Αθήνα, 6 Νοεμβρίου 2020

ΔΕΛΤΙΟ ΤΥΠΟΥ

Ο καθοριστικός ρόλος του Cyber Insurance κατά των κυβερνοαπειλών

Με μεγάλη επιτυχία ολοκληρώθηκε το 2nd Cyber Insurance & Incident Response Conference. Το συνέδριο πραγματοποιήθηκε **μέσα από τη LiveOn,** την ολοκληρωμένη ψηφιακή τεχνολογία επιχειρηματικής επικοινωνίας του **ethosGROUP** και διοργανώθηκε για **δεύτερη χρονιά** από την **ethosEVENTS**, σε συνεργασία με το οικονομικό & επιχειρηματικό portal **banks.com.gr**, το ασφαλιστικό περιοδικό **Insurance World** και το portal **insuranceworld.gr.**

Στο επίκεντρο της συζήτησης του Συνεδρίου βρέθηκαν **οι κίνδυνοι που επηρεάζουν την καθημερινή λειτουργία μιας εταιρείας**, οι οποίοι μπορούν να απειλήσουν την ομαλή λειτουργία και τη διαθεσιμότητα των συστημάτων της, να επιφέρουν σημαντικές επιβαρύνσεις στα οικονομικά της αποτελέσματα και τη φήμη της, καθώς και να βοηθήσει την ανάπτυξη της αγοράς της ασφάλισης cyber insurance, **αναδεικνύοντας τη σημαντικότητά της ως εργαλείο διαχείρισης κινδύνου.**

«Κανένας δεν πρέπει να θεωρεί τον εαυτό του ασφαλή και οφείλει να γνωρίζει πως να αντιδράσει και θωρακιστεί απέναντι στον κίνδυνο», δήλωσε η κ. **Μαργαρίτα Αντωνάκη**, *Γενική Διευθύντρια, Ένωση Ασφαλιστικών Εταιρειών Ελλάδος (ΕΑΕΕ)* κατά την έναρξη του Συνεδρίου. «Από την πλευρά των υπευθύνων χάραξης πολιτικής της Ευρωπαϊκής Ένωσης, η Ursula von der Leyen έχει δεσμευτεί να συνθέσει και να ενισχύσει τους διάσπαρτους νομοθετικούς κανόνες που ισχύουν στην Ευρωπαϊκή Ένωση για την ασφάλεια στον κυβερνοχώρο, δίδοντας έμφαση στην ενίσχυση της «ψηφιακής λειτουργικής ανθεκτικότητας» του χρηματοπιστωτικού τομέα, ο οποίος αναμένεται να βρεθεί στο επίκεντρο των κυβερνοεπιθέσεων. Η Ευρωπαϊκή Επιτροπή έχει ήδη αναλάβει νομοθετική πρωτοβουλία προς αυτήν την κατεύθυνση, για την οποία βρίσκεται σε συνεχείς διαβουλεύσεις με όλους τους φορείς του χρηματοπιστωτικού τομέα, συμπεριλαμβανομένης της ασφαλιστικής αγοράς», τόνισε. **«Η ασφαλιστική βιομηχανία** από την άλλη πλευρά **κατέχει μια μοναδική θέση**, τόσο **ως τομέας** που αποτελεί στόχο κυβερνοεπιθέσεων και επομένως πρέπει να ενισχύσει την ανθεκτικότητά του, αλλά και ως δραστηριότητα που μπορεί **να προσφέρει προστασία** σε άλλες επιχειρήσεις μέσω μιας **σειράς προϊόντων ασφάλισης** κατά των κινδύνων

του κυβερνοχώρου. Η ασφάλιση κατά των κινδύνων του κυβερνοχώρου **παίζει αναμφίβολα καθοριστικό ρόλο** στην προσπάθεια μικρών και μεγάλων επιχειρήσεων να ενισχύσουν την ανθεκτικότητάς τους στον κυβερνοχώρο, προσφέροντας πολλές διαφορετικές υπηρεσίες, **τόσο πριν όσο και μετά από ένα περιστατικό Cyber**», είπε μεταξύ άλλων.

«Τα δεδομένα (data) αποτελούν το αγαθό με την μεγαλύτερη αξία», τόνισε ο **Δρ Κώστας Λαμπρινουδάκης**, *Καθηγητής, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιώς & Τακτικό μέλος, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*. Για τον ίδιο, είναι σαφές ότι μπήκαμε στην εποχή του datism και παρέθεσε παραδείγματα για το κόστος της κυβερνοαπάτης που έχει ξεπεράσει το 1,5 τρις δολάρια, ενώ περί τα 7 δισεκατομμύρια ανέρχονται τα κλεμμένα διαπιστευτήρια με μεγαλύτερη και σοβαρότερη περίπτωση αυτή της υποκλοπής στην υπόθεση της Yahoo. «Το πρόβλημα προκύπτει διότι βλέπουμε αύξηση στην ευπάθεια των συστημάτων. Με την αύξηση των ευπαθειών αυξάνεται η τάση και των κακόβουλων λογισμικών. Είναι σαφές ότι οι επιχειρήσεις πρέπει να κατανοήσουν τις απαιτήσεις ασφάλειας για όλα τα συστήματά τους και να τα προστατέψουν», τόνισε.

Αύξηση των κυβερνοχυπημάτων ransomware, μεταξύ άλλων, διαβλέπει ο κ. **Nicholas Economidis**, *eRisk Insurance Underwriter, Crum & Forster* αλλά και **διψήφιες αυξήσεις** στα ασφάλιστρα έναντι των cyber κινδύνων. Όπως εξήγησε, η συλλογή των εσφαλμένων πληροφοριών οδηγεί στην σύνταξη νέων νομοθεσιών προκειμένου να προστατευτούν τα δεδομένα. «Όλοι θα πρέπει να αγοράζουν καλύψεις κυβερνοκινδύνων, θα πρέπει να υπάρχει διαφάνεια στον κυβερνοχώρο. Όλοι οι ασφαλιστές του κλάδου Περιουσίας και Ατυχημάτων θα πρέπει να έχουν ένα capacity κινδύνων, όπως σε περιπτώσεις πυρκαγιάς για παράδειγμα που χάνονται πολλά δεδομένα», τόνισε. Μεγάλες είναι, επίσης, οι ανησυχίες για τα «χτυπήματα» στις κάρτες πληρωμών. Αρκετές επιχειρήσεις δεν ασφαλίζονται καθώς πιστεύουν ότι το περιστατικό δεν θα συμβεί σε αυτούς. Την ίδια ώρα, πληθαίνουν οι φόβοι για την διαρροή βιομετρικών δεδομένων. Βάσει εκτιμήσεων, η αγορά της κυβερνοασφάλειας αναμένεται να διαμορφωθεί στα 7,8 δις. ευρώ το 2020.

Έμφαση στις επιθέσεις ransomware στα συστήματα Υγείας έδωσε, μεταξύ άλλων, ο **David Derigiotis**, *Corporate Senior Vice President and National Professional Liability Practice Leader, Burns & Wilcox | CIPP/US, CIPM*. Γενικότερα το τοπίο αλλάζει δραστικά αν αναλογιστεί κανείς ότι 24 εκατ. συσκευές IoT, ενώ θα διακινούνται 2,9 εκατ. mails το δευτερόλεπτο. Σήμερα, το 60% των επιχειρήσεων στο κόσμο μετασχηματίζεται ψηφιακά. Σε αυτό το πλαίσιο, εξήγησε, για όλους του

κλάδους οι κίνδυνοι και οι τρόποι ασφάλισης έχουν αλλάξει. Για παράδειγμα, κρίσιμο ζητούμενο εν μέσω πανδημίας είναι διασφάλιση της ιδιωτικότητας σε θέματα όπως η οπτική παρακολούθηση και η θερμομέτρηση καθώς συγκεντρώνονται και μοιράζονται πολλά δεδομένα και μοιράζονται σε πολλά επίπεδα.

Τις τάσεις και τις προοπτικές του Cyber Insurance ανέλυσαν στο panel 1, ο κ. **Κώστας Βούλγαρης**, *Financial Lines and Casualty Manager, AIG* η κ. **Μαργαρίτα Γκολφινοπούλου**, *Head, Mid-Market & Corporate Clients, UW Manager, Casualty & Fin. Lines, HDI Global SE, Hellas* και η κ. **Άννα Χατζηχαλεπλή,** Επικεφαλής Τμήματος Ανάληψης Κινδύνων Ιδιωτών και Μικρομεσαίων Επιχειρήσεων, ΑΧΑ Ασφαλιστική με συντονιστή τον κ. **Νίκο Γεωργόπουλο**, *Cyber Privacy Risks Insurance Advisor, Cromar Insurance Brokers Ltd – Lloyd's Cover Holder.*
Όπως αναφέρθηκε, το ransomware είναι ο πιο συχνός λόγος ζημιών και βασικός παράγοντας διακοπής εργασιών. Τα έξοδα ανάλογα με την σφοδρότητα της ζημιάς είναι λιγότερα ή περισσότερα. Είναι αλήθεια, ωστόσο, πως αν και αρκετοί πελάτες έχουν δεχθεί επιθέσεις και έχουν πληρώσει «λύτρα» αρνούνται να ασφαλιστούν. Οι ζημιές από τις κυβερνοεπιθέσεις μπορεί να είναι μεγάλες και άμεσες. Αυτό αναγκάζει τους ασφαλιστές να ανεβάσουν προς τα πάνω τα rates για να προστατεύσουν την βιωσιμότητα του κλάδου.
Από την πλευρά τους οι ασφαλιστικές εταιρείες καλούνται να προβούν σε ένα πολύ προσεκτικό underwriting ώστε να δοθούν οι κατάλληλες καλύψεις σε κινδύνους. Κομβικό στοιχείο, σε αυτές τις περιπτώσεις είναι να Business Continuity plan και έμφαση δίνεται στο Identity Management.
Σημαντικό, επίσης, είναι το στοιχείο της εκπαίδευσης για όσους εμπλέκονται σε αυτές τις διαδικασίες ακόμα και για τον ασφαλιστικό διαμεσολαβητή. Τεράστιος είναι ο κίνδυνος για τσουχτερά πρόστιμα και νομικές περιπέτειες στις περιπτώσεις διαρροής δεδομένων κλπ από κυβερνοεπιθέσεις.

«Οι επιπτώσεις αυτών των προβλημάτων μειώνονται αν υπάρχει προετοιμασία, ένα πλάνο διαχείρισης. Η κυβερνοασφάλιση βοηθά να μεταφερθεί μέρος του κινδύνου. Παράλληλα μέσα από την ασφαλιστική σύμβαση γίνεται και εύρεση των νομικών συμβούλων», σημειώνει από την πλευρά του ο κ. **Antonis Patrikios**, *Partner, Privacy & Cybersecurity, Dentons.* «Οι έγκαιρες γνωστοποιήσεις και η συνεργασία είναι παράγοντες που μειώνουν τα ποσοστά προστίμων. Σε κάθε περίπτωση η επιβολή προστίμου για cyber επιθέσεις είναι η αρχή της διαδικασίας όχι το τέλος», τόνισε.

Ζητήματα νομοθεσίας και συμμόρφωσης των εταιρειών συζήτησαν ειδικευμένοι νομικοί, στο Panel 2.

Ειδικότερα, η κουλτούρα επιχειρήσεων και φυσικών προσώπων απέχει σημαντικά από το να φτάσει στο επιθυμητό σημείο σε ό,τι αφορά την ενσωμάτωση των νέων αυξημένων απαιτήσεων για την ασφάλεια. Ο δημόσιος και ο ιδιωτικός τομέας και οι κρίσιμες δομές δεν είναι έτοιμες να ενσωματώσουν τι νέες αυξημένες απαιτήσεις ασφαλείας. Είναι σαφές πως απαιτείται αλλαγή νοοτροπίας, ενώ οι διοικήσεις πρέπει να αντιληφθούν ότι μια επίθεση μπορεί να οδηγήσει σε παύση/αναστολή της επιχειρηματικής δραστηριότητας.

Είναι γεγονός πως οι επιθέσεις σε διάφορους κλάδους της οικονομίας αυξάνονται δραματικά. Αναφερόμενοι σε περιστατικό γνωστής εταιρείας τηλεπικοινωνιών, οι ομιλητές του πάνελ σημείωσαν πως ακόμα αξιολογείται ο πραγματικός αντίκτυπος της επίθεσης, ενώ τόνισαν πως και ο πελάτης – καταναλωτής θα πρέπει να αναλάβει την δική του ευθύνη γύρω από αυτά τα ζητήματα.

Στο πάνελ συμμετείχαν ο κ. **Antonis Patrikios**, *Partner, Privacy & Cybersecurity, Dentons*, ο κ. **Ιωάννης Ε. Γιαννακάκης**, Managi*ng Partner – Co Founder, G+ P Law Firm, FIP, CIPM, CIPP/E, CIPP/US, CFE, CDPO, cert. GDPR Practitioner,* ο κ. **Δημήτρης Ζωγραφόπουλος**, *Δικηγόρος (ΔΝ) – Ειδικός επιστήμονας, Υπεύθυνος Προστασίας Δεδομένων (DPO) Υπουργείου Υγείας* και η κ. **Αριάννα Σέκερη**, *CIPP/E, CIPM, CIPT, FIP, DPO, Junior Partner, ALG Manousakis Law Firm*. Το πάνελ συντόνισε ο δικηγόρος κ. **Τάκης Κακούρης.**

«Το cyber crime έχει εμφανίσει αυξητική τάση το τελευταίο εξάμηνο, ωστόσο αυτό δεν συνδέεται αποκλειστικά με τον κορωνοιό, καθώς και το 2018 και το 2019 παρατηρήσαμε εκτίναξη των συμβολαίων και αντίστοιχα των απαιτήσεων με τους κυβερνοεγκληματίες να ζητούν τουλάχιστον 1 εκατ. ευρώ για λύτρα. Παρόλα αυτά η απομακρυσμένη εργασία που επιβλήθηκε λόγω covid-19, η χρήση προσωπικών υπολογιστών με λιγότερο ασφαλή συστήματα έχει αυξήσει τις cyber επιθέσεις και αντίστοιχα τις απαιτήσεις», υποστήριξε από την πλευρά της η κ. **Lindsey Nelson**, Cyber Development Leader, στην εταιρεία CFC Underwriting, με έδρα το Λονδίνο.

Σύμφωνα με τον ίδια «κλειδί» σε όλη την ιστορία αποτελεί το ανθρώπινο λάθος: Πολλοί εργαζόμενοι συχνά ακολουθούν κακόβουλα links με πολύ αρνητικό αντίκτυπο στις επιχειρήσεις. Οι δράστες αποκτούν με τον τρόπο αυτό πρόσβαση σε πολύτιμα αρχεία, οικονομικές ανακοινώσεις, στα emails των εργαζομένων και στα data της εταιρείας.

Σε άλλες περιπτώσεις, πολύ συχνά οι δράστες παριστάνουν τους CFOs μιας εταιρείας, ή τους προμηθευτές και ζητούν άμεσες μεταφορές χρημάτων.

Εκτιμάται πως την τελευταία περίοδο το 75% των απαιτήσεων συνδέονται με κυβερνοεπιθέσεις λόγω ανθρώπινου λάθους. Ένα άλλο πρόσφατο παράδειγμα απάτης είναι η αποστολή emails στα

οποία οι δράστες παριστάνουν τους εκπροσώπους μεγάλων οργανισμών Υγείας που στέλνουν δήθεν συστάσεις για τα μέτρα κατά της πανδημίας.

Ευκαιρία για να πάμε σε πιο ασφαλείς λύσεις αποτελεί η πανδημία, σύμφωνα με όσα τέθηκαν επί τάπητος στο Panel 3, το οποίο ασχολήθηκε με θέματα Cyber Risks Management & Cyber Claims

Συντονιστής του πάνελ ήταν ο κ. **Χρήστος Ξενάκης**, *professor, Department of Digital Systems, University of Piraeus* και ομιλητές η κ. **Δήμητρα Ξηντάρα,** *CISM, CIPM, CIPP/E, FIP, Data Protection Officer, Όμιλος Eurolife FFH* και οι κ.κ. **Δρ Δημήτριος Πατσός,** *Πρόεδρος (ISC)2 Hellenic Chapter & IT GRC Director, SYNTAX IT Group*, **Δρ Ιωάννης Αγραφιώτης,** *Senior Research Fellow in Cyber Security, University of Oxford*, **Leon Hassid,** *Sales Enablement & Training Leader, SecurityScorecard,* **Χρόνης Καπαλίδης,** *Επικεφαλής Τομέα Κυβερνοασφάλειας, EMEA, HudsonANalytix.*

«Βλέπουμε να συντελούνται κανονιστικές αλλαγές όπως για παράδειγμα στην ΤτΕ με την αλλαγή του θεσμικού πλαισίου και την μετάβαση στο cloud. Όλοι πλέον αντιλαμβάνονται την ταχύτητά των εξελίξεων. Ο όρος του cyber insurance έχει ενδιαφέρον γιατί έχει δραστηριοποιήσει τους ειδικούς προς την κατεύθυνση αναζήτησης στοχευμένων λύσεων. Πλέον, στο στόχαστρο των hackers βρίσκεται ο τομέας Υγείας και κυβερνητικοί οργανισμοί», σημείωσε ο κ. Πατσός.

«Κορυφαία απειλή στις μέρες μας αποτελεί το malware. Μια νέα απειλή είναι αυτό που συμβαίνει με τα VPNs, ειδικά στις εταιρείες που λειτουργούν υπό το καθεστώς της τηλεργασίας. Μολονότι η πανδημία επιτάχυνε περισσότερο τον ψηφιακό μετασχηματισμό στην Ελλάδα, διαπιστώνεται ότι ακόμα και σε εξελιγμένες επιχειρήσεις δεν υπήρχε πλήρης κατανόηση πάνω στα λειτουργικά συστήματα. Δεν αρκεί μόνο το risk assessment αλλά θα πρέπει να έρθει η αλλαγή από το managing board», τόνισε ο κ. Αγραφιώτης.

Κρίσιμο στοιχείο σε όλα αυτά είναι να αναδειχθεί το γεγονός πως δεν πρόκειται για ένα απλά security problem αλλά business problem συνολικά, σύμφωνα με τον κ. Hassid. Ο ίδιος τόνισε επίσης πως η ανάπτυξη του οικοσυστήματος Cyber insurance έχει δημιουργήσει την ανάγκη να γίνονται σημαντικές διαβουλεύσεις σε επίπεδο ανώτατων στελεχών γύρω από αυτά τα ζητήματα.

Η κ. Ξηντάρα μίλησε για το ransmware και το spear fishing, που όπως σημείωσε γίνεται στοχευμένα. «Ακόμη και οι εκπαιδευμένοι μπορεί πολύ εύκολα να την πατήσουν, πέφτοντας θύματα των επιθέσεων. Έχουμε να αντιμετωπίσουμε την πρόκληση από την εταιρική στη προσωπική

συσκευή. Οφείλουμε να λειτουργούμε σε συνθήκες zero, καθώς το 'work from home' μετατρέπεται σε 'work from anywhere», τόνισε.

Τέλος, ο κ. Χρόνης Καπαλίδης υπογράμμισε πως η μεγαλύτερη πρόσκληση είναι να εντοπίσουμε ποιες είναι οι υπηρεσίες που προσφέρει η εταιρεία στους πελάτες μας ώστε να εντοπίσουμε τις προτεραιότητες. «Το cyber insurance είναι μέρος της λύσης εντός της διαδικασίας εκτίμησης του ρίσκου. Βλέπουμε ποιες είναι οι απειλές και προχωράμε στα μέτρα για να τις αντιμετωπίσουμε. Ο οργανισμός πρέπει από μόνος του να καταλάβει ποιο είναι το επίπεδο ρίσκου που μπορεί να δεχθεί εσωτερικά και το κομμάτι που 'περισσεύει' καταλήγει στο cyber insurance αλλά μέσω συγκεκριμένης διαδικασίας», σημείωσε.

Ειδικότερα στοιχεία για τον ρόλο του cyber insurance παρέθεσε από την πλευρά του ο κ. **Mark Singer** *Cyber and Tech E&O Claims Manager, Beazley*. Περιέγραψε την ραγδαία άνοδο του ransomware τα τελευταία χρόνια και εξειδίκευσε χρονικά τα στάδια μιας επίθεσης από την ανακάλυψη και την έρευνα μέχρι και την ανταπόκριση που μπορεί να έχει μια οντότητα ως τους τρόπους θωράκισης της άμυνας, ενώ ανέλυσε τις διαδικασίες αποζημίωσης μετά από ένα τέτοιο γεγονός.

Αίτια των επιθέσεων, ανθρώπινος παράγοντας, λύτρα και μέθοδοι απάτης. Αυτά ήταν τα ζητήματα, μεταξύ άλλων, που βρέθηκαν στο επίκεντρο του Panel 4 με θέμα συζήτησης «Ransomware Incident Response».

Συντονιστής της συζήτησης ήταν ο **κ. Δημήτρης Γεωργόπουλος**, *Founder – CEO, Rethink Business Lab – RBL* και ομιλητές: **Ο κ. Νίκος Γεωργόπουλος,** *Cyber Risks Advisor, Cromar Insurance Brokers Ltd – Lloyd's Cover Holder*, ο κ. **Νίκος Καλφιγκόπουλος**, *CEO, Fractis*, ο κ. **Κωνσταντίνος Παπαδάτος**, *Founder & Managing Director, Cyber Noesis* και ο κ. **Νίκος Σκυλακάκης,** *Managing Director, Sk&P.*

Η έλλειψη γνώσης, η ελλιπής εκπαίδευση και η συνειδητοποίηση για το τι πρόκειται οδηγεί πολλούς χρήστες στο να ανοίγουν κακόβουλα emails, ενώ τα προηγούμενα χρόνια κυρίως υπήρχε στοχοποίηση εταιρειών μέσω phishing και spam emails. «Το cyber crime εντάσσεται πλέον στα βασικά ρίσκα μιας επιχείρησης η οποία θα πρέπει να διαμορφώνει ένα risk assessment και να είναι έτοιμη ώστε να ξέρει που να επικοινωνήσει εάν προκύψει πρόβλημα», σημείωσε ο κ. Καλφιγκόπουλος.

«Είναι δύσκολο ακόμα και για έναν έμπειρο χρήστη να ανιχνεύσει μια απάτη τον τελευταίο καιρό. Οι επιθέσεις καλπάζουν και το οργανωμένο έγκλημα είναι εδώ για αυτό πρέπει να μεριμνήσουμε για ισχυρά κίνητρα. Ο ανθρώπινος παράγοντας, παρά τις όποιες επενδύσεις, παραμένει ο αδύναμος κρίκος», τόνισε ο κ. Παπαδάτος.

Δύο είναι οι λόγοι, σύμφωνα με τον κ. Σκυλακάκη, που ο άνθρωπος είναι το πιο αδύναμο σημείο σ' αυτή την εξίσωση: α) Γιατί δεν αισθάνεται υπεύθυνος για το τεχνικό κομμάτι, καθώς άλλος έχει την ευθύνη του ΙΤ, β) Δεν παρατηρεί εύκολα σημάδια εάν δεν είναι υποψιασμένος, καθώς δεν έχει την κατάλληλη εκπαίδευση και κουλτούρα.

Σημαντικά ερωτήματα έθεσε ο κ. Ν. Γεωργόπουλος: «Το Ransomware έχει φέρει πολλές αλλαγές στα τιμολόγια των εταιρειών. Αν κάποιος ζητήσει «λύτρα» μετά την επίθεση, πρέπει να αναλογιστούμε αν είναι αξιόπιστος, θα αναγκαστώ να ξαναπληρώσω; ποιος μου εξασφαλίζει ότι με την καταβολή των λύτρων θα ησυχάσω;»

Όπως σημείωσε, 1 στους 3 ανθρώπους θα πέσει θύμα του phishing και είναι κρίσιμο για ανθρώπους που δεν έχουν εκπαιδευτεί σε όλα αυτά να υπάρξει άμεση ενημέρωση στον τεχνικό ασφαλείας.

*Το **2nd Cyber Insurance & Incident Response Conference** πραγματοποιήθηκε υπό την αιγίδα του **Υπουργείου Ψηφιακής Διακυβέρνησης**, της **Ένωσης Επαγγελματιών Ασφαλιστών Ελλάδος, του Hellenic (ISC)² Chapter, της Ένωσης Ασφαλιστικών Διαμεσολαβητών Ελλάδας, της Πανελλήνιας Ομοσπονδίας Ανεξάρτητων Ασφαλιστικών Διαμεσολαβητών, του Συλλόγου Ασφαλιστικών Πρακτόρων Νομού Αττικής, του ΣΕΜΑ** και άλλων έγκριτων θεσμικών φορέων.*

Δείτε περισσότερες πληροφορίες ΕΔΩ *& στο* **ethosevents.eu**

Περισσότερες πληροφορίες:

κ. *Αλεξάνδρα Παπασπηλιωτοπούλου, PR & Marketing Communications Manager, Ethos Media S.A, τηλ. 210 9984917*, papaspiliotopoulou.a@ethosmedia.eu