Αθήνα, 15/11/2021

Δελτίο Τύπου

Το Cyber Insurance, βασικό μέρος της λύσης για την αντιμετώπιση των αυξανόμενων κυβερνοαπειλών

Cyber Insurance & Incident Response Conference 2021

Επίκαιρο όσο ποτέ ήταν το φετινό Cyber Insurance & Incident Response Conference, που πραγματοποιήθηκε στις 11 Νοεμβρίου 2021 και είχε θέμα: "Ransomware Ready". Το συνέδριο διοργανώθηκε για τρίτη συνεχόμενη χρονιά από **την ethosEVENTS**, σε συνεργασία με το οικονομικό & επιχειρηματικό portal **banks.com.gr**, το ασφαλιστικό περιοδικό **Insurance World** και το portal **insuranceworld.gr**, και ήταν μία ψηφιακή παραγωγή με την τεχνολογία **LiveOn**, από το **καινοτόμο 3D εκθεσιακό και συνεδριακό της κέντρο**, το **LiveOn Expo Complex**.

Η έλευση της πανδημίας σε συνδυασμό με την ευρεία χρήση των νέων τεχνολογιών από οργανισμούς και επιχειρήσεις δημιουργούν ένα τοπίο αυξανόμενων cyber κινδύνων. Ειδικότερα, περισσότεροι από **30 διακεκριμένοι ομιλητές με πολυετή παρουσία στην εγχώρια και διεθνή αγορά** ασχολήθηκαν, μεταξύ άλλων, **με τα περιστατικά που απασχολούν τη παγκόσμια κοινότητα, τη διαχείριση των κινδύνων και τις αξιώσεις μετά από ένα γεγονός**. Ανέλυσαν το **νομοθετικό πλαίσιο, τις βέλτιστες πρακτικές** ως «απάντηση» των εν λόγω απειλών και **τον κρίσιμο ρόλο του Cyber Insurance ως ένα βασικό μέρος της λύσης για τη διαχείριση του κινδύνου.**

Στο χαιρετισμό του, ο CEO του ethosGroup, κ. **Κωνσταντίνος Ουζούνης** ανέδειξε τη σημαντικότητα του συνεδρίου ως ένα πρωτοποριακό event που αφορά την εξέλιξη των ελληνικών και διεθνών επιχειρήσεων. «*Το cyber insurance συνολικά ως θέμα είναι ένα μεγάλο κομμάτι του risk management, γεγονός που αφορά όλους τους οργανισμούς*», σημείωσε.

«*Κάθε περιστατικό ασφάλειας γεννά μια κρίση. Η πληροφορία αποτελεί το πιο σημαντικό στοιχείο μιας επιχείρησης*», τόνισε μεταξύ άλλων, ο κ. **Νίκος Γεωργόπουλος** Cyber Privacy Risks Insurance Advisor, Cromar Insurance Brokers Ltd – Lloyd's Cover Holder. Τα περιστατικά παραβίασης ασφάλειας αποτελούν πλέον στοιχείο της καθημερινότητας και η αντιμετώπισή τους απαιτεί τη βοήθεια εξειδικευμένων συμβούλων. Ωστόσο, είναι απαραίτητη πλέον η πρόληψη και λήψη μέτρων ασφαλείας για τη προστασία του πιο σημαντικού στοιχείου μιας εταιρείας: τη πληροφορία. «*Η μεγαλύτερη αξία ενός ισολογισμού, γύρω στο 80%, αφορά τα άυλα περιουσιακά στοιχεία μιας εταιρείας (πληροφορία, δεδομένα, πατέντες), στοιχεία που είναι συνήθως ανασφάλιστα*», σημείωσε.

«*Η εμφάνιση της πανδημίας ανέδειξε με τον πιο εμφατικό τρόπο τη σημασία της ψηφιοποίησης προκειμένου οι κοινωνίες να μπορέσουν να δουλέψουν στις ειδικές συνθήκες που διαμορφώθηκαν. Παρότι*

ethosEVENTS
Lysikratous 64 | GR 17674, Kallithea, Athens
T: (+30) 210 998 4950,
E: info@ethosevents.eu, **W**: www.ethosevents.eu

τα οφέλη, ασυζητητί, είναι προφανή, η αυξανόμενη εξάρτηση οδηγεί αναπόφευκτα σε αύξηση των κινδύνων στην ψηφιακή ασφάλεια και την πιθανότητα ψηφιακών εγκλημάτων», τόνισε από τη πλευρά της η Γενική Διευθύντρια της Ένωσης Ασφαλιστικών Εταιρειών Ελλάδος (Ε.Α.Ε.Ε), κα **Μαργαρίτα Αντωνάκη.** Όπως τόνισε, «η επίθεση με κακόβουλο λογισμικό αποτελεί την Νο1 απειλή στον κυβερνοχώρο, σε όλη την ΕΕ. Πρωταγωνιστικό ρόλο σε αυτή την αγορά έχει η αγορά των ΗΠΑ όπου σημειώνεται κατακόρυφη άνοδος των ασφαλίστρων. Ωστόσο, είναι ακόμη νωρίς για να εκτιμηθούν το ύψος των μελλοντικών ζημιών στο κυβερνοχώρο, που μπορούν να πυροδοτήσουν μια αλυσίδα σχετιζόμενων κινδύνων. Ο ρόλος της ασφαλιστικής αγοράς είναι σημαντικός καθώς: καθοδηγεί τους πελάτες με οδηγίες πρόληψης, αποζημιώνει, παρέχει νομική υποστήριξη για τη καλύτερη διαχείριση». **Από τη πλευρά της η ΕΑΕΕ έχει δημιουργήσει έναν οδηγό ασφάλισης Cyber κινδύνων, ενώ ετοιμάζει και άλλες δράσεις με στόχο την ενημέρωση και τη καλύτερη θωράκιση από τέτοιες απειλές.**

Σχεδόν **20 γνωστοποιήσεις το μήνα λαμβάνει η Αρχή Προστασίας Δεδομένων Προσωπικού χαρακτήρα** από την αρχή του 2021, γεγονός που αποτελεί μια **κατακόρυφη αύξηση των παραβιάσεων**. Αυτό σημείωσε από τη πλευρά της Εποπτικής Αρχής ο Δρ Μηχ. Η/Υ και Πληροφορικής, ΕΕΠ της Αρχής, κ. **Γεώργιος Ρουσόπουλος. Το μεγαλύτερο κομμάτι των παραβιάσεων εντοπίζεται στον ιδιωτικό τομέα έναντι του δημοσίου, ενώ το 30% των επιθέσεων αφορούν υποθέσεις ransomware.** *«Ενδιαφέρον στοιχείο είναι να δούμε πόσα φυσικά πρόσωπα επηρεάζονται από περιστατικά παραβίασης προσωπικών δεδομένων. Όσο περισσότερα πρόσωπα (πελάτες-συνεργαζόμενοι) τόσο μεγαλύτερος είναι ο κίνδυνος για μια επιχείρηση»* είπε.

Την ασφαλή και καινοτόμο **πλατφόρμα ολοκληρωμένης ψηφιακής επικοινωνίας LiveON** παρουσίασε ο κ. **Ορέστης Φοίβος Πιτσάβας**, Head of Business Development, LiveOn. Όπως επισήμανε, «η **κυβερνοασφάλεια είναι βασικό στοιχείο της πλατφόρμας.** Η LiveOn μεταμορφώνει πλήρως ολόκληρη την εμπειρία της επιχειρηματικής σχέσης σε κάθε είδους εκδήλωση, είτε πλήρως ψηφιακή είτε υβριδική, διασφαλίζοντας ότι οι επιχειρήσεις και οι συμμετέχοντες απολαμβάνουν μοναδικές ευκαιρίες για ενδιαφέρον περιεχόμενο, επαγγελματική δικτύωση και στοχευμένη προώθηση, χωρίς τους περιορισμούς (ταξίδια, χώρος κ.λπ.) των φυσικών εκδηλώσεων και σε κλάσμα του κόστους τους.»

Τις διεθνείς τάσεις της αγοράς γύρω από το Cyber Insurance ανέδειξε σε ομιλία του ο κ. **Nick Economidis**, Vice President, eRisk, Crum & Forsterμ αναλύοντας, μεταξύ άλλων, **τρόπους ώστε να τεθεί υπό έλεγχο το κυβερνοέγκλημα: με εξειδικευμένη εκπαίδευση και κατανόηση, επιλύοντας ζητήματα συστημικού κινδύνου.**

Την ανάγκη εκπαίδευσης και κατανόησης των πελατών και των στελεχών εταιριών για την ασπίδα που προσφέρουν οι υπηρεσίες του Cyber Insurance σε ένα περιβάλλον που ψηφιοποιείται ταχύτατα και μεταβάλλεται διαρκώς, προέβαλαν οι ειδικοί του **πρώτου Πάνελ του συνεδρίου,** με τίτλο **«Τάσεις και Προοπτικές της Αγοράς ασφάλισης Cyber Insurance»**, το οποίο συντόνισε ο κ. **Νίκος**

Γεωργόπουλος, Cyber Privacy Risks Insurance Advisor, της Cromar Insurance Brokers Ltd. Στο πάνελ μετείχαν οι κ.κ. **Κώστας Βούλγαρης** Financial Lines Manager της AIG, **Σπύρος Λαθούρης**, IT Security & Cyber Risks Expert, του Ομίλου Howden Matrix και η κα **Δήμητρα Ξηντάρα**, Senior Cyber Risk Strategist, του Ομίλου Eurolife FFH.

Όπως τόνισαν, μεταξύ άλλων, οι ομιλητές **το Cyber Insurance είναι ένα προϊόν αξίας που προσφέρει περισσότερα από όσο κοστίζει και «ενηλικιώνεται σταθερά όσο η αγορά ωριμάζει».** Ωστόσο, οι μικρότερες επιχειρήσεις δεν έχουν αντιληφθεί τη σπουδαιότητα του κινδύνου. Γενικότερα, **υπάρχει ανάγκη εκπαίδευσης** για να κατανοήσουν οι πελάτες ότι, π.χ. στο Cloud, ανάλογα με το μοντέλο που επέλεξαν και μπορεί να είναι υβριδικό, μπορεί να έχουν και οι ίδιοι μερίδιο του κινδύνου. Ειδικότερη αναφορά έγινε για **το ζήτημα του underwriting**, καθώς οι πελάτες είναι υποχρεωμένοι να ακολουθήσουν οδηγίες και όρους που αναλύονται σε μακροσκελή απαιτητικά τεχνικά κείμενα, με πολλές λεπτομέρειες οι οποίες πρέπει να εφαρμοστούν. Σήμερα, η αγορά βρίσκεται σε φάση παραμετρικού underwriting: πολλοί παράγοντες πρέπει να υπολογιστούν σωστά και τελικά ενδέχεται να μην είναι όλοι οι κίνδυνοι ασφαλίσιμοι.

Διαρκής είναι η **αύξηση των περιστατικών ransomware** όπως είπε, επίσης, ο κ. **Antonis Patrikios**, Partner, Privacy & Cybersecurity, Dentons. «*Οι εγκληματίες ψάχνουν να βρουν αδυναμίες ώστε να διεισδύσουν στο δίκτυο και στη συνέχεια είτε ζητούν λύτρα είτε κλέβουν δεδομένα*». Εκτιμάται πως στο 25% ransomware επιθέσεων οι επιχειρήσεις-θύματα αποφασίζουν να πληρώσουν. Όμως ακόμη κι αυτό, σύμφωνα με τον ίδιο «δεν μας εξασφαλίζει ότι θα αποκτήσουμε πίσω τα δεδομένα μας και πως όλα θα τελειώσουν». Παράλληλα, ανέδειξε το γεγονός ότι σε αρκετά περιστατικά οι επιπτώσεις των επιθέσεων αφορούν παραπάνω από μία δικαιοδοσίες, υπάρχουν διεθνή περιστατικά, που ενέχουν ένα επιπλέον επίπεδο πολυπλοκότητας. Κατά τα άλλα, το cyber crime έχει εξελιχθεί σε ένα δύσκολο θέμα για τις ασφαλιστικές, γιατί ο αριθμός των περιστατικών που καλούνται να καλύψουν ως αποζημιώσεις είναι αρκετά μεγάλος.

Εξειδικευμένα ζητήματα γύρω από τη **Νομοθεσία και τη Συμμόρφωση** απασχόλησαν το **δεύτερο Πάνελ** του συνεδρίου. Συμμετείχαν ο κ. **Antonis Patrikios**, Partner, Privacy & Cybersecurity, Dentons, ο κ. **Απόστολος Βόρρας**, Εταίρος και Επικεφαλής του Τμήματος Data Protection & Digital Technologies, Δικηγορική Εταιρεία Κοϊμτζόγλου – Μπακάλης – Βενιέρης – Λεβέντης & Συνεργάτες (Μέλος του Δικτύου Δικηγορικών Εταιρειών Deloitte Legal), ο κ. **Ιωάννης Γιαννακάκης**, Group General Counsel & Chief Compliance Officer, Avramar Group και η κα Μίνα Ζούλοβιτς, Partner Lawyer at Zoulovits Kontogeorgo Law Firm. Συντονιστής ήταν ο δικηγόρος κ. **Τάκης Κακούρης**.

Ιδιαίτερες αναφορές έγιναν σε ζητήματα κουλτούρας και εξειδίκευσης, ενώ επισημάνθηκε πως πολλές φορές ότι υπάρχει σύγχυση σε έναν οργανισμό για το ρόλο του DPO. Κατά τους ομιλητές πρέπει να «αποενοχοποιηθεί» το γεγονός ότι κάποιος έπεσε θύμα παραβίασης, καθώς δεν θα πρέπει να λογίζεται ως ένα γεγονός που αμαυρώνει τη φήμη μιας εταιρείας. Επίσης, περιέγραψαν τα βήματα για το ποιες ενέργειες

πρέπει να λάβουν χώρα αν συμβεί μία επίθεση, και στηλίτευσαν το γεγονός πως αρκετοί προσπαθούν να γνωστοποιήσουν τα περιστατικά σε χώρες όπου οι Αρχές είναι πιο ελαστικές με τα πρόστιμα.
Κατά γενική ομολογία, οι επιθέσεις αυξάνονται και σε ΜμΕ οι οποίες, καθώς δεν έχουν πολλά περιθώρια επιλογής, θα πρέπει να αναζητήσουν τις κατάλληλες ασφαλιστικές καλύψεις. Στην ελληνική πραγματικότητα, υπάρχει άρνηση κατ' αρχήν ή δισταγμός των οργανισμών να γνωστοποιήσουν τα περιστατικά, παρά την ύπαρξη της νομικής υποχρέωσης.

Σε ειδική παρουσίαση ο κ. **David Derigiotis**, Corporate Senior Vice President and National Professional Liability Practice Leader, Burns & Wilcox ανέλυσε τα τελευταία δεδομένα και ειδικότερα πώς το ransomware επηρεάζει ιδιώτες, επιχειρήσεις και μεγάλους οργανισμούς ξεχωριστά. Κατά τον ίδιο, πρόκειται το Ransomware αποτελεί το μεγαλύτερο «πονοκέφαλο» που πρέπει να απασχολεί το Cyber Insurance. Σύμφωνα με στοιχεία του FBI το 2020 οι απώλειες από τέτοιες επιθέσεις αυξήθηκαν εκ νέου και διαμορφώθηκαν στα 4,2 δις δολάρια και οι κυβερνοεγκληματίες αναμένεται να εκμεταλλευτούν το γεγονός πως πλέον όλοι εργάζονται και απασχολούνται διαδικτυακά. Αξιοσημείωτο είναι το γεγονός πως ενώ στο παρελθόν η Ελλάδα δεν ήταν στις σχετικές λίστες αναφοράς για το cyber crime, βρέθηκε στην 4η θέση (επιθέσεις ανά πληθυσμό).

Τους **τεχνολογικούς και cyber κινδύνους ανά κλάδο** ανέλυσε στην ομιλία του ο κ. **Alex King**, Cyber & Tech Underwriter, Beazley με τίτλο «Technology Risk and Resilience. Σύμφωνα με τα συμπεράσματα σχετικής έρευνας, **οι cyber κίνδυνοι είναι πλέον αισθητά υψηλότεροι, αλλά οι εταιρείες αισθάνονται πιο έτοιμες να τον διαχειριστούν**. Κάτι άλλο που πρέπει να απασχολεί είναι η αποτυχία στην υιοθέτηση νέων τεχνολογιών καθώς κάποιοι οργανισμοί δεν συμβαδίζουν με τις εξελίξεις. Επίσης, οι σωστές προσλήψεις στελεχών και οι κατάλληλες επενδύσεις αποτελούν «κλειδί» στο νέο αυτό τοπίο. Τέλος, η έννοια της ανθεκτικότητας είναι κάτι που συνεχώς μεταβάλλεται.

Στο **Maritime Cyber Insurance** εστίασε κατά την ομιλία του ο κ. **Sarif Gardner**, Head of Training and Advisory Services, AXIS Capital. Όπως εξήγησε απαιτείται «κοινή γλώσσα» ανάμεσα στους ανθρώπους που ασχολούνται με την ναυτιλία και τους ειδικούς του cyber insurance ώστε να υπάρξει πρόοδος και συνεργασία σε αυτό τον τομέα. Αναλύοντας τον θαλάσσιο κυβερνοχώρο, σύμφωνα με τον ίδιο, απειλές μπορούν να υπάρξουν σε οποιαδήποτε επιχείρηση της εφοδιαστικής αλυσίδας, να υπάρχει διακοπή εργασιών και οποιαδήποτε cyber επίθεση σε σκάφος όπως συμβαίνει στη στεριά. Στην αγορά ασφάλισης υπάρχουν καλύψεις όπως θαλάσσιες cyber παραβιάσεις, αποτυχία διασύνδεσης, καλύψεις για επιθέσεις ransomware και εκβιασμών, απώλεια εισοδήματος και επιπλέον έξοδα από αποτυχία εξωτερικού παρόχου, ασφάλεια διασύνδεσης και ευθύνη απορρήτου, ζημιά φορτίου πελάτη/αλλοίωση ή περιορισμός φορτίου και πολλά άλλα.

Σημαντικούς ομιλητές είχε και το **τρίτο Πάνελ** με τίτλο **«Cyber Risks Management & Cyber Claims»** και συντονιστή τον κ. **Χρήστο Ξενάκη**, Καθηγητή στο Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου

Πειραιώς. Συμμετείχαν οι κ. **Theodoros Bitis**, Head of Cyber Center ofExcellence, Howden Germany, κ. **Νότης Ηλιόπουλος**, Director, Cyber Security Services, κ. **Χρόνης Καπαλίδης**, Principal, Information Security Forum, κα. **Παναγιώτα Λαγού**, Senior Manager, Cyber Security Consulting, Adacom S.A και ο κ. **Χριστόφορος Παπαχρήστου**, Strategic Account Manager, Census Labs. Μεταξύ άλλων, επισημάνθηκε πως **για την ασφάλιση cyber κινδύνων ελέγχεται η διακυβέρνηση και η πολιτική των εταιρειών** (phising campaigns, tests) και άλλοι παράμετροι, ώστε οι ασφαλιστικές να προχωρήσουν στις απαιτούμενες καλύψεις. Σοβαρό ζητούμενο είναι πως στις μέρες μας πως **οι διάφοροι τύποι των ιών στο διαδίκτυο μεταλλάσσονται, δημιουργώντας ενδεχομένως μια μεικτή απειλή**. Αξιοσημείωτο είναι, επίσης, πως τα ανθρώπινα λάθη είναι συχνά και για αυτό το λόγο απαιτείται περαιτέρω εκπαίδευση, ενώ τονίστηκε πως η «υπερβολική εμπιστοσύνη ότι τα αυτόματα συστήματα λειτουργούν επαρκώς, δημιουργεί κενά που μπορούν να εκμεταλλευτούν οι hackers». Επισημάνθηκε, πως οι cyber απειλές δεν είναι κάτι που πρέπει να προβληματίζει μόνο το IT, αλλά το σύνολο μιας επιχείρησης και των εργαζομένων. Όπως είπαν οι ομιλητές, ο στρατηγικός σχεδιασμός ενός οργανισμού σήμερα πρέπει να πηγαίνει «χέρι χέρι» με το cyber security.

Τίποτα δεν είναι ασφαλές 100% σύμφωνα με τον κ. **Αργύρη Μακρυγεώργου**, υπεύθυνο μελών του Ελληνικού Chapter (ISC)2 όπως σημείωσε στην ομιλία του με τίτλο **«IR: Not your standard last-minute hotel deal».** Μίλησε, ειδικότερα, για το «πριν και το μετά» ενός περιστατικού ασφαλείας το οποίο μπορεί να έχει κάθε έκταση. Σε κάθε περίπτωση, χωρίς την κατάλληλη προετοιμασία, δεν θα μπορεί να υπάρξει επιτυχής αντιμετώπιση. «Το γεγονός πλέον δεν είναι αν θα συμβεί κάτι, αλλά το πότε», σημείωσε χαρακτηριστικά.

Πόσο σημαντική είναι τελικά η ύπαρξη ενός πλάνου αντιμετώπισης περιστατικών; Τη διαχείριση περιστατικών παραβίασης ασφαλείας έθεσε επί τάπητος ο κ. **Θεόδωρος Στεργίου**, Director, Cyber Security Consulting, KPMG in Greece. Όπως τόνισε, μεταξύ άλλων, είναι κρίσιμο να απαντηθούν ερωτήματα όπως: ποιος είναι τελικά ο σκοπός του πλάνου, πώς καθορίζονται οι στόχοι του, τι συνεπάγεται η ανάθεση ρόλων, ποια η σύνδεση του με την επιχειρησιακή συνέχεια και την ανθεκτικότητα της εταιρείας, πώς εκπαιδεύονται όλα τα εμπλεκόμενα μέρη ή πως εν τέλει δοκιμάζεται το πλάνο κ.ά.

Με την αντιμετώπιση των περιστατικών ασχολήθηκαν, μεταξύ άλλων, οι ομιλητές του **τέταρτου Πάνελ,** στο οποίο συντονιστής ήταν ο κ. **Δημήτρης Γεωργόπουλος**, Founder – CEO, Rethink Business Lab-RBL. Συμμετείχαν ο κ. **Νίκος Γεωργόπουλος**, ο κ. **Θεόδωρος Στεργίου**, ο κ. **George Platsis**, Senior Lead Technologist, Proactive Incident Response & Resiliency, Booz Allen Hamilton, ο κ. **Κωνσταντίνος Παπαδάτος**, Founder & Managing Director, Cyber Noesis και ο κ. **Ανάργυρος Χρυσάνθου**, Ερευνητής και Ειδικός Ανάλυσης Ψηφιακών Πειστηρίων, Ερευνητικό Κέντρο Αθήνα. Όπως τόνισαν, υπάρχει μια **τάση μη πληρωμής λίτρων και επένδυσης σε υπηρεσίες που θα συμβάλλουν στην ανάκαμψη μετά το «χτύπημα».** Αυτή τη στιγμή παίζει καθοριστικό ρόλο ο covid στην επανεκκίνηση της αγοράς, η οποία είναι απαραίτητη, μετά την ένταση της ψηφιοποίησης. Χρειάζεται, επίσης, πολλή προσοχή, γιατί οι μορφές των επιθέσεων μεταβάλλονται συνεχώς, καθιστώντας δύσκολη την ανίχνευση. Κρίσιμο στοιχείο είναι το γεγονός

πως κάθε οργανισμός που δέχεται επίθεση, ασχέτως αποτελέσματος, πρέπει να ξεχάσει τον πρότερο τρόπο λειτουργίας του. Τέλος, επισημάνθηκε πως κατά τη διάρκεια αντιμετώπισης τέτοιων περιστατικών γίνονται – και – λάθος χειρισμοί με αποτέλεσμα να χάνονται πολύτιμες ώρες και δεδομένα μιας επιχείρησης.

Για πληροφορίες μπορείτε να επισκεφτείτε την επίσημη ιστοσελίδα του συνεδρίου https://ethosevents.eu/event/cyber-insurance-amp-incident-response-conference-2021/ καθώς επίσης και τα social κανάλια Facebook, LinkedIn, και YouTube.

Για περισσότερες πληροφορίες:

κ. Παπασπηλιωτοπούλου Αλεξάνδρα, PR & Marketing Communications Manager, ethosGROUP, τηλ. 210 9984 917, e-mail: papaspiliotopoulou.a@ethosmedia.eu