7ο Infocom Security 2017
On the IT Roadmap Expect the Unexpected

Συνεχίζοντας για ακόμα μια χρονιά την ανοδική του πορεία, το κορυφαίο 2ήμερο Συνέδριο στην Νοτιοανατολική Ευρώπη για την Ψηφιακή Ασφάλεια, InfoCom Security, πραγματοποιήθηκε για 7η φορά στις 29 & 30 Μαρτίου 2017 με τίτλο "On the IT Roadmap - Expect the Unexpected".

Η πολύ μεγάλη επιτυχία και της 7ης διοργάνωσης του Συνεδρίου **Infocom Security** και η συνέχιση της ανοδικής του πορείας, αποτυπώνεται τόσο στα ποσοτικά στοιχεία, όσο και στις πολύ θετικές εντυπώσεις που αποκόμισαν όσοι είχαν την ευκαιρία να επισκεφτούν το διήμερο **29 και 30 Μαρτίου** το ξενοδοχείο Divani Caravel, όπου πραγματοποιήθηκε για ακόμα μια φορά το κορυφαίο συνέδριο για την ψηφιακή ασφάλεια, αλλά και ένα από τα **πλέον επιτυχημένα συνέδρια ευρύτερα στο χώρο της πληροφορικής** στην Ελλάδα.

Συνολικά, το συνέδριο προσέλκυσε πάνω από **2300 επαγγελματίες** του τομέα της πληροφορικής (CTOs, CIOs, IT Managers, IT Administrators, IT Security Managers, IT Auditors κλπ.) από μεγάλες εταιρείες και οργανισμούς του Ιδιωτικού και Δημόσιου τομέα, αλλά και στελέχη επιχειρήσεων από το κανάλι της Πληροφορικής. Επίσης, παρευρέθηκαν φοιτητές, ακαδημαϊκοί, επιστήμονες και ερευνητές με ευρύτερο ενδιαφέρον στον τομέα της πληροφορικής και ειδικότερα την ασφάλεια δεδομένων.

Οι επισκέπτες είχαν την ευκαιρία να παρακολουθήσουν συνολικά στις **2 ημέρες** του συνεδρίου, **6 μεγάλες θεματικές ενότητες, 46 ομιλίες και 21 παράλληλα workshops,** καθώς και να συναντηθούν με στελέχη από τις συνολικά **50 εταιρείες – χορηγούς** του συνεδρίου που εκπροσωπούσαν κορυφαία brands από το τομέα της ψηφιακής ασφάλειας στην Ελλάδα και το εξωτερικό.

Σημείο Αναφοράς για τις εξελίξεις στο χώρο του IT Security

Σε σχέση με το περιεχόμενο του συνέδριου, επιβεβαιώθηκε με τον πλέον εμφατικό τρόπο, ότι το **InfoCom Security** αποτελεί το σημείο αναφοράς των εξελίξεων στον τομέα της ασφάλειας πληροφοριών και της αντιμετώπισης των ψηφιακών απειλών. Οι ομιλητές του συνεδρίου ανέδειξαν μέσα από τις παρουσιάσεις που πραγματοποίησαν, τις πλέον σύγχρονες τάσεις και προκλήσεις στο χώρο της ψηφιακής ασφάλειας. Επιχειρώντας να ξεχωρίσουμε τα κυριότερα θεματικά αντικείμενα, στα οποία εστίασαν πολλές παρουσιάσεις, σίγουρα θα πρέπει να αναφερθούμε πρώτα από όλα στο νέο Ευρωπαϊκό Γενικό Κανονισμό για την Προστασία των Δεδομένων, μιας και το ακρωνύμιο του GDPR ακούστηκε πάρα πολλές φορές στην αίθουσα της ολομέλειας αλλά και στα παράλληλα Workshops. Η προσέγγιση φυσικά του **GDPR** διέφερε από ομιλητή σε ομιλητή ανάλογα με την εταιρία ή το φορέα που εκπροσωπούσε ο καθένας. Έτσι, είχαμε την ευκαιρία να ενημερωθούμε για τις **βέλτιστες πρακτικές συμμόρφωσης στα νέα δεδομένα που θα επιφέρει ο GPDR** είτε αυτές αφορούν θέματα **πολιτικής** και **εσωτερικών διαδικασιών,** είτε **υπηρεσιών και προϊόντων** που θα βοηθήσουν τους οργανισμούς να προσαρμοστούν είτε ακόμα τον κρίσιμο ρόλο που θα αναλάβει ο Data Protection Officer.

Σε πολλές από τις ομιλίες του συνεδρίου επίσης, κεντρικό θέμα αποτέλεσαν οι **σύγχρονες επιθέσεις** με έμφαση στα κακόβουλα λογισμικά **Ransomware** αλλά και άλλου τύπου προηγμένες απειλές. Όπως διαπιστώσαμε οι κίνδυνοι είναι πολλοί και αναπάντεχοι με αποτέλεσμα να καθίσταται επιτακτική ανάγκη, σε οποιοδήποτε σχεδιασμό ανάπτυξης IT αλλά και υιοθέτησης των νέων τάσεων όπως το cloud, το mobility και το IoT, να λαμβάνεται υπόψη η κρίσιμη παράμετρος της προστασίας των δεδομένων.

Σημαντικό χαρακτηριστικό του συνεδρίου, ήταν φυσικά επιπρόσθετα από την **business προσέγγιση** για το IT Security, το ευρύτερο **επιστημονικό και τεχνολογικό περιεχόμενο** για το Cyber Security. Κομβικό ρόλο σε αυτή τη προσέγγιση είχε φυσικά ο 2ος διαγωνισμός **EthiHak Contest** που πραγματοποιήθηκε σε συνεργασία με την ομάδα του **Secnews.gr** και έδωσε την ευκαιρία σε επαγγελματίες και μη, σε hackers, ερευνητές ασφάλειας αλλά και απλούς φανς, να αγωνιστούν εναντίον πολλών live στόχων, δοκιμάζοντας τις ικανότητες τους.

*Ο Αντιπρόεδρος της Α.Δ.Α.Ε, **Μιχάλης Σακκάς**.*

*Ο Διευθυντής Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, **Γεώργιος Παπαπροδρόμου**.*

Στην έναρξη του συνεδρίου χαιρετισμό απεύθυναν ο **Κώστας Νόστης**, ως Πρόεδρος της Οργανωτικής Επιτροπής του συνεδρίου αλλά και ο **Μιχάλης Σακκάς**, Αντιπρόεδρος της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε) ο οποίος επισήμανε ότι το αυτόνομο και θεμελιώδες δικαίωμα στο απόρρητο των επικοινωνιών αποτελεί, ένα από τα σημαντικότερα έννομα αγαθά διεθνώς και συνεπώς απαιτείται να εντείνουμε, τις προσπάθειές για την προστασία του δικαιώματος αυτού. Επίσης, στην έναρξη του συνεδρίου είχαμε την ευκαιρία να παρακολουθήσουμε τον **Γεώργιο Παπαπροδρόμου** - Διευθυντή της **Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος**, όπου αναφέρθηκε στην αποστολή και στη Δομή της Υπηρεσίας, τις συνεργασίες που αναπτύσσει σε τοπικό, ευρωπαϊκό και διεθνές επίπεδο, εστιάζοντας παράλληλα στις δράσεις ενημέρωσης του κοινού, αλλά και στις καινοτόμες εφαρμογές που έχει δημιουργήσει η Υπηρεσία της Διεύρυνσης Δίωξης Ηλεκτρονικού Εγκλήματος, όπως το Cyberkid και το FeelSafe, τονίζοντας χαρακτηριστικά ότι: «Όπου θα αποτύχει το Cyber Security θα ασχοληθούμε έμεις, ως Cyber Crime».

Στις επόμενες σελίδες μπορείτε να διαβάσετε τα βασικά σημεία των παρουσιάσεων των ομιλητών καθώς και να δείτε πλούσιο φωτογραφικό υλικό από τις 2 ημέρες του συνεδρίου.

1η ημέρα - 29 Μαρτίου

Αχιλλέας Κουτσούκος

Πρώτος ομιλητής της 1η θεματικής ενότητας του Συνεδρίου ήταν ο **Αχιλλέας Κουτσούκος** - Product Manager της **ENCODE** - που επισήμανε ότι ένα Security Operation Center (SOC) στις μέρες μας καλείται να αντιμετωπίσει σημαντικές προκλήσεις όπως ο μεγάλος όγκος alerts από εγκατεστημένες λύσεις ασφάλειας, η έλλειψη εργαλείων και συγκεντρωτικής πληροφόρησης, κ.ά. Η ENCODE λαμβάνοντας υπόψη αυτές τις προκλήσεις, ανέπτυξε το προϊόν **SOCStreams** μέρος της σουίτας Enorasys. Πρόκειται για ένα Incident Response Orchestration προϊόν το οποίο σε συνδυασμό με τη **SIEM λύση IBM QRadar,** εξυπηρετεί στη μείωση του χρόνου απόκρισης αλλά και στη συνολική βελτίωση της αποτελεσματικότητας των φάσεων της Διαχείρισης ενός Περιστατικού Ασφάλειας.

Δρ Κωνσταντίνος Παπαπαναγιώτου

Η ομιλία του **Δρ Κωνσταντίνου Παπαπαναγιώτου** - Information Security Sales Manager του Ομίλου **OTE**, εστίασε στις σημαντικές προκλήσεις για το cloud, όπως η απρόσκοπτη διαθεσιμότητα σύνδεσης στο internet και η προστασία των προσωπικών δεδομένων, κυρίως από κυβερνοεπιθέσεις. Χαρακτηριστικά, ανέφερε ότι πλέον οι επιθέσεις DDoS είναι συνηθισμένο φαινόμενο, ενώ κάθε επίθεση κατά μέσο όρο μπορεί να υπερβαίνει ακόμα και τα 4Gbps. Πέρα από απρόσκοπτη συνδεσιμότητα, η COSMOTE διαθέτει μια εξειδικευμένη πλατφόρμα αντιμετώπισης επιθέσεων DDoS. Οι επιθέσεις αυτές αντιμετωπίζονται πριν καν φτάσουν στους πελάτες, ενώ παρέχουν συγκεκριμένα SLAs, με τα οποία εξασφαλίζεται η διαθεσιμότητα του Internet ακόμα και σε περίπτωση επίθεσης DDoS.

Δήμητρα Ζέρβα

Διανύουμε μια εποχή όπου οι παραβιάσεις δεδομένων είναι αναπόφευκτες επισήμανε η **Δήμητρα Ζέρβα** - Information Security Consultant, Networking Division της **Space Hellas** αναφέροντας ότι είναι εξαιρετικά δύσκολο για τους οργανισμούς να μειώσουν το ενδεχόμενο των παραβιάσεων χωρίς την ύπαρξη ενός συνεκτικού και αξιόπιστου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, το οποίο θα καλύπτει κάθε πλευρά της επιχειρηματικής τους ζωής. Οι τεχνικές λύσεις από μόνες τους δεν επαρκούν από τη στιγμή που οι εσωτερικές απειλές αποτελούν θέμα καθαρά των ανθρώπων. Η Space Hellas προσφέροντας επιστημονική γνώση και αποδεδειγμένη εμπειρία σε θέματα Ασφάλειας Πληροφοριών και διεθνή πρότυπα, είναι σε θέση να εντοπίσει, να αξιολογήσει και να προτείνει τις βέλτιστες πρακτικές που έχουν υιοθετηθεί τόσο από την ίδια όσο και από τους πελάτες της.

Δρ. Δημήτρης Πατσός

Ένα ιδιαίτερα χρήσιμο θέμα με τίτλο «Εξηγώντας τα οικονομικά, το χρέος και το ρίσκο της κυβερνοασφάλειας στο Διοικητικό Συμβούλιο» ανέπτυξε ο **Δρ. Δημήτρης Πατσός** - Chief Technology Officer της **ADACOM** - επισημαίνοντας ότι συνήθως το εκάστοτε Δ.Σ μιας επιχείρησης βλέπει λανθασμένα την ασφάλεια ως ένα σύνθετο αντικείμενο που απαιτεί σημαντικές επενδύσεις που μπορεί να μην αποδώσουν. Αυτό που οι άνθρωποι της ασφάλειας οφείλουν να πετύχουν είναι να αλλάξουν το παραγωγικό μοντέλο σε κάτι πιο σύγχρονο και εξελισσόμενο με βάση 4 συνιστώσες, όπως: την ασφαλή υποδομή, την κουλτούρα ασφάλειας, την επαγρύπνηση στους κινδύνους και ένα πλάνο αντιμετώπισης περιστατικών.

Χρήστος Βιδάκης

Ο **Χρήστος Βιδάκης** - Principal, Risk Advisory, **Deloitte** - ανέφερε ότι ο κυβερνοχώρος αποτελούσε, αποτελεί και θα αποτελεί κίνδυνο για την ασφάλεια των οργανισμών. Αυτό όμως που θα διαφοροποιείται στο προσεχές μέλλον είναι ο βαθμός της ψηφιακής έκθεσης των οργανισμών (στον κυβερνοχώρο), αυξάνοντας το πεδίο δράσης των επιτιθέμενων, σε συνδυασμό με τις αυξημένες κανονιστικές απαιτήσεις αλλά και την έλλειψη δεξιοτήτων, ανθρώπινου δυναμικού και προϋπολογισμού. Ο κ. Βιδάκης παρουσίασε το δίκτυο κυβερνοευφυΐας της Deloitte το οποίο αποτελείται από 29 κέντρα, στρατηγικά τοποθετημένα σε 18 χώρες, για την παροχή ολιστικών, εξειδικευμένων και παραμετροποιήσιμων υπηρεσιών κυβερνοασφάλειας.

Γιάννης Γκιόκας

Κατά την ομιλία του ο **Γιάννης Γκιόκας** - VP Research & Development at PCCW Global and Founder of **Crypteia Networks** - υποστήριξε ότι η μεγαλύτερη πρόκληση για τους οργανισμούς σήμερα είναι η διαχείριση του πολύ μεγάλου όγκου των περιστατικών ασφάλειας με δεδομένη την εκθετική ανάπτυξη των τεχνολογιών και των χρηστών. Έτσι έχει δημιουργηθεί η ανάγκη για μια στροφή προς την τεχνητή νοημοσύνη όπου θα αντικαταστήσει την ανθρώπινη ανάλυση. Προς σε αυτή τη κατεύθυνση έρευνας και ανάπτυξης κινείται και η ομάδα της εταιρίας του με στόχο να προσφέρουν ολοκληρωμένη προστασία έναντι στο ολοένα και πιο εξελισσόμενο τοπίο της εγκληματικότητας στον κυβερνοχώρο.

Δημήτρης Στασινόπουλος

Στην ομιλία του, ο manager της διεύθυνσης IT Governance της **PRIORITY**, **Δημήτρης Στασινόπουλος,** ανέλυσε γιατί ο GDPR διαφέρει σημαντικά από τις άλλες κανονιστικές υποχρεώσεις των επιχειρήσεων και παρουσίασε τα συστατικά για την ολοκληρωμένη προσέγγιση στο νέο θεσμικό πλαίσιο μέσα από το Gap Analysis, την ανάπτυξη του Compliance Plan και το σχεδιασμό ενός Personal Information Management System. Η PRIORITY υλοποιεί ήδη τρία έργα σε επιχειρήσεις με υψηλή επικινδυνότητα προσωπικών δεδομένων για τη διάγνωση της συμμόρφωσής τους με τον GDPR, τη δημιουργία του αρχείου δραστηριοτήτων επεξεργασίας, τη μελέτη εκτίμησης επιπτώσεων (Privacy Impact Assessment) και τον καθορισμό του Compliance Plan με τις απαιτούμενες ενέργειες συμμόρφωσης με τον GDPR και περιορισμού των κινδύνων.

Moti Sagey

Η διαφορά που κάνει τη σημασία σε σχέση με τις τεχνολογίες προστασίας, αποτέλεσε την κεντρική ιδέα της παρουσίασης του **Moti Sagey** - Head of Strategic Marketing, **Check Point Software**. Ο ομιλητής παρουσίασε ένα μοντέλο ασφάλειας που κερδίζει την εμπιστοσύνη των πελατών και είναι βασισμένο σε τρεις βασικούς πυλώνες και συγκεκριμένα: 1.Uncompromised Security - 2.Everywhere Architecture - 3.Operational Efficiency. Το μοντέλο αυτό αναδεικνύει την πρόληψη ως βασική φιλοσοφία προστασίας σε συνδυασμό με την ενίσχυση της παραγωγικότητας.

Άγγελος Πρίντεζης

Ο Άγγελος Πρίντεζης - Manager, IthacaLabs™ της Odyssey ανέφερε στην ομιλία του ότι η εκμετάλλευση των ευπαθειών σε επίπεδο Λειτουργικού Συστήματος και εφαρμογών, τα Ransomware καθώς και τα Advanced Persistent Threats είναι παραδείγματα απειλών που λειτουργούν σχεδόν αόρατα στις επιχειρήσεις. Οι παραδοσιακοί μηχανισμοί προστασίας και διαχείρισης απειλών δεν αρκούνε πλέον για να αντιμετωπιστούν τις σύγχρονες απειλές. Η λύση Sandblast Zero-day protection της Checkpoint, το Enterprise Endpoint Protection της SentinelOne και το ClearSkies NG SIEM Threat Management Process της Odyssey Cyber Security κλείνουν τα κενά προστασίας των παραδοσιακών λύσεων.

Νίκος Μουρτζίνος

Η πρόσφατη Ετήσια Έκθεση Ασφάλειας (Annual Cybersecurity Report) της Cisco για το 2017, παρουσιάζει ένα δύσκολο τοπίο για τη διαδικτυακή ασφάλεια ανέφερε ο **Νίκος Μουρτζίνος** - Security Product Sales Specialist, Cisco. Οι επικεφαλής των οργανισμών και εταιρειών πρέπει να αναγνωρίσουν τη σημασία της ασφάλειας και να ηγηθούν οι ίδιοι του στρατηγικού σχεδιασμού. Η προσθήκη «ενός ακόμα προμηθευτή» δεν μπορεί να συνεχίσει να αποτελεί την απάντηση, στις προκλήσεις των θεμάτων ασφάλειας. Οι vendors που ενσωματώνουν προϊόντα και υπηρεσίες πληροφορικής στις προσφορές τους, πρέπει να προσφέρουν λύσεις που οι πελάτες να μπορούν να εμπιστευτούν και οι οποίες να έχουν σχεδιαστεί με γνώμονα την ασφάλεια, την ενσωμάτωση στην υπάρχουσα υποδομή, προσφέροντας αυτοματοποίηση στο εντοπισμό στον νέων απειλών.

Jose Grandmougin

Στο Security Fabric της Fortinet, επικεντρώθηκε η ομιλία του **Jose Grandmougin** – Director System Engineering, Telco and Global Alliances της **Fortinet.** Ο ομιλητής επισήμανε ότι η συγκεκριμένη λύση της Fortinet επιτρέπει στην ασφάλεια ενός οργανισμού να επεκτείνεται και να προσαρμόζεται δυναμικά, καθώς όλο περισσότερες συσκευές και εφαρμογές προστίθενται σε αυτόν. Ταυτόχρονα έχει τη δυνατότητα να ακολουθεί και να προστατεύει τα δεδομένα, τους χρήστες και τις εφαρμογές τους, καθώς αυτά μετακινούνται ανάμεσα σε συσκευές IoT, έξυπνες συσκευές και το cloud σε όλο το δίκτυο.

Bogdan Tobol

Ο ομιλητής της CyberArk **Bogdan Tobol** - Regional Sales Executive - South-East Europe, CyberArk - που βρέθηκε στο συνέδριο ως καλεσμένος της NSS έδωσε έμφαση στα ζητήματα ασφάλειας που μπορούν να προκύψουν στις επιχειρήσεις με τη διαχείριση των δικαιωμάτων των χρηστών. Όλες οι επιχειρήσεις οφείλουν να βρουν το σωστό τρόπο διαχείρισης των δικαιωμάτων χρηστών, έτσι ώστε χωρίς να μειωθεί η παραγωγικότητα να αυξηθεί το επίπεδο ασφάλειας στην επιχείρηση. Είναι γνωστό άλλωστε ότι ιδιαιτέρως τα δικαιώματα προνομιακών χρηστών (privileged users / administrators) αποτελούν σημαντική βάση για κακόβουλες ενέργειες. Η πρόσεγγιση της Cyberark δίνει πολύτιμα εργαλεία στις επιχειρήσεις για το σκοπό αυτό και προσθέτει ένα ακόμη επίπεδο ασφάλειας ιδιαίτερα σημαντικό.

Angelo Gentili

Στο πλαίσιο του συνεδρίου ο **Angelo Gentili**, **Head,** Business Development, EMEA της **PartnerNET** παρουσίασε την ολοκληρωμένη σειρά ψηφιακής ασφάλειας και Data Leakage Prevention της Seqrite. Συγκεκριμένα, η ομιλία περιλάμβανε τα Seqrite Mobile Device Management System - παροχή ασφάλειας και κεντρικού ελέγχου του «φορητού εργασιακού χώρου», δίνοντας τη δυνατότητα στις επιχειρήσεις να αξιοποιούν στο έπακρο την φορητότητα των εργαζομένων τους, Seqrite Endpoint Security - ολοκληρωμένη προστασία και έλεγχος των επιτραπέζιων και φορητών υπολογιστών μέσω διαχείρισης κεντρικής κονσόλας, Seqrite Server Security -σχεδιασμένη για τις ανάγκες των servers μεγάλων επιχειρήσεων.

Γιάννης Βόρδος

Η ραγδαία αύξηση των απειλών στο διαδίκτυο και η συνεχώς μεγαλύτερη πολυπλοκότητα τους έχει καταστήσει επιτακτική την ανάγκη λήψης προληπτικών μέτρων στον τομέα της ασφάλειας στο διαδίκτυο υποστήριξε ο **Γιάννης Βόρδος** - Security Solutions Product Manager, **Intracom Telecom**. Cyber Threat Intelligence (CTI) είναι η γνώση των δυνατοτήτων, της υποδομής, των κινήτρων, των στόχων, και των πηγών που σχετίζονται με τις απειλές. Τα συσσωρευμένα αυτά δεδομένα, δίνουν τη δυνατότητα στις επιχειρήσεις να λαμβάνουν, εκ των προτέρων, μέτρα αντιμετώπισης των απειλών. Η Intracom-Telecom έχοντας ήδη αναγνωρίσει τη χρησιμότητα της εν λόγω τεχνολογίας, έχει διερευνήσει και αξιολογήσει σημαντικό αριθμό από τις προσφερόμενες λύσεις.

Erol Dogan

Ο **Erol Dogan** - Regional Sales Engineer BG, GR,TR, **Gemalto** ως καλεσμένος της Adacom παρουσίασε στους συνέδρους την πρόταση της εταιρίας σχετικά με τις τεχνολογίες Identity & Data Protection, εστιάζοντας στις δυνατότητες προστασίας των δεδομένων κατά τη διάρκεια όλου του κύκλου ζωής των δεδομένων αλλά και στα οφέλη που προκύπτουν από την ενσωμάτωση της λύσης με ένα πολύ μεγάλο αριθμό εφαρμογών και τεχνολογιών άλλων κατασκευαστών.

Γρηγόρης Τσόλιας

Μια εκτενή αναφορά στον GDPR έκανε ο **Γρηγόρης Τσόλιας** - Δικηγόρος, Μέλος (αν.) της Α.Π.Δ.Π.Χ και της Νομοπαρασκευαστικής Επιτροπής, Μέλος του Expert Group της Ευρωπαϊκής Επιτροπής για τον GDPR. Κατά την παρουσίαση του εξήγησε σε τι αποσκοπεί ο κανονισμός όπως η ανάγκη συνεκτικής και ομοιόμορφης εφαρμογής των κανόνων προστασίας των προσωπικών δεδομένων στην Ε.Ε. Επίσης αναφέρθηκε στον κρίσιμο ρόλο του υπευθύνου προστασίας δεδομένων (DPO) που θα μεριμνά για τη λήψη όλων των αναγκαίων τεχνικών και οργανωτικών μέτρων για την τήρηση των αρχών και των υποχρεώσεων που περιγράφονται.

Βασίλης Βλάχος

Ο Επίκουρος Καθηγητής του **ΤΕΙ Θεσσαλίας Βασίλης Βλάχος** αναφέρθηκε στο πρόβλημα της ιδιωτικότητας και ειδικότερα στις εξελιγμένες τεχνικές ταυτοποίησης που χρησιμοποιούν μεγάλες εταιρίες, καταπιεστικά κράτη αλλά και επιτήδειοι προκειμένου να καταγράψουν με λεπτομέρεια την δραστηριότητα των χρηστών στο Διαδίκτυο. Στα πλαίσια του Ευρωπαϊκού Ερευνητικού έργου PrivacyFlag, το Ινστιτούτο Τεχνολογίας Υπολογιστών & Εκδόσεων «Διόφαντος», συμβάλλει στην ανάπτυξη τεχνολογιών που αξιοποιούν τον πληθοπορισμό (crowdsourcing), δηλαδή την συλλογική ευφυΐα των χρηστών, ώστε να αντιμετωπιστούν ανάλογες απειλές.

Κωνσταντίνος Μαρκαντωνάκης

Μια πολύ ενδιαφέρουσα ομιλία είχαμε την ευκαιρία να παρακολουθήσουμε από τον **Κωνσταντίνο Μαρκαντωνάκη** - Professor of Information Security, **Royal Holloway University of London** - που ανέδειξε τις προκλήσεις σε σχέση με την ιδιωτικότητα στα Wireless Avionics Networks (SHAWN) και Future Integrated Transportation (DICE) εστιάζοντας στις σημαντικές αλλαγές που έχει επιφέρει η χρήστη των smartphones και της τεχνολογίας NFC στην διαχείριση των εισιτήριων των μεταφορών.

Ανδρέας Μαυρογένης

E.S.I είσαι ο καλύτερος φίλος του Hacker. E.S.I και ο κάθε ένας από εμάς ανέφερε χαρακτηριστικά ο Ανδρέας Μαυρογένης - IS Architect, Editor Secnews. Επισημαίνοντας ότι όλοι μας κινδυνεύουμε από τους Social Engineers διότι είναι σχετικά εύκολο να μας αποσπάσουν σημαντικές πληροφορίες. (Essential Security Information). Οι τεχνικές που χρησιμοποιούν οι Hackers και οι Social Engineers μπορεί να φαντάζουν «μαγικές» αλλά είναι κατά 80% περισσότερο πετυχημένες από όσο ένα phishing email attack. Δυστυχώς, πολλά μεγαλοστελέχη εταιρειών, κατάλαβαν αργά την ανησυχία των IT Managers για ασφάλεια και εκπαίδευση των χρηστών και τώρα καλούνται να βάλουν βαθιά το χέρι στην τσέπη.

Αναστάσιος Παπαθανασίου & Γεώργιος Γέρμανος

Για το ηλεκτρονικό επιχειρείν που βρίσκεται στο στόχαστρο των κυβερνοεγκληματιών και τα επίκαιρα τεχνάσματα & επιβεβλημένα αντίμετρα στο ψηφιακό εταιρικό περιβάλλον μας μίλησαν ο **Αναστάσιος Παπαθανασίου και ο Γεώργιος Γέρμανος** - Αξιωματικοί της ΕΛ.ΑΣ της **Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος**. Οι δυο αξιωματικοί αναφέρθηκαν στα πολλά περιστατικά επιθέσεων Ransomware & Cryptoware, τις απάτες CEO, τις επιθέσεις Man-in-the-middle, τις εκβιάσεις με επίθεση DDoS και τις επιθέσεις Phishing. Σε σχέση με τα αντίμετρα οι δυο ομιλητές επισήμαναν την ανάγκη εφαρμογής μεθόδων κρυπτογράφησης αλλά τον κρίσιμο ρόλο της ενημέρωσης και εκπαίδευσης του προσωπικού των εταιριών μιας και όπως είπανε χαρακτηριστικά όσα μέτρα ασφαλείας κι αν ληφθούν, σε οποιοδήποτε επίπεδο, αδύναμος κρίκος παραμένει ο άνθρωπος!

2η ημέρα - 30 Μαρτίου

Ιωάννης Ψαλλίδας

Κάθε επιχείρηση θα πρέπει να αναπτύξει μια στρατηγική προσέγγιση για να διασφαλίζει τις πληροφορίες και τις πληροφοριακές υποδομές της υποστήριξε ο **Ιωάννης Ψαλλίδας** - Προϊστάμενος Διεύθυνσης Διασφάλισης Υποδομών και Απορρήτου Υπηρεσιών και Εφαρμογών Διαδικτύου, **ΑΔΑΕ.** Ειδικότερα, οι πάροχοι ηλεκτρονικών επικοινωνιών είναι υποχρεωμένοι να εφαρμόζουν τον Κανονισμό της ΑΔΑΕ για την Ασφάλεια και Ακεραιότητα των Δικτύων και Υπηρεσιών (ΦΕΚ 1742/Β/15-7-2013). Σύμφωνα με τον Κανονισμό, οι πάροχοι θα πρέπει να λαμβάνουν συγκεκριμένα οργανωτικά, τεχνικά και διαδικαστικά μέτρα, με στόχο την πρόληψη και την αποτελεσματική αντιμετώπιση περιστατικών ασφάλειας που επηρεάζουν τη συνέχεια της λειτουργίας των δικτύων και υπηρεσιών τους. Η ΑΔΑΕ ελέγχει την εφαρμογή των προβλεπόμενων μέτρων διενεργώντας προγραμματισμένους ελέγχους, καθώς και έκτακτους ελέγχους για τη διερεύνηση περιστατικών ασφάλειας.

Θωμάς Αιλιανός

Το κόστος για την ανάκαμψη από σύγχρονες Κυβερνο-επιθέσεις γίνεται ολοένα και μεγαλύτερο λόγω της καθυστερημένης αναγνώρισης και της ανταπόκρισης στα περιστατικά ασφαλείας τόνισε ο **Θωμάς Αιλιανός** - SOC Senior Security Engineer, **ENCODE.** Για να μειώσει το χρόνο αυτό, η Encode έχει δημιουργήσει μια νέα υπηρεσία με το όνομα Malware Detection and Response. Κύριο χαρακτηριστικό είναι η αυξημένο visibility στα συστήματα των Εταιριών, ενώ η ειδοποιός διαφορά του νέου αυτού service είναι η δυνατότητα που έχει το Encode Security Operation Center (SOC) να διενεργεί έρευνα σε βάθος των endpoints και να αντιμετωπίζει άμεσα περιστατικά χρησιμοποιώντας τα προϊόντα της Enorasys Πλατφόρμας.

Δημήτρης Μουζακίτης

Για έναν οργανισμό, οποιουδήποτε μεγέθους, η ασφάλεια των πληροφοριών απαιτεί μια ολοκληρωμένη προ-

σέγγιση και θα πρέπει να εντάσσεται στις βασικές επιχειρηματικές του διαδικασίες και την εταιρική του κουλτούρα υποστήριξε ο **Δημήτρης Μουζακίτης** - Manager, Governance, Compliance and Risk Management, της **Odyssey.** Ο Υπεύθυνος Ασφάλειας θα πρέπει να προβεί στις απαραίτητες ενέργειες ώστε να εμπλουτίσει τους βασικούς πυλώνες ασφάλειας (Πολιτικές, Διαδικασίες, συμπεριφορά Ανθρώπινου Δυναμικού και Τεχνολογία) σε όλο το φάσμα των επιχειρηματικών λειτουργιών. Η πρόκληση αυτή απαιτεί τη θέσπιση ενός στρατηγικού Προγράμματος Ασφάλειας Πληροφοριών το οποίο θα αποτελεί τη δομημένη, τεκμηριωμένη και καταγεγραμμένη προσέγγιση του οργανισμού ως προς το σχεδιασμό και την εφαρμογή πρακτικών ασφάλειας.

Χριστίνα Μπούρα

Η **Χριστίνα Μπούρα** - Τομεάρχης Ασφάλειας Πληροφοριακών Συστημάτων της **Δ.Ε.Η** - μίλησε για την επικίνδυνη τάση της κουλτούρας του «όχι» και του Shadow IT που δημιουργεί σημαντικά προβλήματα σε πολλούς οργανισμούς και πηγάζει από την άρνηση πολλών ανθρώπων μέσα στην εταιρία να εναρμονιστούν με τις εσωτερικές πολιτικές και κανονισμούς για την διασφάλιση των δεδομένων. Επίσης τόνισε τον κρίσιμο ρόλο του υπεύθυνου ασφάλειας IT σε ένα οργανισμό που είναι να ακολουθεί τη γενική στρατηγική, να συμβουλεύει την εταιρεία να αναπροσαρμόζει τη στρατηγική, να είναι διερευνητικός και να είναι φύλακας, δηλαδή proactive.

Νικήτας Κλαδάκης

Έναν καινούριο όρο εισήγαγε στη παρουσίαση του ο **Νικήτας Κλαδάκης** -Information Security Director της **Netbull**. Πρόκειται για τις ανεικονικές απειλές, τις οποίες ο ομιλητής προσδιόρισε ως τις απειλές που δεν είναι ορατές και δεν έχουμε για αυτές σχηματισμένη εικόνα, ενώ χρησιμοποιούν εξειδικευμένες τεχνικές επίθεσης. Επίσης, παρακίνησε τις εταιρίες να υιοθετήσουν τον κύκλο ζωής της ασφάλειας πληροφοριακών συστημάτων, βασισμένο στο σωστό σχεδιασμό, στην επιλογή λύσεων ολιστικής προστασίας, στη καθημερινή λειτουργικότητα της ασφάλειας και την αποτίμηση της οποιαδήποτε ομπρέλας προστασίας. Περιέγραψε επίσης τα οφέλη του Netbull Threat Management Platform, που περιλαμβάνει μια σειρά από τεχνολογίες που εντοπίζουν τις ανεικονικές απειλές.

Πάνος Μωραΐτης

Σε μια εκτενή ανάλυση των προκλήσεων και των ευκαιριών που δημιουργεί ο κανονισμός GDPR προχώρησε ο **Πάνος Μωραΐτης** - CEO της **Aspida Cyber Security** - εστιάζοντας μεταξύ άλλων στον κρίσιμο ρόλο του DPO. Ο ομιλητής τόνισε την ανάγκη έγκαιρου προγραμματισμού συμμόρφωσης με τον κανονισμό κάτι που μπορεί να επιφέρει ανταγωνιστικά πλεονεκτήματα, επισημαίνοντας χαρακτηριστικά «...Αδράξτε την ευκαιρία». Επίσης, επισήμανε την ανάγκη καλλιέργειας μια κουλτούρας ασφάλειας.

Νίκος Γεωργόπουλος

Τη συσχέτιση μεταξύ του κανονισμού GDPR και της ασφάλισης Cyber Insurance προσέγγισε η ομιλία του **Νίκου Γεωργόπουλου** - Cyber Privacy Risks Advisor, **Cromar coverholder at Lloyd's** - που υποστήριξε ότι η ασφάλιση Cyber Insurance αποτελεί ένα κρίσιμο κομμάτι της συνολικής στρατηγικής για τη διαχείριση των κινδύνων κάθε εταιρείας. Ενώ η ασφάλιση δεν μπορεί να εμποδίσει ένα περιστατικό ασφαλείας, μπορεί να βοηθήσει το πρόγραμμα ασφάλειας των πληροφοριών της εταιρείας με την παροχή βοήθειας μέσω εξειδικευμένων παρόχων που παρέχουν τις κατάλληλες υποδομές και το κατάλληλο ανθρώπινο δυναμικό, όταν εμφανίζεται συμβάν ασφάλειας μειώνοντας τις επιπτώσεις της παραβίασης στους πελάτες, τη φήμη της εταιρείας και το εμπορικό σήμα της.

Νίκος Καλλέργης

Στην ασφάλεια των δεδομένων από μια τεχνική προσέγγιση στο τομέα της Ναυτιλίας επικεντρώθηκε η παρουσίαση του **Νίκου Καλλέργη** - Network Engineer της **Inttrust** - ο οποίος παρουσίασε τη προσέγγιση και τις λύσεις ασφάλειας της Checkpoint για αυτό τομέα. Η υιοθέτηση αυτών των λύσεων επιταχύνει ισχυρή αποτελεσματικότητα, ενισχύει την παραγωγικότητα και τη διαχείριση και μειώνει σημαντικά το κόστος λειτουργίας.

Chester Wisniewski

Είναι γεγονός, ότι το IoT εισέρχεται ολοένα και περισσότερο στη ζωή μας. Εκτός όμως από τα προφανή οφέλη του IoT, δημιουργείται ένα νέο υπόστρωμα για απειλές από τις οποίες πρέπει να προστατευτούμε. Ο διακεκριμένος Blogger και Senior Security Advisor της Sophos, **Chester Wisniewski**, αφού ανέλυσε τις νέες αυτές απειλές, μας έδειξε και τον τρόπο αντιμετώπισής τους χρησιμοποιώντας τις τεχνολογίες της Sophos. Η Sophos μια διακεκριμένη εταιρία στο Security, είναι η πρώτη που έφερε στην αγορά τη Συνδυαστική Ασφάλεια (Synchronized Security) όπου τα συστήματα ασφάλειας της περιμέτρου ανταλλάζουν σημαντικές πληροφορίες με τις τερματικές συσκευές, προσφέροντας τεχνητή νοημοσύνη στη λήψη αποφάσεων για τη διαχείριση ασφάλειας σε μία επιχείρηση χωρίς εξειδικευμένους ανθρώπινους πόρους.

Σωτήρης Σαράντος & Ευάγγελος Καψαλάκης

Η μετάβαση των υποδομών μιας επιχείρησης στο Microsoft Azure είναι πια αντικείμενο καθημερινών συζητήσεων. Πρωτεύον μέλημα αποτελεί η ασφάλεια των δεδομένων, όπως μας εξήγησαν ο **Σωτήρης Σαράντος** - Channel Manager, **Digital Sima** και ο **Ευάγγελος Καψαλάκης** - Solution Specialist, Cloud Infrastructure της **Microsoft**. Η Barracuda, ο πρώτος Microsoft Azure Certified Security solution provider, έχει λύση με το Web Application Firewall (WAF) για το MS Azure.
Η λύση WAF της Barracuda, προσφέρει Application Security (OWASP Top 10, application layer DDoS, SQL injection, κα), proactive defense χαρακτηριστικά (Geo-IP Control, Application Cloaking, IP Reputation), Data Loss Prevention, αλλά επιπλέον Identity & Access Management καθώς επίσης υψηλή διαθεσιμότητα, Autoscaling, Load Balancing.Η Microsoft αναλαμβάνει την υποδομή του MS Azure. Η Barracuda με το Web Application Firewall, μπορεί να προστατέψει το περιεχόμενο της υποδομής και να διασφαλίσει τα δεδομένα της εταιρείας!

David Grout

Την αναγκαιότητα μετάβασης από μια reactive σε μια proactive προσέγγιση τόνισε ο **David Grout** - Technical Director South Emea της **Fireeye**. Μια προσέγγιση που μετουσιώνεται σε πράξη μέσα από λύσεις Endpoint & Intelligence. Επίσης παρουσίασε την πρόταση FireEye Security Orchestrator που επιτυγχάνει την αξιολόγηση, τον εντοπισμό και αποτροπή απειλών, την ανάλυση και άμεση ανταπόκριση καθώς και την βελτιστοποίηση ROI/TCO.

Ανδρέας Λάλος & Arik Kasha

Με το 90% των περιστατικών ασφάλειας να οφείλονται σε εσωτερικούς χρήστες (σύμφωνα με το Verizon Report 2015), η αντιμετώπιση του ρίσκου που ενέχεται στη δραστηριότητα των χρηστών (Inside Threat) είναι ίσως η μεγαλύτερη πρόκληση στο IT Security. Ο **Ανδρέας Λάλος** από την **Besecure** μαζί με τον Regional Manager της **ObserveIT**, για την Ελλάδα και την Κύπρο, **Arik Kasha** παρουσίασαν την πλέον ολοκληρωμένη λύση στην κατηγορία του Inside Threat. Το ObserveIT συνδυάζει την καταγραφή της δραστηριότητας των χρηστών με τη δημιουργία και αποθήκευση ευανάγνωστων metadata logs, καθιστώντας την αναζήτηση του περιστατικού πολύ απλή και γρήγορη. Με την εγκατάσταση του ObserveIT περισσότερες από 180 έτοιμες προς εφαρμογή και προσαρμόσιμες πολιτικές, δημιουργούν ένα πλαίσιο κανόνων το οποίο μπορεί να χρησιμοποιηθεί για να ειδοποιεί ή ακόμη και να σταματάει εν τη γενέσει ύποπτες ή επικίνδυνες δραστηριότητες.

Mehmet Dagdevirenturk

Ο Mehmet Dandevirenturk - Channel Manager της **Trend Micro** για Τουρκία, Ελλάδα και Κύπρο - μας μίλησε για την επαναστατική νέα τεχνολογία XGen. Οι απειλές τύπου Crypto-ransomware επηρέασαν δραματικά την εξέλιξη της αγοράς της ασφάλειας, με αποτέλεσμα να δημιουργηθεί η ανάγκη ανάπτυξης προηγμένων λύσεων που να περιέχουν νέες τεχνικές ανίχνευσης όπως Machine Learning.Έχουμε δει όμως ότι ούτε και αυτές από μόνες τους αρκούν για να αποτρέψουν τις απειλές αποτελεσματικά. Κλείνοντας την ομιλία του, ευχαρίστησε την Cysoft ΕΠΕ - Gold Partner της Trend Micro για την πρόσκλησή της να παρουσιάσει την Trend Micro στην Infocom Security 2017 και υπέδειξε την ειδικότητά της στην κατηγορία Enterprise Products.

Χάρης Πυλαρινός

Οι επιθέσεις σε εταιρικά δίκτυα είναι πλέον συχνό φαινόμενο. Μία στοχευμένη επίθεση ενδέχεται να παρακάμψει τους περιμετρικούς μηχανισμούς ασφαλείας καθώς και τα συμβατικά antivirus υποστήριξε ο **Χάρης Πυλαρινός** - Systems Engineer, **Naftomar Shipping and Trading** που μίλησε στο συνέδριο ως καλεσμένος της IT WAY. Σε αυτή την περίπτωση ο οργανισμός είναι εκτεθειμένος και ο επιτιθέμενος αποκτά πρόσβαση στο εσωτερικό δίκτυο, ελεύθερος να επεκταθεί μέχρι να φτάσει στον στόχο του. Η παρουσίαση είχε ως στόχο να αναδείξει μεθόδους και τεχνικές που

χρησιμοποιούνται από κακόβουλους χρήστες και να αναλύσει τα διαφορετικά στάδια στα οποία εξελίσσεται μία επίθεση, εξηγώντας παράλληλα τρόπους έγκαιρης αντίληψης αυτών χρησιμοποιώντας την πλατφόρμα της Rapid7, InsightIDR.

Παναγιώτης Κουρής & Μάνος Πέπης

Η Office Line και η Creative Ideas, ηγέτιδες εταιρείες παροχής ολοκληρωμένων λύσεων Πληροφορικής έδωσαν γι' ακόμα μία φορά δυναμικό παρών στο InfoCom Security 2017. Στο πλαίσιο της συμμετοχής τους αποτύπωσαν από κοινού το στίγμα γύρω από τις εξελίξεις, τη δυναμική και την αξιοποίηση του cloud στο σύγχρονο επιχειρείν. Ο CEO της Office Line **Παναγιώτης Κουρής**, σε συνεργασία με τον CEO της Creative Ideas **Μάνο Πέπη**, ανέπτυξαν τα πλεονεκτήματα της χρήσης τεχνολογιών cloud και πώς cloud based λύσεις και υπηρεσίες μπορούν να συμβάλλουν στην ενίσχυση της παραγωγικότητας των επιχειρήσεων. Παράλληλα ανέλυσαν πρακτικές πάνω σε ένα πολύ επίκαιρο θέμα, αυτό της προστασίας των δεδομένων, παρουσιάζοντας cloud υποδομές κι εργαλεία για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας τόσο των προσωπικών, όσο και των εταιρικών δεδομένων, σε συνάρτηση με τη θέσπιση του νέου Ευρωπαϊκού Κανονισμού GDPR.

Luis Angel del Valle

Η καινοτόμος λύση ασφάλειας εγγράφων της Sealpath αναπτύχθηκε έτσι ώστε να εξασφαλιστεί ότι οι εμπιστευτικές πληροφορίες θα πρέπει να φτάνουν μόνο στους σωστούς αποδέκτες και όχι σε τρίτους. Η λύση, που μας παρουσίασε ο **Luis Angel del Valle** - Chief Executive Officer and Co-founder, **SealPath** - ως καλεσμένος της NSS, διαχειρίζεται το θέμα της ασφάλειας των εγγράφων ακόμα και αν αυτά φύγουν από την ασφαλή περίμετρο ή τις προστατευμένες τερματικές συσκευές μίας εταιρίας, δίνοντας τη δυνατότητα στην επιχείρηση να έχει τον πλήρη έλεγχό τους όπου και αν βρίσκονται. Η λύση εκτός από την κρυπτογράφηση των εγγράφων, επιτρέπει στον δημιουργό του εκάστοτε εγγράφου να διαχειρίζεται σε πραγματικό χρόνο τα δικαιώματά του, προσαρμόζοντας το επίπεδο ασφάλειας του οποιαδήποτε στιγμή.

Πάνος Οπλοποιός

Σε μια πολύ ξεχωριστή ομιλία, ο Σύμβουλος σε θέματα Ψηφιακής Τεχνολογίας του Υπουργείου Τουρισμού, **Πάνος Οπλοποιός** ανέδειξε στο κοινό την ιστορία πίσω από Μπλέτσλεϊ Πάρκ (Bletchley Park) που βρίσκεται 80 χιλιόμετρα βορειοδυτικά του Λονδίνου και κατά το Β' Παγκόσμιο Πόλεμο αποτέλεσε τη βασικότερη υπηρεσία αποκρυπτογράφησης της Βρετανίας. Εκεί ο διάσημος μαθηματικός Αλαν Τούρινγκ, κατάφερε να αποκρυπτογραφήσει μαζί με την ομάδα του, την περιβόητη μηχανή κρυπτογράφησης των Ναζί με την ονομασία "Enigma" που ήταν το βασικό σύστημα ασύρματης κωδικοποιημένης μετάδοσης πληροφοριών των Γερμανών, δημιουργώντας μια αντίστοιχη μηχανή με την ονομασία "The Bombe". Χάρη σε αυτό το επίτευγμα η έκβαση του Β' Παγκοσμίου πολέμου μειώθηκε τουλάχιστον κατά 2 χρόνια, με αποτέλεσμα να σωθούν εκατομμύρια άνθρωποι.

Κωνσταντίνος Παπαχριστοφής

Ο **Κωνσταντίνος Παπαχριστοφής** ως Educational ICT Consultant/Instructor Security Expert (CCNP Sec) του εκπαιδευτικού οργανισμού **InterLei**, παρουσίασε τις προοπτικές και τα οφέλη των εκπαιδευτικών προγραμμάτων για τη νέα γενιά των penetration testers που θα μπορούν να ανταποκριθούν αποτελεσματικά στην αντιμετώπιση των νέων προηγμένων ψηφιακών απειλών. Τα προγράμματα αυτά μπορούν να αναβαθμίσουν σε μεγάλο βαθμό τις τεχνικές γνώσεις των Ethical Hackers και να αυξήσουν σημαντικά τις πιθανότητες να απορροφηθούν σε τμήματα ασφάλειας κάποιου οργανισμού.

Θανάσης Διόγος

Εκπροσωπώντας το **(ISC)2 Hellenic Chapter** ο **Θανάσης Διόγος**, ανέδειξε το τοπίο των APTs σε βάθος χρόνου, κάνοντας μια ιστορική αναδρομή και περιγράφοντας την εξέλιξη των απειλών μέσα από συγκεκριμένα παραδείγματα, όπου malware προκάλεσαν σημαντικά προβλήματα. Βασικοί σταθμοί αυτής της αναδρομής είναι τα Botnets αλλά και οι τεχνικές των Social Engineering. Ο ομιλητής επισήμανε ότι από την πλευρά των θυμάτων του οργανωμένου ηλεκτρονικού εγκλήματος, παρατηρούνται ακόμα αδύναμοι μηχανισμοί ανίχνευσης αλλά και αδυναμία ανταπόκρισης στα περιστατικά ασφάλειας.

Ιωάννης Πάσχος

Για το πολύ σημαντικό θέμα των ψηφιακών forensics είχαμε την ευκαιρία να ενημερωθούμε από τον πλέον ειδικό στο συγκεκριμένο τομέα, κύριο **Ιωάννη Πάσχος** - Αξ/κός ΕΛ.ΑΣ

ε.α, Εξεταστής ψηφιακών πειστηρίων, Δικαστικός Πραγματογνώμονας. Η αναγνώριση, διατήρηση, εξαγωγή, ερμηνεία και καταγραφή των ευρημάτων που εντοπίζονται στα ψηφιακά πειστήρια και η παρουσίασή τους στο δικαστήριο είναι μια πολύ σημαντική διαδικασία στις μέρες μας ενώ θα πρέπει να δίνεται ιδιαίτερη σημασία στη διατήρηση των log files και σίγουρα θα πρέπει να απευθυνόμαστε σε ειδικούς όταν προκύψει ένα πρόβλημα και όχι μέτα.

Δρ. Χριστόφορος Νταντογιάν

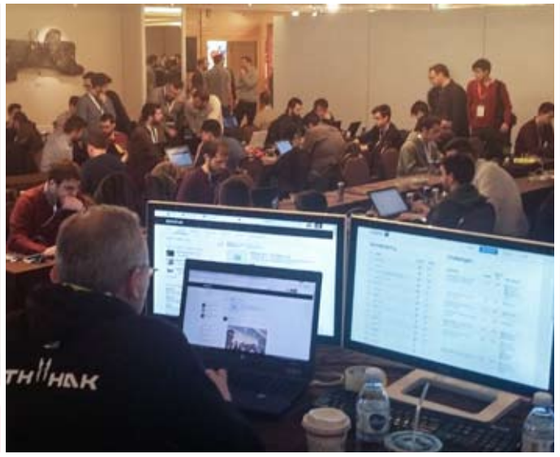
Η χρήση διαφορετικών μυστικών κωδικών (passwords) για κάθε εφαρμογή ως μοντέλο αυθεντικοποίησης έχει αποτύχει, καθώς δεν παρέχει το επίπεδο ασφάλειας που απαιτούν οι σημερινές εφαρμογές Διαδικτύου επισήμανε στην ομιλία του ο **Δρ. Χριστόφορος Νταντογιάν** - Research Associate, Τμήμα Ψηφιακών Συστημάτων, **Πανεπιστήμιο Πειραιά.** Επιπλέον, οι μυστικοί κωδικοί δεν είναι εύκολοι στη χρήση, καθώς εύκολα μπορεί να ξεχαστούν. Συνδυάζοντας καινούργιες τεχνολογίες όπως η βιομετρική αυθεντικοποίηση, το πρωτόκολλο FIDO, η χρήση υλικού για ασφαλή εκτέλεση εφαρμογών (Trusted Execution Environment) και τα ανώνυμα διαπιστευτήρια (Anonymous Credentials), ο στόχος του H2020 έργου -με το όνομα ReCRED- είναι η προώθηση της κινητής συσκευής του χρήστη ως πύλη για την είσοδο του στον ψηφιακό κόσμο.

Χρήστος Ξενάκης

Ο Αναπλ. Καθηγητής από το Τμήμα Ψηφιακών Συστημάτων, **Πανεπιστήμιο Πειραιά** κ. Ξενάκης παρουσίασε την Ελληνική συμμετοχή στον Πανευρωπαϊκό διαγωνισμό κυβερνοασφάλειας, European Cyber Security Challenge 2017 (ECSC '17). Ο διαγωνισμός αποσκοπεί στην ανεύρεση, προσέλκυση και ανάδειξη νέας γενιάς ταλέντων στον χώρο της προστασίας και ασφάλειας πληροφοριακών συστημάτων και δικτύων. Η Ελλάδα για δεύτερη συνεχή χρονιά θα δώσει το παρόν στο διαγωνισμό, με μία 10μελή ομάδα ταλέντων στη Μάλαγα της Ισπανίας, από τις 30 Οκτωβρίου έως τις 3 Νοεμβρίου 2017. Την ευθύνη της Ελληνικής συμμετοχής για φέτος φέρει το Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά.

2ο Ethihak Contest

Ο Κωνσταντίνος Βαβούσης - Αρχισυντάκτης του secnews.



Για 2η συνεχή χρονιά ο διαγωνισμός EthiHak που διοργανώθηκε από την ομάδα του SecNews.gr στα πλαίσια του InfoCom Security έλαβε σάρκα και οστά και στέφθηκε με επιτυχία. Το EthiHak απέδειξε ξανά ότι οι ethical-hackers **βρίσκονται στο πλευρό εταιρειών και επιχειρηματιών**, καθώς κρίνονται ιδιαίτερα χρήσιμοι στην **ενδυνάμωση των πληροφοριακών συστημάτων** έναντι των σύγχρονων τεχνολογικών προκλήσεων και κινδύνων. Οι διαγωνιζόμενοι χρησιμοποιώντας τις ικανότητες τους στο hacking, κλήθηκαν να αξιολογήσουν την ασφάλεια πληροφοριακών συστημάτων και υποδομών, εναντίον live στόχων.

Σκοπός του EthiHak ήταν για ακόμα μια φορά να δώσει τη δυνατότητα στους συμμετέχοντες να εξασκηθούν στο έπακρον στην εφαρμογή εργαλείων επίθεσης εναντίον πραγματικών στόχων και όχι θεωρητικών σεναρίων. Ταυτόχρονα, μέσα από την διαδικασία του διαγωνισμού, οι παρευρισκόμενοι ενημερώνονται σχετικά με σύγχρονες απειλές, κενά ασφαλείας αλλά και τρόπους χρήσης του διαδικτύου.

Στόχος της προσπάθειας του **SecNews** αλλά και του **EthiHak** ήταν να αναδείξει τους **ethical hackers** -τους ηθικούς hackers- και όχι να παροτρύνει την κακόβουλη χρήση του internet. Στην ουσία, οι νέοι που ασχολούνται με την πληροφορική και δη με την ασφάλεια πληροφοριακών συστημάτων, μαθαίνουν να βρίσκουν αδυναμίες στα συστήματα με στόχο την επίλυση τους και όχι την εκμετάλλευση προς ίδιον όφελος. Αξίζει ένα μεγάλο μπράβο σε όλους τους διαγωνιζόμενους του EthiHak, σε όποιο σημείο και αν έφτασαν, στην **Odyssey** που ως Χορηγός του διαγωνισμού, φρόντισε και φέτος όπως και πέρσι να δώσει ακόμα ένα κίνητρο στα παιδιά του Ethihak να συμμετάσχουν αλλά και σε όλη την ομάδα του Secnews.gr που οργάνωσε το διαγωνισμό. Φυσικά το μεγαλύτερο μπράβο οφείλουμε να το πούμε στους νικητές του φετινού **EthiHak, την ομάδα Greunion**. Η Greunion ισοβάθμησε με την ομάδα An0ncore αλλά κατάφερε να κερδίσει στα σημεία, δηλαδή στη βαθμολογία που φάνηκε στο αναλυτικό report της ομάδας. **Οι τρεις πρώτες θέσεις διαμορφώθηκαν ως εξής:**

1η θέση: **Greunion**
2η θέση: **An0ncore**
3η θέση: **Aggressive Cake**

Όλοι οι Νικητές του 2ου Ethihak Contest.

Οι Χορηγοί του InfoCom Security 2017

Για ακόμα μια χρονιά, η συμβολή των χορηγών εταιρειών του InfoCom Security στη διοργάνωση και την επιτυχία του συνεδρίου ήταν καθοριστική.

Encode

Checkpoint

Odyssey

Cisco & Space

Adacom με Fireye & Gemalto

Cosmote

Deloitte

Fortinet

Aspida

Crypteia Networks

Netbull

NSS

ESET

CYSOFT

Digital Sima

ITWAY με RAPID

Partnernet

Priority

BeSecure

Premium IT

BitDefender

Report

Rohde & Schwarz

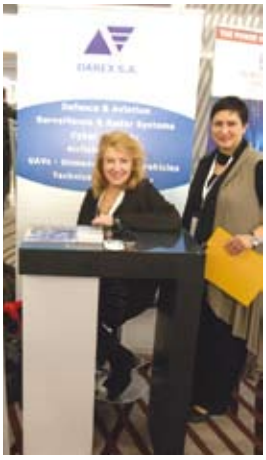
Creative Ideas & Office Line

AQS

Arebas

Audax

Avira



Darex

iPhoenix

Interlei

Mediterranean College

Metropolitan College

Πανεπιστήμιο Πειραιά

CL8