κυβερνοχώρο, δίδοντας ιδιαίτερη έμφαση στην ενίσχυση της «ψηφιακής επιχειρησιακής ανθεκτικότητας» του χρηματοπιστωτικού τομέα, ο οποίος αναμένεται να βρεθεί στο επίκεντρο των κυβερνοεπιθέσεων. Οι διαβουλεύσεις και οι πρωτοβουλίες για τη διαμόρφωση του κατάλληλου κανονιστικού πλαισίου για την ενίσχυση της ψηφιακής ασφάλειας και ανθεκτικότητας των ευρωπαϊκών επιχειρήσεων και οργανισμών είναι συνεχείς. Άλλωστε το περιβάλλον της ψηφιακής τεχνολογίας είναι συνεχώς εξελισσόμενο και η διασφάλιση της κυβερνοασφάλειας απαιτεί επαγρύπνηση και συνεχή προσπάθεια.

4. Η **ασφαλιστική βιομηχανία κατέχει μια μοναδική θέση** σε αυτή την προσπάθεια ενίσχυσης της ψηφιακής ανθεκτικότητας της Ευρωπαϊκής Ένωσης, μια και **ως τομέας** αποτελεί **στόχο κυβερνοεπιθέσεων** και επομένως **πρέπει να ενισχύσει την ανθεκτικότητά του,** συγχρόνως όμως **ως δραστηριότητα** είναι αυτή που **θα προσφέρει προστασία** σε άλλες επιχειρήσεις μέσω μιας **σειράς προϊόντων ασφάλισης** κατά των κινδύνων του κυβερνοχώρου.

   Η **ασφάλιση κατά των κινδύνων του κυβερνοχώρου** διαδραματίζει **καθοριστικό ρόλο** στην προσπάθεια μικρών και μεγάλων επιχειρήσεων να ενισχύσουν την ανθεκτικότητά τους στον κυβερνοχώρο, προσφέροντας πολλές διαφορετικές υπηρεσίες, **τόσο πριν όσο και μετά από ένα περιστατικό κυβερνοεπίθεσης.** Η προστασία που παρέχει η ασφάλιση έχει δύο όψεις :

   - Οι ασφαλιστές διαδραματίζουν αποφασιστικό ρόλο **στη λήψη μέτρων πρόληψης**, συνδράμοντας την ασφαλιζόμενη επιχείρηση να αντιληφθεί τα τρωτά της σημεία και την έκθεσή της στον κίνδυνο αξιολογώντας και ενισχύοντας την ψηφιακή ανθεκτικότητά της.

   - Και **εάν η απειλή γίνει πραγματικότητα**, η ασφάλιση προσφέρει **δίχτυ ασφαλείας** στην επιχείρηση βοηθώντας την να αντιμετωπίσει αποτελεσματικά τις οικονομικές επιπτώσεις της κρίσης, **όχι μόνη της, αλλά με την πολύτιμη συμβολή του ασφαλιστή της.**

   Η πανδημία επιβεβαίωσε τη σημασία της ανθεκτικότητας στον κυβερνοχώρο για τις επιχειρήσεις όλων των μεγεθών και ανέδειξε τον σημαντικό ρόλο των ασφαλιστών στην πρόληψη, τον μετριασμό και την ανάληψη μέρους του ρίσκου των επιχειρήσεων.

5. Η **ασφάλιση κατά των κινδύνων του κυβερνοχώρου** είναι ομολογουμένως μία **πολύπλοκη νέα μορφή ασφάλισης**. Αυτή τη στιγμή προσφέρεται στη χώρα μας από ορισμένο αριθμό ασφαλιστικών εταιριών, είτε **ως αυτοτελές ασφαλιστήριο συμβόλαιο** (standalone cyber insurance), είτε **ως επέκταση άλλης ασφαλιστικής κάλυψης**. Ωστόσο, η ασφάλιση cyber risk απασχολεί ολοένα και περισσότερο την ελληνική ασφαλιστική αγορά από την άποψη τόσο της προοπτικής ανάπτυξης, όσο και των προκλήσεων και των ειδικών θεμάτων που αναδεικνύονται και πρέπει να αντιμετωπιστούν, όπως είναι τα ζητήματα underwriting, risk management, προστασίας προσωπικών δεδομένων κ.ά..

ΟΔΗΓΟΣ ΑΣΦΑΛΙΣΗΣ CYBER: Μία πρωτοβουλία της ΕΑΕΕ για την ασφαλέστερη προσέγγιση των προκλήσεων του κυβερνοχώρου

1. Η **ΕΑΕΕ** αναγνωρίζοντας το σημαντικό ρόλο που μπορεί να διαδραματίσει η ασφαλιστική αγορά στην αντιμετώπιση των αυξανόμενων προκλήσεων που εμφανίζει το τοπίο των κινδύνων στον κυβερνοχώρο, προχώρησε στη σύσταση ειδικής **Ομάδας Εργασίας για την Ασφάλιση των Κινδύνων του Κυβερνοχώρου.**

   Στόχος της Ομάδας αυτής είναι η στενή παρακολούθηση των εξελίξεων στον τομέα των κινδύνων του κυβερνοχώρου σε εθνικό και ευρωπαϊκό επίπεδο και η ανάληψη δράσεων ενημέρωσης των εταιριών μελών της ΕΑΕΕ και των ενδιαφερόμενων φορέων και οργανισμών.

2. Ο **«Οδηγός Ασφάλισης Cyber»** είναι μία πρωτοβουλία της ειδικής αυτής Ομάδας Εργασίας της ΕΑΕΕ που έχει τους εξής κυρίως στόχους :

   - να παρουσιάζει με απλό και κατανοητό τρόπο τις **βασικές έννοιες & τους κινδύνους** που θα ήταν χρήσιμο κάποιος να γνωρίζει προκειμένου να προσεγγίσει καλύτερα τον τομέα του κυβερνοχώρου,

   - να παρέχει χρήσιμες πληροφορίες σχετικά με τις **παρεχόμενες από την ασφαλιστική αγορά καλύψεις για την ασφάλιση των κινδύνων του κυβερνοχώρου**, αλλά και για τη βέλτιστη κατά το δυνατόν **αντιμετώπιση των ειδικών θεμάτων** που απασχολούν την ασφαλιστική αγορά και αφορούν στον τομέα αυτό (όπως είναι για παράδειγμα η κρυφή έκθεση ή αλλιώς «silent exposure» σε κινδύνους του κυβερνοχώρου άλλων ασφαλιστικών καλύψεων, ειδικά ζητήματα underwriting, προστασίας προσωπικών δεδομένων κ.α.),

   - να ενημερώνει για **τις σημαντικότερες μελέτες και εκθέσεις που δημοσιεύονται σε διεθνές επίπεδο** για θέματα κυβερνοασφάλειας, αλλά και ειδικότερα για θέματα που αφορούν στην ασφάλιση των κινδύνων του κυβερνοχώρου.

   Ο **«Οδηγός Ασφάλισης Cyber»** θα εμπλουτίζεται συνεχώς με νέα κείμενα. Έχει αποκλειστικά και μόνο ενημερωτικό και μη δεσμευτικό χαρακτήρα και απώτερος σκοπός του είναι η προαγωγή του επιστημονικού διαλόγου και η κατά το δυνατόν καλύτερη και συνεχής ενημέρωση ασφαλιστικών εταιριών και ασφαλισμένων.

   Θέλουμε να πιστεύουμε ότι ο **«Οδηγός Ασφάλισης Cyber»** θα αποτελέσει ένα **χρήσιμο εργαλείο** για όλους τους ενδιαφερόμενους.

ΕΝΝΟΙΕΣ – ΚΙΝΔΥΝΟΙ

Phishing

Phishing είναι η επικοινωνία μέσω ηλεκτρονικής αλληλογραφίας, η οποία προέρχεται φαινομενικά από μια νόμιμη πηγή και προτρέπει τους χρήστες να αποκαλύψουν προσωπικά ή εταιρικά στοιχεία ή να ακολουθήσουν κάποιο σύνδεσμο σε άλλο ιστότοπο, με απώτερο σκοπό την κλοπή δεδομένων ή την εγκατάσταση κακόβουλου λογισμικού. Αποτελεί μέθοδο κοινωνικής μηχανικής (Social engineering).

Pharming

Pharming είναι είδος επίθεσης που στόχο έχει την ανακατεύθυνση του προγράμματος περιήγησης (browser) σε άλλες ψεύτικες ιστοσελίδες με απώτερο σκοπό την κλοπή δεδομένων ή την εγκατάσταση κακόβουλου λογισμικού. Σε περίπτωση επιτυχημένης επίθεσης Pharming, ακόμη και αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, η ανακατεύθυνση θα τον οδηγεί πάντα σε ψεύτικη.

Social engineering

Social engineering (κοινωνική μηχανική) είναι η τακτική πίσω από μερικές από τις πιο διάσημες επιθέσεις χάκερ. Είναι μια μέθοδος που βασίζεται στην έρευνα και την πειθώ που είναι συνήθως στη ρίζα του spam, phishing, και spear phishing απατών, οι οποίες διαδίδονται μέσω ηλεκτρονικού ταχυδρομείου. Ο σκοπός των επιθέσεων social engineering είναι να κερδίσει την εμπιστοσύνη του θύματος για να κλέψει δεδομένα και χρήματα. Τα περιστατικά Social engineering συχνά περιλαμβάνουν τη χρήση κακόβουλου λογισμικού, όπως ransomware και trojans.

Οι περιπτώσεις Social engineering που αναφέρονται παρακάτω δίνουν μια ιδέα για το πώς λειτουργούν αυτές οι επιθέσεις και πόσο δαπανηρές μπορούν να γίνουν για τις εταιρείες, τους ανθρώπους και τις κυβερνήσεις.

- **Shark Tank, 2020**

Τηλεοπτική δικαστής εξαπατήθηκε για σχεδόν 400.000 δολάρια. Ένας κυβερνοεγκληματίας μιμήθηκε την βοηθό της και έστειλε ένα email στον λογιστή της ζητώντας μια πληρωμή που σχετίζεται με επενδύσεις σε ακίνητα. Χρησιμοποίησε μια διεύθυνση ηλεκτρονικού ταχυδρομείου παρόμοια με τη νόμιμη. Η απάτη ανακαλύφθηκε μόνο αφού ο λογιστής έστειλε ένα μήνυμα ηλεκτρονικού ταχυδρομείου στη σωστή διεύθυνση του βοηθού ζητώντας λεπτομέρειες για τη συναλλαγή.

- **Toyota, 2019**

Η Toyota Boshoku Corporation, προμηθευτής εξαρτημάτων αυτοκινήτων, έπεσε θύμα μιας επίθεσης social engineering το 2019. Τα χρήματα που χάθηκαν ανέρχονται σε 37 εκατομμύρια δολάρια. Χρησιμοποιώντας την πειθώ, οι επιτιθέμενοι έπεισαν ένα στέλεχος

του οικονομικό τμήματος να αλλάξει τις πληροφορίες του τραπεζικού λογαριασμού του παραλήπτη σε ένα έμβασμα.

- **Cabarrus County, 2018**

Λόγω του social engineering και της απάτης bec (business email compromise), η κομητεία Cabarrus, στις Ηνωμένες Πολιτείες, υπέστη απώλεια 1,7 εκατομμυρίων δολαρίων ΗΠΑ το 2018. Χρησιμοποιώντας κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου, οι χάκερ παριστάναν τους προμηθευτές της κομητείας και ζήτησαν πληρωμές σε νέο τραπεζικό λογαριασμό. Στα μηνύματα ηλεκτρονικού ταχυδρομείου, οι απατεώνες παρουσίασαν προφανώς νόμιμη τεκμηρίωση.

- **Ethereum Classic, 2017**

Αρκετοί άνθρωποι έχασαν χιλιάδες δολάρια σε κρυπτονόμισμα μετά από την επίθεση χάκερ στην ιστοσελίδα Ethereum Classic, το 2017. Χρησιμοποιώντας social engineering , οι χάκερ μιμήθηκαν τον ιδιοκτήτη του Ethereum Classic, απέκτησαν πρόσβαση στο domain και, στη συνέχεια, ανακατεύθυναν το domain στον δικό τους διακομιστή. Οι εγκληματίες εξήγαγαν το κρυπτονόμισμα Ethereum από τα θύματα αφού εισαγάγανε έναν κωδικό (code injection) στον ιστότοπο που τους επέτρεπε να βλέπουν ιδιωτικά κλειδιά που χρησιμοποιούνται για συναλλαγές.

- **Democratic Party, 2016**

Στις προεδρικές εκλογές των Ηνωμένων Πολιτειών το 2016 οι επιθέσεις spear phishing οδήγησαν στη διαρροή μηνυμάτων ηλεκτρονικού ταχυδρομείου και πληροφοριών από το Δημοκρατικό Κόμμα. Οι χάκερ δημιούργησαν ένα ψεύτικο μήνυμα ηλεκτρονικού ταχυδρομείου από το Gmail, καλώντας τους χρήστες, μέσω ενός συνδέσμου, να αλλάξουν τους κωδικούς πρόσβασής τους λόγω ασυνήθιστης δραστηριότητας. Στη συνέχεια, οι απατεώνες είχαν πρόσβαση σε εκατοντάδες μηνύματα ηλεκτρονικού ταχυδρομείου που περιείχαν ευαίσθητες πληροφορίες σχετικά με την εκστρατεία Κλίντον.

- **Ubiquiti Networks, 2015**

Η Ubiquiti Networks, κατασκευαστής τεχνολογίας για δικτύωση, έχασε σχεδόν 40 εκατομμύρια το 2015, μετά από μια επίθεση ηλεκτρονικού "ψαρέματος". Πιστεύεται ότι ένας λογαριασμός ηλεκτρονικού ταχυδρομείου υπαλλήλου έχει παραβιαστεί στο Χονγκ Κονγκ. Στη συνέχεια, οι χάκερ χρησιμοποίησαν την τεχνική της απομίμησης για να ζητήσουν δόλιες πληρωμές, οι οποίες έγιναν από το λογιστικό τμήμα.

- **Sony Pictures, 2014**

Μετά από έρευνα, το FBI επεσήμανε ότι η κυβερνοεπίθεση στη Sony Pictures, το 2014, ήταν ευθύνη της κυβέρνησης της Βόρειας Κορέας. Χιλιάδες αρχεία, συμπεριλαμβανομένων επιχειρηματικών συμφωνιών, οικονομικών εγγράφων και πληροφοριών των εργαζομένων, κλάπηκαν. Η Sony Pictures ήταν στόχος από χάκερ για να αντιγράψουν πληροφορίες από πιστωτικές και χρεωστικές κάρτες των πελατών.

- **Target, 2013**

Ως αποτέλεσμα της παραβίασης δεδομένων της target, το 2013, οι χάκερ απέκτησαν πρόσβαση σε πληροφορίες πληρωμής 40 εκατομμυρίων πελατών. Μέσω ηλεκτρονικού

"ψαρέματος", οι εγκληματίες εγκατέστησαν ένα κακόβουλο λογισμικό σε μια συνεργαζόμενη εταιρεία της Target, το οποίο τους επέτρεψε να έχουν πρόσβαση στο δίκτυο του δεύτερου μεγαλύτερου καταστήματος λιανικής πώλησης πολυκαταστημάτων στις Ηνωμένες Πολιτείες. Στη συνέχεια, οι χάκερ εγκατέστησαν ένα άλλο κακόβουλο λογισμικό στο σύστημα της Target και μπόρεσα να κλέψουν πληροφορίες για πιστωτικές κάρτες.

- **South Carolina Department of Revenue, 2012**

Οι χάκερ έκλεψαν εκατομμύρια αριθμούς κοινωνικής ασφάλισης και χιλιάδες πληροφορίες πιστωτικών και χρεωστικών καρτών από το Τμήμα Εσόδων της Νότιας Καρολίνας, το 2012. Οι υπάλληλοι έπεσαν θύματα σε αυτή την απάτη ηλεκτρονικού "ψαρέματος", μοιράζοντας ονόματα χρηστών και κωδικούς πρόσβασής. Μετά από αυτό, με τα διαπιστευτήρια στα χέρια, οι χάκερ απέκτησαν πρόσβαση στο δίκτυο της κρατικής υπηρεσίας.

- **RSA, 2011**

Η RSA, μια εταιρεία ασφαλείας, εκτιμάται ότι έχει δαπανήσει περίπου 66 εκατομμύρια δολάρια λόγω της παραβίασης δεδομένων της, το 2011. Η επίθεση ξεκίνησε με ένα έγγραφο του Excel, το οποίο στάλθηκε σε μια μικρή ομάδα υπαλλήλων μέσω ηλεκτρονικού ταχυδρομείου. Το θέμα ηλεκτρονικού ταχυδρομείου είχε τίτλο "Σχέδιο Προσλήψεων". Το συνημμένο περιείχε ένα κακόβουλο αρχείο που άνοιξε μια κερκόπορτα για τους χάκερ.

Telephone Hacking

Το τηλεφωνικό δίκτυο μιας επιχείρησης δεν είναι απλά το άθροισμα των τηλεφώνων που διαθέτει ούτε καν ένα απλό ψηφιακό κέντρο που κατανέμει γραμμές. Είναι ένα σύγχρονο ηλεκτρονικό σύστημα που καταγραφεί κλήσεις, διανέμει πόρους δικτύου, προσφέρει ψηφιακές υπηρεσίες, έχει υψηλό κόστος αγοράς και είναι μια κρίσιμη υποδομή της κάθε εταιρίας.

Η παραβίαση του θα έχει λοιπόν τις ίδιες συνέπειες που έχει και η παραβίαση κάθε άλλης ηλεκτρονικής υποδομής, δηλαδή διακοπή εργασιών, διαρροή προσωπικών δεδομένων και εμπιστευτικών εταιρικών πληροφοριών, ζημιά στη φήμη και την αξιοπιστία της εταιρίας συν μία ακόμα:

Οι Hackers αποκτώντας τον έλεγχο του τηλεφωνικού δικτύου της επιχείρησης μπορούν να προκαλέσουν και άμεση οικονομική ζημία μέσω τηλεφωνικών χρεώσεων για τις οποίες είναι υπεύθυνη η Εταιρεία ως αποτέλεσμα της αυθαίρετης χρήσης των τηλεφωνικών συστημάτων της.

Με δεδομένο ότι είναι πολύ πιθανό η Εταιρία να μην αντιληφθεί την παραβίαση ίσως και για 2 μήνες, (μέχρι να εμφανιστεί ο επόμενος λογαριασμός!) και λαμβάνοντας υπόψη το κόστος που έχουν οι κλήσεις σε αριθμούς αυξημένης χρέωσης, το κέρδος για τους hackers μπορεί να είναι μεγάλο και αντίστοιχα μεγάλη να είναι η ζημιά για την Εταιρία.

PCI DSS

Το PCI DSS, (Payment Card Industry Data Security Standard), είναι το πρότυπο ηλεκτρονικής ασφάλειας δεδομένων που έχουν υιοθετήσει οι εκδότριες εταιρίες πιστωτικών καρτών, (Visa, Mastercard κ.λ.π.) και έχει ως σκοπό να προστατέψει τα δεδομένα των χρηστών και να μειώσει την απάτη που γίνεται με τη χρήση πιστωτικών καρτών.

Προκειμένου μια εταιρία να λάβει την πιστοποίηση PCI DSS πρέπει να πληροί 12 σημαντικές (τεχνικές) προϋποθέσεις ασφαλείας. Δεν είναι υποχρεωτικό για μια εταιρία να έχει λάβει την πιστοποίηση αυτή για να κάνει συναλλαγές με πιστωτικές κάρτες, είναι κάτι όμως που της προσδίδει κύρος και αξιοπιστία και έτσι ιδιαίτερα οι μεγάλες εμπορικές εταιρίες το επιδιώκουν.

Εφόσον όμως λάβουν την πιστοποίηση αυτή, οι εταιρίες αναλαμβάνουν ταυτόχρονα και κάποιες συμβατικές υποχρεώσεις διαρκούς συμμόρφωσης. Οι υποχρεώσεις αυτές δεν θα υπήρχαν αλλιώς. Δεν προβλέπονται από κάποια νομοθεσία. Είναι το «αντάλλαγμα» που δέχεται η εταιρία για να λάβει την πιστοποίηση αυτή. Έτσι σε περίπτωση που υπάρξει μη συμμόρφωση με οποιοδήποτε Πρότυπο Ασφαλείας Προσωπικών Δεδομένων PCI, άρα ουσιαστικά παραβίαση ασφαλείας μιας εταιρίας, εκτός των άλλων «κλασικών» συνεπειών, στην εταιρία μπορεί να επιβληθεί και χρηματικό πρόστιμο από το φορέα διαχείρισης του PCI DSS. Το πρόστιμο αυτό μπορεί να αποτελέσει αντικείμενο ασφαλιστικής κάλυψης.

Προστασία Προσωπικών Δεδομένων

Η προστασία των **φυσικών** προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είναι θεμελιώδες δικαίωμα. Η αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα, απαιτεί την ενίσχυση και τον λεπτομερή καθορισμό των δικαιωμάτων των υποκειμένων των δεδομένων καθώς και των υποχρεώσεων όσων επεξεργάζονται και καθορίζουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα αλλά και των αντίστοιχων εξουσιών παρακολούθησης και διασφάλισης της συμμόρφωσης προς τους κανόνες προστασίας των προσωπικών δεδομένων και των αντίστοιχων κυρώσεων για τις παραβιάσεις αυτών.

Βασική νομοθεσία που διέπει την προστασία των προσωπικών δεδομένων σε εθνικό και ευρωπαϊκό επίπεδο είναι η εξής: ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 (στο εξής ΓΚΠΔ), ο ν. 4624/2019, ο ν. 2472/1997 καθώς και ο ν. 3471/2006 στον τομέα των ηλεκτρονικών επικοινωνιών.

Ειδικότερα, ο ΓΚΠΔ από τις 25.5.2018 έχει άμεση εφαρμογή σε όλα τα κράτη μέλη, τα οποία υποχρεούνται να λάβουν τα αναγκαία μέτρα για την προσαρμογή της εθνικής νομοθεσίας τους. Με τον ν. 4624/2019, ορίζονται μέτρα εφαρμογής του ΓΚΠΔ και ενσωματώνεται στην εθνική νομοθεσία η Οδηγία (ΕΕ) 2016/680. Ο ν. 2472/1997 καταργήθηκε, εκτός των διατάξεων που αναφέρονται ρητά στο άρθρο 84 του ν. 4624/2019.

Ο ν. 3471/2006 που ενσωματώνει την Οδηγία 2002/58/ΕΚ (Οδηγία e-Privacy), όπως έχει τροποποιηθεί με την Οδηγία 2009/136/ΕΚ, αποτελεί συμπλήρωση και εξειδίκευση του θεσμικού πλαισίου της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

Σύμφωνα με τον ΓΚΠΔ :

«Δεδομένα προσωπικού χαρακτήρα» αποτελεί κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

«Προσωπικά δεδομένα ειδικών κατηγοριών» είναι τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία, δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

Σε ένα ασφαλιστήριο συμβόλαιο για την κάλυψη cyber risks που απευθύνεται κυρίως σε επιχειρήσεις/ νομικά πρόσωπα, η νομοθεσία για την προστασία των προσωπικών δεδομένων βρίσκει εφαρμογή στην ασφάλιση επαγγελματιών / ατομικών επιχειρήσεων και των εργαζομένων τους καθώς και στην κάλυψη πελατών, συνεργατών, προμηθευτών ή τρίτων συνήθως από **«παραβίαση δεδομένων προσωπικού χαρακτήρα».**

Ως τέτοια ορίζεται η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας διαβίβαση, δημοσιοποίηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Η Εποπτική Αρχή για την εφαρμογή των παραπάνω είναι η ανεξάρτητη «**Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**» (ΑΠΔΠΧ), η οποία ιδρύθηκε με το ν. 2472/1997 και λειτουργεί βάσει του ν. 4624/2019 (άρθρα 9-20). Σύμφωνα με τον ΓΚΠΔ, η ΑΠΔΠΧ έχει επιφορτιστεί με την παρακολούθηση της εφαρμογής του, με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας που τα αφορούν και τη διευκόλυνση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα στην Ένωση.

Επιπλέον, για τις ανάγκες του Cyber Guide αναφέρονται και οι εξής ορισμοί του ΓΚΠΔ : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, αποτελεί τον **Υπεύθυνο Επεξεργασίας** σε έναν οργανισμό. Ενώ, το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου της επεξεργασίας, είναι ο «**Εκτελών την επεξεργασία**».

Υπεύθυνος Προστασίας Δεδομένων ή Data Protection Officer (DPO)

Ο «**Υπεύθυνος προστασίας δεδομένων» (DPO)** είναι το φυσικό ή νομικό πρόσωπο που ορίζεται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και το οποίο συμμετέχει δεόντως και εγκαίρως, σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ο Υπεύθυνος Προστασίας Δεδομένων (DPO) διευκολύνει τη συμμόρφωση ενός οργανισμού με τις νομικές του υποχρεώσεις που απορρέουν από την εκάστοτε ισχύουσα εθνική και ευρωπαϊκή νομοθεσία σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, με άλλα λόγια ενημερώνει, συμβουλεύει και συνδράμει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ο DPO μπορεί να είναι υπάλληλος του οργανισμού / επιχείρησης ή εξωτερικός συνεργάτης. Σε κάθε περίπτωση είναι ο αρμόδιος να επιβλέπει το εάν η επιχείρηση λειτουργεί σε πλήρη συμφωνία με τον ΓΚΠΔ, και δεσμεύεται από την τήρηση του απορρήτου και της εμπιστευτικότητας σε ό,τι αφορά την εκτέλεση των καθηκόντων του, τα οποία πρέπει να είναι σε πλήρη συμφωνία με τον ΓΚΠΔ.

Ο DPO συνεργάζεται με την ΑΠΔΠΧ. Τα στοιχεία του οριζόμενου DPO ανακοινώνονται στην ΑΠΔΠΧ.

Στον ΓΚΠΔ προβλέπονται συγκεκριμένες περιπτώσεις όπου ο υπεύθυνος ή ο εκτελών την επεξεργασία υποχρεούται να ορίσει DPO.

Κάλυψη Ηλεκτρονικών & Διαδικτυακών Κινδύνων (Cyber Risks) – Η προσέγγιση της αυτοτελούς (standalone) ασφαλιστικής σύμβασης

Η προσέγγιση της αυτοτελούς (standalone) ασφαλιστικής σύμβασης

Η ασφαλιστική βιομηχανία αναγνωρίζοντας τους πολύπλοκους κινδύνους του κυβερνοχώρου (Cyber Risks) και την πρόκληση που συνιστά η ασφάλισή τους προχώρησε στη δημιουργία ενός νέου τύπου ασφάλισης που καλύπτει μεγάλο αριθμό των Cyber Risks, των Ηλεκτρονικών & Διαδικτυακών δηλαδή Κινδύνων που αντιμετωπίζουν οι επιχειρήσεις και οι επαγγελματίες σήμερα.

Τα βασικά σημεία μίας αυτοτελούς (standalone) ασφαλιστικής σύμβασης για την κάλυψη των κινδύνων του κυβερνοχώρου παρατίθενται κατωτέρω. Επισημαίνεται ωστόσο ότι η ασφάλιση των κινδύνων του κυβερνοχώρου είναι μια δυναμικά εξελισσόμενη ασφαλιστική κάλυψη, η οποία αναπτύσσεται διαρκώς κατά τρόπον ώστε να προσφέρει την ευρύτερη δυνατή κάλυψη στους ασφαλισμένους.

Α. Έκταση Κάλυψης

Με την ασφάλιση Cyber Risks, Ηλεκτρονικών και Διαδικτυακών Κινδύνων, ο Ασφαλιστής αναλαμβάνει την υποχρέωση να αποζημιώσει τον Ασφαλισμένο για διάφορες Οικονομικές Αξιώσεις που θα εγείρουν Τρίτοι, (ενδεικτικά πελάτες, συνεργάτες, προμηθευτές, ρυθμιστικές αρχές), οι οποίοι θα ισχυριστούν και θα αποδείξουν ότι με πράξεις ή παραλήψεις του Ασφαλισμένου ή από κακόβουλη ενέργεια τρίτων (hackers) που σχετίζεται με Ηλεκτρονικούς και Διαδικτυακούς Κινδύνους προκλήθηκε σε αυτούς οικονομική ζημιά ή ηθική βλάβη, για την οποία δικαιούνται και διεκδικούν εκ του νόμου χρηματική αποζημίωση. Ο Ασφαλιστής θα αποζημιώσει επίσης και την άμεση οικονομική ζημία που θα υποστεί ο Ασφαλισμένος. Τα παραπάνω ισχύουν πάντα μέχρι των ορίων ευθύνης και του εύρους των καλύψεων που συμφωνούνται με την Ασφαλιστική Σύμβαση.

Για την ενεργοποίηση της Ασφαλιστικής αυτής Σύμβασης και την καταβολή της σχετικής αποζημίωσης, συμφωνείται συνήθως η σωρευτική συνδρομή των ακόλουθων προϋποθέσεων:

i. Το ζημιογόνο γεγονός να αφορά δραστηριότητα του Λήπτη της Ασφάλισης εντός των Γεωγραφικών Ορίων που συμφωνούνται στην Ασφαλιστική Σύμβαση και να εγείρεται αξίωση και πάλι εντός των Γεωγραφικών Ορίων που συμφωνούνται στην Ασφαλιστική Σύμβαση,

ii. Το ζημιογόνο γεγονός να οφείλεται σε συμβάν που λαμβάνει χώρα κατά τη διάρκεια της Ασφαλιστικής Περιόδου ή μετά την Ημερομηνία Αναδρομικής Ισχύος της Κάλυψης που ενδεχομένως έχει συμφωνηθεί και μέχρι τη λήξη της Ασφαλιστικής Περιόδου της Ασφαλιστικής Σύμβασης,

iii. Οι αξιώσεις να εγερθούν για πρώτη φορά εντός της Ασφαλιστικής Περιόδου της Ασφαλιστικής Σύμβασης, καθώς και να έχουν αναγγελθεί εγγράφως από τον Ασφαλισμένο στον Ασφαλιστή εντός της Ασφαλιστικής Περιόδου ή και μέχρι την ημερομηνία λήξης της Εκτεταμένης Περιόδου Αναγγελίας / Δήλωσης Απαιτήσεων (εφόσον έχει συμφωνηθεί τέτοια και σύμφωνα με τους ειδικότερους όρους και προϋποθέσεις που αναφέρονται στην Ασφαλιστική Σύμβαση και αφορούν τη συμφωνία αυτή).

Επισημάνσεις:

i. Διευκρινίζεται ότι Λήπτης της Ασφάλισης στην εν λόγω Ασφαλιστική Σύμβαση είναι η εταιρία (νομικό πρόσωπο), ενώ Ασφαλισμένοι είναι εκτός από τον Λήπτη και τα φυσικά πρόσωπα που εργάζονται για αυτόν.

ii. Εξωτερικοί συνεργάτες και ανεξάρτητοι εργολάβοι που εργάζονται για λογαριασμό του Λήπτη της Ασφάλισης, πάντα για σχετικές με τον Λήπτη της Ασφάλισης εργασίες, μπορούν επίσης να καλυφθούν για όλες ή μέρος των προσφερόμενων καλύψεων.

iii. Ανάλογα με τη φύση των εργασιών της κάθε εταιρίας, ο βασικός καλυπτόμενος κίνδυνος μπορεί να είναι οι Απαιτήσεις Τρίτων ή οι ιδίες ζημιές είτε και τα δύο.

iv. Είναι ιδιαίτερα σύνηθες στη κάλυψη αυτή οι Ασφαλιστές να παρέχουν και σειρά υπηρεσιών άμεσης διαχείρισης των περιστατικών με σκοπό την υποστήριξη του ασφαλισμένου, αλλά και τον περιορισμό της Ζημιάς. Η χρήση των υπηρεσιών αυτών είναι προαιρετική προς τους Ασφαλισμένους, αλλά συνήθως δίνονται κίνητρα για χρήση τους όπως χαμηλότερες απαλλαγές. Εκ της φύσεως όμως της κάλυψης είναι απαραίτητο ο ασφαλισμένος να έχει προβλέψει διαδικασία διαχείρισης κρίσεων που θα σχετίζεται με Ηλεκτρονικούς και Διαδικτυακούς Κινδύνους.

v. Διευκρινίζεται τέλος ότι η ασφαλιστική αυτή κάλυψη δεν μπορεί να χρησιμοποιηθεί από τον Ασφαλισμένο για την ενίσχυση και βελτίωση των ηλεκτρονικών συστημάτων ασφαλείας του.

Β. Ειδικότερες Εξαιρέσεις από την Κάλυψη Ευθύνης Ηλεκτρονικών & Διαδικτυακών Κινδύνων

Πέραν των εξαιρέσεων που αναφέρονται στο λήμμα «Εξαιρέσεις Ασφαλίσεων Αστικής Ευθύνης που συνάπτονται για λόγους επαγγελματικούς» του Ερμηνευτικού Λεξικού και δεν αντίκεινται στην παρούσα ασφαλιστική κάλυψη, συνήθεις εξαιρέσεις που μπορεί επιπλέον να προβλεφθούν στην ασφάλιση Ευθύνης Ηλεκτρονικών & Διαδικτυακών Κινδύνων μπορεί να είναι και οι ακόλουθες :

i. Εξαίρεση κάλυψης ζημίας που οφείλεται σε Μόλυνση /Ρύπανση /Υποβάθμιση του Περιβάλλοντος /Περιβαλλοντική Ευθύνη.

ii. Εξαίρεση κάλυψης ζημίας που οφείλεται σε Σωματικές Βλάβες και Υλικές Ζημιές.

iii. Εξαίρεση κάλυψης ζημίας που οφείλεται σε παραβίαση Πνευματικής Ιδιοκτησίας.

iv. Εξαίρεση κάλυψης ζημίας που οφείλεται σε παράλειψη αποκατάστασης γνωστών αδυναμιών των συστημάτων της Εταιρίας.

Γ. Βασικές Καλύψεις Ευθύνης Ηλεκτρονικών και Διαδικτυακών Κινδύνων

i. Κάλυψη αμοιβών διαφόρων Συμβούλων για νομικά θέματα, θέματα IT, θέματα επικοινωνίας.

ii. Κάλυψη εξόδων για ανάκτηση, αποκατάσταση, επαναδημιουργία ηλεκτρονικών αρχείων.

iii. Κάλυψη εξόδων για επαναφορά / αποκατάσταση ηλεκτρονικών συστημάτων.

iv. Κάλυψη απαιτήσεων Τρίτων, καθώς και νομικών δαπανών για παραβίαση προσωπικών δεδομένων / απώλεια εμπιστευτικών πληροφοριών.

v. Κάλυψη εξόδων ερευνών ρυθμιστικών Αρχών.

Δ. Βασικές Επεκτάσεις Κάλυψης

i. Κάλυψη για απαιτήσεις σχετικές με εκβιασμό λόγω κλειδώματος ή κλοπής δεδομένων.

ii. Κάλυψη για απαιτήσεις συνεπεία διακοπής εργασιών λόγω παραβίασης της ασφαλείας συστημάτων.

iii. Κάλυψη εξόδων από κακόβουλη χρήση του τηλεφωνικού δικτύου της εταιρίας από Τρίτους.

iv. Κάλυψη απαιτήσεων που σχετίζονται με τη χρήση cloud και την παραβίαση ασφάλειας του.

v. Κάλυψη απαιτήσεων που σχετίζονται με κλοπή χρημάτων του ασφαλισμένου μέσω ηλεκτρονικής απάτης.

Ε. Ενδεικτικά παραδείγματα καλυπτόμενων ζημιών

Για την πληρέστερη κατανόηση των ανωτέρω, παρατίθενται ορισμένα ενδεικτικά παραδείγματα ζημιών που μπορούν να καλύπτονται από την εν λόγω ασφάλιση υπό την αυτονόητη προϋπόθεση της τήρησης των λοιπών όρων και προϋποθέσεων που προβλέπονται από την εκάστοτε συναφθείσα μεταξύ ασφαλιστή και ασφαλισμένου ασφαλιστική σύμβαση:

i. Απαίτηση αποζημίωσης μετά από διαρροή ιατρικών πληροφοριών ασθενούς.

ii. Απαίτηση αποζημίωσης συνεργαζόμενης εταιρίας εξαιτίας διαρροής εμπορικών μυστικών της που είχε λόγω συνεργασίας στη κατοχή του ο Ασφαλισμένος.

iii. Έξοδα για επαναφορά συστημάτων, τα οποία είχαν παραβιαστεί από hacker και είχε διακοπεί η λειτουργία τους.

iv. Έξοδα νομικών για ενημέρωση της Αρχή Προστασίας Προσωπικών Δεδομένων μετά από παραβίαση προσωπικών δεδομένων.

v. Έξοδα ενημέρωσης των υποκείμενων των προσωπικών δεδομένων μετά τη διαρροή τους.

vi. Απώλεια κερδών μετά από διακοπή εργασιών του Ασφαλισμένου.

vii. Κάλυψη ζημίας λόγω μεταφοράς χρημάτων της εταιρίας από hacker με ηλεκτρονικά μέσα σε μη δικαιούχο.

viii. Απαίτηση λύτρων, για αποκρυπτογράφηση αρχείων του Ασφαλισμένου που είχαν κλειδωθεί από hacker.

Κάλυψη Διακοπής Εργασιών / Απώλειας Κερδών συνεπεία Κυβερνοκινδύνων

A. Έκταση Κάλυψης

Με την κάλυψη της διακοπής εργασιών / απώλειας κερδών συνεπεία κυβερνοκινδύνων καλύπτονται το λειτουργικό κέρδος που η ασφαλιζόμενη επιχείρηση δεν κατέστη δυνατόν να παράξει καθώς και οι σταθερές δαπάνες λειτουργίας που δεν κατέστη δυνατόν να καλύψει ως αποτέλεσμα διακοπής ή/και παρεμπόδισης των εργασιών της (λόγω συγκεκριμένων αιτίων που σχετίζονται με κινδύνους του κυβερνοχώρου σύμφωνα με την έκταση παρεχόμενης κάλυψης) μέχρι τη χρονική στιγμή που η απώλεια κερδών παύει να υφίσταται ή μέχρι το τέλος της περιόδου αποζημίωσης, οποιοδήποτε είναι χρονικά νωρίτερα.

Επιπλέον καλύπτονται τα αυξημένα έξοδα που αποδεδειγμένα πραγματοποιούνται κατά τη διάρκεια ασφάλισης - μετά το πρώτο συμβάν απώλειας δεδομένων / λογισμικού - για την πρόληψη/αποφυγή ή τον περιορισμό της διακοπής εργασιών της επιχείρησης και τα οποία δεν προέκυψαν ως μέρος της συνήθους λειτουργίας της ασφαλισμένης επιχείρησης.

A1. Λειτουργικό Κέρδος

Λειτουργικό κέρδος είναι το καθαρό κέρδος που απορρέει από τη λειτουργία της επιχείρησης και το οποίο προκύπτει από τον κύκλο εργασιών της που πραγματοποιήθηκε στις εγκαταστάσεις της επιχειρηματικής λειτουργίας της, από το οποίο αφαιρούνται τα έξοδα της επιχείρησης συμπεριλαμβανομένων των αποσβέσεων.

Στα καθαρά κέρδη της επιχείρησης δεν συμπεριλαμβάνονται οι εισπράξεις από διάθεση στοιχείων του κεφαλαίου, ούτε λαμβάνεται υπόψη οποιαδήποτε πληρωμή που επιβαρύνει το κεφάλαιο.

Με άλλα λόγια στον υπολογισμό των καθαρών κερδών δεν λαμβάνονται υπόψη έσοδα ή/και έξοδα που δεν σχετίζονται με παραγωγικές και εμπορικές λειτουργίες της επιχείρησης, τα οποία παράγονται ή προκύπτουν εκτός του πλαισίου του πραγματικού σκοπού της (π.χ. επενδύσεις κεφαλαίων ή συναλλαγές επί ακινήτων).

A2. Σταθερές δαπάνες λειτουργίας

Σταθερές δαπάνες λειτουργίας είναι οι πάγιες λειτουργικές δαπάνες της επιχείρησης, οι οποίες εξακολουθούν να τη βαρύνουν παρά τη διακοπή ή παρεμπόδιση των εργασιών της.

Σημείωση:
Οι πάγιες λειτουργικές δαπάνες και τα έξοδα αποζημιώνονται στον ασφαλισμένο εφόσον υπάρχει νομική υποχρέωση για την συνεχιζόμενη καταβολή τους από τον ασφαλισμένο ή αν αυτή δικαιολογείται οικονομικά και εάν τα κόστη αυτά θα δημιουργούνταν ακόμη κι αν δεν είχε λάβει χώρα η διακοπή ή/και παρεμπόδιση των εργασιών της.

Α3. Αυξημένα έξοδα

Αυξημένα έξοδα είναι τα έξοδα που αποδεδειγμένα πραγματοποιούνται κατά τη διάρκεια ασφάλισης - μετά το πρώτο συμβάν απώλειας δεδομένων / λογισμικού - για την αποφυγή ή τον περιορισμό της διακοπής εργασιών της επιχείρησης και τα οποία δεν προέκυψαν ως μέρος της συνήθους λειτουργίας της ασφαλισμένης επιχείρησης.

Τα αυξημένα έξοδα σχετίζονται κατά βάση με:

- υπερωρίες εργαζομένων
- προσωρινή απασχόληση εποχικών υπαλλήλων
- προσωρινή ενοικίαση ή/και χρήση Εξοπλισμού Επεξεργασίας Δεδομένων που ανήκει σε τρίτους
- προσωρινή χρήση υπηρεσιών τρίτων

και προκύπτουν αναγκαστικά και εύλογα ως αποτέλεσμα απώλειας δεδομένων/λογισμικού που αφορά την ασφαλισμένη επιχείρηση για τη διασφάλιση της συνέχισης των εργασιών της.

Σημείωση:
Οι δαπάνες για την ανάκτηση δεδομένων/λογισμικού δεν λογίζονται ως αυξημένα έξοδα και δεν αφορούν την κάλυψη απώλειας κερδών.

Β. Περίοδος Αποζημίωσης

Περίοδος αποζημίωσης είναι η περίοδος για την οποία παρέχεται ασφαλιστική κάλυψη για απώλεια κερδών, όπως αυτή ορίζεται στην ασφαλιστική σύμβαση. Η περίοδος αποζημίωσης ξεκινά με την επέλευση του πρώτου συμβάντος διακοπής ή παρεμπόδισης της τεχνικής χρήσης δεδομένων/λογισμικού, αλλά όχι αργότερα από την έναρξη της απώλειας κερδών.

Γ. Αφαιρετέα Χρονική Απαλλαγή

Αφαιρετέα χρονική απαλλαγή είναι η περίοδος αναμονής που έχει συμφωνηθεί στο ασφαλιστήριο για κάθε ασφαλισμένο γεγονός και η οποία βαρύνει τον ίδιο τον ασφαλισμένο. Η περίοδος αναμονής ξεκινά με την επέλευση του πρώτου συμβάντος διακοπής ή παρεμπόδισης της τεχνικής χρήσης δεδομένων/λογισμικού και διαρκεί για το διάστημα που ορίζεται στο ασφαλιστήριο. Η κάθε ασφαλιστική σύμβαση εξειδικεύει και καθορίζει το περιεχόμενο, τους όρους και τις προϋποθέσεις με τις οποίες συμφωνείται μεταξύ ασφαλιστή και ασφαλισμένου η αφαιρετέα χρονική απαλλαγή.

Οικονομικές Ζημίες συνεπεία Κινδύνων Κυβερνοχώρου (γενική αναφορά)

Το κυβερνοέγκλημα μπορεί να δημιουργήσει οικονομική ζημιά σε μια επιχείρηση **σε δύο (2) διαφορετικούς βασικούς πυλώνες :**

- Ο πρώτος πυλώνας αφορά στις **Απαιτήσεις πελατών / προμηθευτών ή τρίτων** για οικονομικές ζημιές που θα υποστούν από την διαρροή στοιχείων τους σαν αποτέλεσμα κυβερνοεγκλήματος που θα συμβεί στην ασφαλισμένη επιχείρηση. Πρόκειται δηλαδή για **απαιτήσεις αστικής ευθύνης,** στην περίπτωση που η επιχείρηση αμέλησε να πάρει τα σωστά μέτρα για να αποτρέψει αυτή τη διαρροή.

- Ο δεύτερος πυλώνας αφορά στις **Άμεσες Οικονομικές Ζημίες** που μπορεί να προκύψουν για την ίδια την ασφαλισμένη επιχείρηση, γνωστές διεθνώς ως **direct financial losses ή first party losses.**

Στις **άμεσες οικονομικές ζημίες** συνεπεία κινδύνων κυβερνοχώρου εμπίπτουν ενδεικτικά οι εξής :

1. **Απώλεια χρημάτων ή περιουσιακών στοιχείων** από τη μη εξουσιοδοτημένη πρόσβαση στους τραπεζικούς λογαριασμούς της επιχείρησης.
2. **Απώλεια κερδών** σε περίπτωση συμβάντος διακοπής εργασιών.
3. **Ζημία Φήμης (Reputation Damage)** και δη το κόστος των δημοσίων σχέσεων, διαφήμισης και άλλα συναφή έξοδα για την αντιμετώπιση της κρίσης και περιορισμό της ζημιάς στη **φήμη** της επιχείρησης.
4. **New Hardware,** εφόσον τα δεδομένα ή το υλικό είναι κατεστραμμένα, και είναι αναγκαίο να προχωρήσει η επιχείρηση στην αγορά νέου υλικού.
5. **Πρόστιμα και Κυρώσεις (Fines & Penanties),** δηλαδή τα πρόστιμα και κυρώσεις που ενδέχεται να επιβληθούν στην επιχείρηση από εποπτικές / ρυθμιστικές αρχές και σχετίζονται με εξ αμελείας μη έγκαιρη γνωστοποίηση ή εξ αμελείας λανθασμένη πράξη/ παράλειψη στη διαχείριση του περιστατικού κυβερνοεγκλήματος και για τα οποία δεν απαγορεύεται εκ του νόμου η ασφαλιστική κάλυψη αυτών.

Οι παραπάνω ενδεικτικά αναφερόμενες άμεσες οικονομικές ζημίες μπορεί να καλύπτονται ή όχι, ανάλογα με την έκταση της παρεχόμενης προς τον ασφαλισμένο ασφαλιστικής κάλυψης.

Η κάθε ασφαλιστική σύμβαση εξειδικεύει και προσδιορίζει συγκεκριμένα το περιεχόμενο, τους όρους και τις προϋποθέσεις με τις οποίες παρέχεται ασφαλιστική κάλυψη στον ασφαλισμένο τόσο για τις απαιτήσεις αστικής ευθύνης τρίτων σε βάρος του, όσο και για τις άμεσες οικονομικές ζημίες του συνεπεία των κινδύνων του κυβερνοχώρου.

Silent Cyber - Σιωπηρός Κίνδυνος Κυβερνοχώρου

Τι είναι το Silent Cyber

Ο Σιωπηρός Κίνδυνος Κυβερνοχώρου αναφέρεται στην έκθεση σε κινδύνους που περιέχονται εντός των παραδοσιακών ασφαλιστηρίων συμβολαίων περιουσίας και ευθύνης, τα οποία πιθανόν να μην καλύπτουν ούτε να εξαιρούν ρητά τον κίνδυνο κυβερνοχώρου. Αναφέρεται κάποιες φορές και ως «μη επιβεβαιωμένος» (non-affirmative) κίνδυνος κυβερνοχώρου.

Σε αντίθεση με τα standalone ασφαλιστήρια συμβόλαια κυβερνοχώρου, τα οποία ορίζουν ξεκάθαρα τις παραμέτρους της κάλυψης από κινδύνους κυβερνοχώρου, πολλά παραδοσιακά συμβόλαια περιουσίας και ευθύνης δεν αναφέρονται συγκεκριμένα στον κίνδυνο αυτό και θεωρητικά θα μπορούσε κανείς να συμπεράνει ότι αποζημιώνουν ζημιές από κίνδυνο κυβερνοχώρου σε ορισμένες περιπτώσεις που προκύπτει ζημιά η οποία θα μπορούσε να καλύπτεται από το ασφαλιστήριο συμβόλαιο, τα αίτια της οποίας όμως ανάγονται στον κυβερνοχώρο, γεγονός το οποίο δεν είχε αξιολογηθεί κατά την ανάληψη του κινδύνου από τον ασφαλιστή και ως εκ τούτου η κάλυψή του δεν αποτελούσε πρόθεση του ασφαλιστή.

Αυτό μπορεί να προκύψει εάν :

- Οι κυβερνοεπιθέσεις ως αιτία ζημιάς δεν περιλαμβάνονται ρητά ούτε εξαιρούνται.
- Το λεκτικό της εξαίρεσης στο ασφαλιστήριο συμβόλαιο δεν είναι σαφές.
- Το λεκτικό της κάλυψης δεν είναι σαφές ή έρχεται σε αντίθεση με άλλο λεκτικό του ασφαλιστηρίου συμβολαίου.

Παραδείγματα

- **Ασφαλιστήριο Συμβόλαιο Περιουσίας:** Καλύπτει υλικές ζημίες και διακοπή εργασιών από φυσική ζημιά σε περιουσιακά αντικείμενα.

  Πιθανή αιτία απαίτησης : Κακόβουλο λογισμικό επηρεάζει τα δεδομένα σε προγραμματιζόμενο μηχάνημα, με αποτέλεσμα την εκδήλωση πυρκαγιάς σε μια μονάδα παραγωγής.

  Τα «δεδομένα» αποτελούν περιουσιακό στοιχείο ;

  Μια επίθεση με κακόβουλο λογισμικό εμπίπτει στην «κακόβουλη ενέργεια» ;

- **Ασφαλιστήριο Συμβόλαιο Γενικής Αστικής Ευθύνης:** Καλύπτει σωματικές βλάβες και υλικές ζημίες τρίτων και εργαζομένων

  Πιθανή αιτία απαίτησης : Κυβερνοεπίθεση προκαλεί υπερθέρμανση στο σύστημα θέρμανσης ενός καταστήματος, το οποίο εκρήγνυται προκαλώντας σωματικές βλάβες και υλικές ζημίες.

- **Ασφαλιστήριο Συμβόλαιο Ευθύνης Διευθυντών και Στελεχών:** Καλύπτει αξιώσεις που προκύπτουν από ανακριβή παρουσίαση δεδομένων ή παραβιάσεις του καθήκοντος εμπιστοσύνης.

Πιθανή αιτία απαίτησης : Εισηγμένη Εταιρία δέχεται κυβερνοεπίθεση στα δεδομένα της, με απώτερο αποτέλεσμα την πτώση της μετοχής της και σχετική αγωγή από τους μετόχους.

Γιατί προβληματίζονται οι Ασφαλισμένοι για το Σιωπηρό Κίνδυνο Κυβερνοχώρου

Η έλλειψη σαφήνειας σε κάποια τυποποιημένα ασφαλιστήρια συμβόλαια περιουσίας και ευθύνης μπορεί επίσης να οδηγήσει σε σύγχυση και παρανοήσεις σχετικά με την κάλυψη των κινδύνων κυβερνοχώρου. Ορισμένοι Ασφαλισμένοι μπορεί να θεωρούν ότι έχουν επαρκή κάλυψη για κινδύνους κυβερνοχώρου, ενώ στην πραγματικότητα αυτό δεν ισχύει. Επιπλέον, ένα λεκτικό «μη επιβεβαιωμένου» κινδύνου κυβερνοχώρου σε ένα παραδοσιακό συμβόλαιο, μπορεί να γίνει αντικείμενο διαφορετικών ερμηνειών από τις Ασφαλιστικές Εταιρίες, πράγμα το οποίο θα οδηγήσει σε διαμάχες.

Γιατί προβληματίζονται οι Ασφαλιστικές Εταιρίες για το Σιωπηρό Κίνδυνο Κυβερνοχώρου

Οι Ασφαλιστικές Εταιρίες και οι Εθνικές Ρυθμιστικές Αρχές ανησυχούν για το ότι ο Σιωπηρός Κίνδυνος Κυβερνοχώρου μπορεί να αντιπροσωπεύει ένα σοβαρό και μη αναμενόμενο κίνδυνο στα χαρτοφυλάκια των Ασφαλιστών. Μια Ασφαλιστική Εταιρία που χρησιμοποιεί ένα λεκτικό «μη επιβεβαιωμένου» κινδύνου κυβερνοχώρου δεν θα μπορούσε να είχε υπολογίσει τον πιθανό κίνδυνο κυβερνοχώρου που ακούσια καλύπτεται, και επομένως δεν μπορεί να έχει μετρήσει την αυξημένη έκθεση του Ασφαλισμένου ή να έχει προσαρμόσει το ασφάλιστρο ανάλογα, ή να έχει υπολογίσει την πιθανή συγκέντρωση κινδύνου στο χαρτοφυλάκιό της.

Το πρόβλημα της συσσώρευσης (accumulation) Σιωπηρού Κινδύνου Κυβερνοχώρου

Σύμφωνα με τα ως άνω, το μεγαλύτερο πρόβλημα που παρουσιάζει για την ασφαλιστική αγορά ο Σιωπηρός Κίνδυνος Κυβερνοχώρου είναι ο κίνδυνος συσσώρευσης (accumulation). Η συσσώρευση κινδύνου από μόνο το cyber ως αυτοτελώς ασφαλιζόμενο κίνδυνο είναι ήδη θέμα, αλλά αυτό είναι μικρό πρόβλημα μπροστά στη συγκέντρωση του κινδύνου cyber από διάφορους κλάδους ασφάλισης.

Σε έναν κόσμο που όλο κα περισσότερο στηρίζεται στην ψηφιακή τεχνολογία, είναι δύσκολο να σκεφτούμε έναν κλάδο ασφάλισης που δεν επηρεάζεται με κάποιο τρόπο από τον κίνδυνο cyber. Όμως το λεκτικό των περισσότερων ασφαλιστηρίων γράφτηκαν στην προ – ψηφιακή εποχή και σε αρκετές περιπτώσεις δεν έχει γίνει ακόμη επεξεργασία τους, ώστε να αντιμετωπίζουν ρητά την αναδυόμενη έκθεση που προκύπτει από τη χρήση της ψηφιακής τεχνολογίας. Αυτό οδηγεί σε μια τεράστια γκρίζα περιοχή όπου η κάλυψη του κινδύνου cyber πιθανόν να παρέχεται από συμβόλαια, τα οποία αρχικά δεν σχεδιάστηκαν για αυτή την κάλυψη.

Αξίζει να τονιστεί, ότι ο κίνδυνος cyber δεν γνωρίζει γεωγραφικά όρια, πράγμα που τον κάνει δυνητικά τον πιο επικίνδυνο από άποψη συσσώρευσης. Για τους καταστροφικούς κινδύνους φυσικών φαινομένων, όπως για παράδειγμα οι τυφώνες, η συγκέντρωση κινδύνου είναι περιορισμένη από γεωγραφικές παραμέτρους. Ο κίνδυνος cyber όμως δεν έχει γεωγραφικούς περιορισμούς – ολόκληρη η γη είναι μια ζώνη CAT ως προς το cyber. Αυτό επιδεινώνει τους κινδύνους από τον Σιωπηρό Κίνδυνο Κυβερνοχώρου και το καθιστά μείζον

θέμα που απασχολεί ασφαλιστές, αντασφαλιστές, ρυθμιστικές αρχές και οίκους αξιολόγησης.

Τι πρέπει να κάνουν οι Ασφαλιστικές Εταιρίες

Οι Ασφαλιστικές Εταιρίες έχουν αρχίσει να ασχολούνται με το θέμα του silent cyber. Σε ορισμένες χώρες αυτό έχει ζητηθεί από τις Εθνικές Ρυθμιστικές Αρχές. Κάποιες Ασφαλιστικές Εταιρίες έχουν κάνει ξεκάθαρη την πρόθεσή τους με το να ορίσουν τον κίνδυνο του κυβερνοχώρου και κατόπιν να τον εξαιρέσουν από τα non cyber ασφαλιστήρια συμβόλαια. Άλλες Ασφαλιστικές Εταιρίες αρχίζουν να χρησιμοποιούν νέο λεκτικό και νέες οδηγίες ανάληψης. Για παράδειγμα στο Ηνωμένο Βασίλειο ήδη η Ρυθμιστική Αρχή (Prudential Regulation Authority) είχε ζητήσει από το 2019 ένα σχέδιο δράσης από τους Ασφαλιστές, ενώ οι Lloyd's έχουν ζητήσει από τους Ασφαλιστές είτε να εξαιρούν ρητά είτε να καλύπτουν ρητά τον κίνδυνο cyber στα παραδοσιακά ασφαλιστήρια, από τον Ιανουάριο του 2020.

Η σύντομη προθεσμία οδήγησε τους περισσότερους στο να περιλάβουν εξαιρέσεις στα παραδοσιακά συμβόλαια. Όμως σε αρκετές περιπτώσεις το λεκτικό είναι ασαφές, έρχεται σε αντίθεση με άλλα σημεία του συμβολαίου και σε κάποιες περιπτώσεις τόσο ευρύ, ώστε καταλήγει να εξαιρεί αιτίες ζημιάς που καλύπτονταν πριν την εξαίρεση, μόνο και μόνο επειδή στην αλυσίδα της αιτίας ζημίας εμπλέκεται η τεχνολογία. Το νέο λεκτικό δεν πρέπει να παραβλέπει το γεγονός ότι η τεχνολογία είναι ενσωματωμένη στις επιχειρηματικές διαδικασίες και λειτουργίες όλων των τομέων δραστηριότητας.

Κατά την προσέγγιση του κινδύνου κυβερνοχώρου πρέπει να ληφθεί μέριμνα να περιοριστούν τα κενά και οι επικαλύψεις και να μεγιστοποιηθεί το εύρος της κάλυψης. Σε περίπτωση κάλυψης, πρέπει να υιοθετηθεί θετική φρασεολογία, η οποία να παρέχει πλήρη κάλυψη στα παραδοσιακά συμβόλαια, δηλαδή για παράδειγμα, να διασφαλίζεται ότι καλύπτεται υλική ζημιά ανεξάρτητα από την εμπλοκή τεχνολογίας στην αιτία της ζημιάς. Επίσης πρέπει να ορίζονται οι κακόβουλες και μη κακόβουλες πράξεις και να περιγράφεται η φυσική και μη φυσική ζημιά. Η μη φυσική ζημιά μπορεί να εξαιρείται εάν καλύπτεται από ασφαλιστήριο συμβόλαιο κυβερνοχώρου.

Η αξιολόγηση κινδύνων που δεν αναγράφονται καταφατικά στα ασφαλιστήρια συμβόλαια περιουσίας, ευθυνών και διαφόρων κινδύνων, όπως για παράδειγμα marine και aviation, είναι ένας διαρκής κύκλος. Νέοι κίνδυνοι προκύπτουν και θα προκύπτουν συνέχεια όσο η τεχνολογία προχωράει και εξελίσσεται.