

REPORT

3ο Infocom Security

Οι νέες τάσεις στο IT...
και οι “εντάσεις” στην Ασφάλεια!



Η δυναμική του τομέα της Ασφάλειας Πληροφοριών και οι τάσεις που επικρατούν, αποτυπώθηκαν πλήρως στο συνέδριο Infocom Security που διοργανώθηκε φέτος για 3η συνεχόμενη χρονιά, συνιστώντας την κορυφαία ετήσια συνεδριακή εκδήλωση του χώρου.

Η πολύτιμη κληρονομιά από την επιτυχία των δύο προηγούμενων διοργανώσεων, είναι λογικό να είχε δημιουργήσει αυξημένες απαιτήσεις και για το φετινό συνέδριο Infocom Security. Με πολυάριθμη λοιπόν συμμετοχή άνω των 800 συνέδρων – επαγγελματιών IT, από μεγάλες επιχειρήσεις και Οργανισμούς, υποστήριξη από 23 χορηγούς – σημαντικές εταιρείες του χώρου, καθώς και 24 παρουσιάσεις με πολύ ενδιαφέρον περιεχόμενο από εξειδικευμένους ομιλητές από την Ελλάδα αλλά και το εξωτερικό, η 3η διοργάνωση του **Infocom Security** κάλυψε και με το παραπάνω τις υψηλές αυτές απαιτήσεις, επιβεβαιώνοντας στην πράξη τη δυναμική που έχει αναπτύξει η συγκεκριμένη συνεδριακή εκδήλωση. Το 3ο Συνέδριο Infocom Security - που πλέον αποτελεί σημείο αναφοράς στον τομέα των εκδηλώσεων της Ασφάλειας Πληροφοριών - πραγματοποιήθηκε στις 10 Απριλίου στο Divani Caravel και την ευθύνη της διοργάνωσης είχαν σε συνεργασία, το περιοδικό **IT Security Professional** της εταιρείας Press Line και η εταιρεία Smart Press που εκδίδει το

περιοδικό **INFOCOM** και διοργανώνει κάθε χρόνο σειρά επιτυχημένων συνεδρίων τεχνολογίας στο χώρο της πληροφορικής και των επικοινωνιών.

Η κεντρική ιδέα του φετινού συνεδρίου μετουσιώθηκε στον τίτλο «**Οι νέες τάσεις στο IT... και οι “εντάσεις” στην Ασφάλεια**» θέλοντας έτσι να αναδείξουμε τις επιπτώσεις που προκύπτουν και τις παραμέτρους που πρέπει να λαμβάνονται υπόψη σχετικά με την ασφάλεια πληροφοριών στο νέο οικοσύστημα του IT, όπως αυτό έχει διαμορφωθεί με την υιοθέτηση των νέων τάσεων από πλευράς των επιχειρήσεων στις υποδομές πληροφορικής.

Στην έναρξη του Συνεδρίου χαιρετισμό απηύθυνε ο Πρόεδρος της Οργανωτικής Επιτροπής **Κώστας Νόσσης**, καθώς και οι κύριοι **Δημήτρης Μπογιατζής** (Μέλος Δ.Σ., e-TEE), **Νίκος Φαλδαμής** (Πρόεδρος, HePIS), **Δημήτρης Δρακούλης** (Πρόεδρος ΕΜηΠΕΕ) και **Ανέστης Δημόπουλος** (Αντιπρόεδρος Δ.Σ. ΙΕΣΠ - ISACA Athens Chapter), οι οποίοι εκπροσώπησαν φορείς και Οργανισμούς που υποστήριξαν το Infocom Security 2013.

REPORT

3ο Infocom Security

1η Ενότητα - Ο μετασχηματισμός του IT και οι επιπτώσεις στην ασφάλεια

Στην πρώτη ενότητα του Συνεδρίου, την οποία συντόνισε ο δημοσιογράφος **Γιάννης Ριζόπουλος**, οι ομιλητές αναφέρθηκαν κυρίως στα ρίσκα που ανακύπτουν από τη χρήση των νέων τάσεων όπως τα Social Media, το mobility, το BYOD και φυσικά το Cloud.



Ο κος **Δημήτρης Γκριτζαλής**, Καθηγητής Ασφάλειας ΤΠΕ στο Οικονομικό Πανεπιστήμιο Αθηνών

Συγκεκριμένα, με ιδιαίτερο ενδιαφέρον παρακολούθησαμε την εναρκτήρια ομιλία του συνεδρίου που έγινε από τον Καθηγητή Ασφάλειας ΤΠΕ στο Οικονομικό Πανεπιστήμιο Αθηνών, **Δημήτρη Γκριτζαλή**, με τίτλο "Ιστορίες Χαράς και Τρόμου από το Θαυμαστό Καινούριο Κόσμο των Social Media". Η παρουσίαση του κ. Καθηγητή βασίστηκε σε μια έρευνα που βρίσκεται σε εξέλιξη από τον ίδιο και τους συνεργάτες του και αφορά στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων στα κοινωνικά δίκτυα. Από τα αποτελέσματα της έρευνας αυτής προκύπτει ότι η μεθοδική αξιοποίηση των ευρημάτων δεδομένων από κοινωνικά δίκτυα όπως το Twitter και το You Tube, μπορούν να οδηγήσουν στην αξιολόγηση προδιάθεσης παραβατικής συμπεριφοράς (π.χ. εκ των έσω απειλές σε κρίσιμες υποδομές), στη δημιουργία μορφώτου που χρήστη με στόχο προσωποποιημένη προβολή/διαφήμιση (π.χ. consumer profiling) ή ακόμα στη δυνατότητα πρόληψης αυτοκαταστροφικών

ενεργειών (π.χ. εφηβικές αυτοκτονίες).



Ο κος **Δημήτρης Μουζακίτης**, Senior Information Security Management Consultant, **Odyssey Consultants**

Συνεχίζοντας την αναφορά του στα κοινωνικά δίκτυα και τη σχέση τους με την ασφάλεια - αλλά σε επαγγελματικό περιβάλλον αυτή τη φορά - ο επόμενος ομιλητής, κος **Δημήτρης Μουζακίτης**, (Senior Information Security Management Consultant, **Odyssey Consultants**) τόνισε την ανάγκη για την υιοθέτηση μιας «Social Media Policy» για κάθε εταιρικό χρήστη, μέσα από τη θέσπιση κανόνων που θα πρέπει να ακολουθούν όλοι μέσα στον Οργανισμό. Επίσης επισήμανε την αναγκαιότητα εκπαίδευσης του προσωπικού για θέματα που σχετίζονται με τα κοινωνικά δίκτυα και τους κινδύνους που μπορεί να προκύπτουν από την αλόγιστη χρήση τους στο εταιρικό περιβάλλον.



Ο κος **Αλέξανδρος Ντέτσικας**, Information Security Consultant της **Space Hellas**

Η βέλτιστη διαχείριση της τάσης του BYOD ήταν το θέμα που ανέπτυξε ο κος **Αλέξανδρος Ντέτσικας**, Information Security Consultant της **Space Hellas**. Ο ομιλητής υποστήριξε πως η τάση της αξιοποίησης των προσωπικών φορητών συσκευών στο εταιρικό περιβάλλον, είναι

μία πραγματικότητα που οι επιχειρήσεις οφείλουν να αποδεχθούν με βάση κάποιους κανόνες - και όχι να αποτρέψουν. Η εφαρμογή του BYOD μπορεί να είναι μια επιτυχημένη διαδικασία για τον Οργανισμό, αρκεί αυτός να εκπαιδεύει συνεχώς τους χρήστες σε θέματα ασφάλειας και διαχείρισης δεδομένων και να συνεργάζεται μαζί τους, τόνισε ο κος Ντέτσικας.



Ο Δρ. **Θεόδωρος Σεργίου**, Security Solutions Product Manager, Marketing Department, Services Business Division, **Intracom Telecom**

Από την πρώτη ενότητα δεν θα μπορούσαν φυσικά να λείπουν οι αναφορές για την ασφάλεια στο cloud. Έτσι, ο Δρ. **Θεόδωρος Σεργίου** (Security Solutions Product Manager, Marketing Department, Services Business Division, **Intracom Telecom**) ανέλαβε στη συνέχεια να μας παρουσιάσει 4 βασικά διδάγματα που οφείλουν να ακολουθούν οι επιχειρήσεις, σε σχέση με την ανάπτυξη των υπηρεσιών cloud. Σε αυτά περιλαμβάνονται: η διαπίστωση ότι στο cloud πρέπει να λαμβάνονται υπόψη πολλές παράμετροι - κάτι που δεν είναι μια εύκολη υπόθεση - και ότι σε αυτές τις παραμέτρους κυρίαρχο ρόλο έχει η ασφάλεια, η συμμόρφωση με πρότυπα και κανονιστικά πλαίσια, καθώς επίσης και η ιδιαίτερη προσοχή που πρέπει να δίνουν οι Οργανισμοί στην επιλογή του συνεργάτη, για τη δημιουργία ενός public ή private cloud.



Ο κος **Ibrahim Yusuf**,
Presales Engineer,
Sophos

Τα ρίσκα που ανακύπτουν από τη χρήση των smartphones στο εταιρικό περιβάλλον καθώς και το πώς μπορούν οι επιχειρήσεις να τα διαχειριστούν, ήταν το θέμα που ανέ-

λυσε στην παρουσίασή του ο κος **Ibrahim Yusuf**, Presales Engineer της εταιρείας **Sophos**. Αφού μας παρουσίασε το νέο περιβάλλον στο IT, όπως αυτό έχει διαμορφωθεί με τη ραγδαία ανάπτυξη της φορητότητας, ο ομιλητής έδωσε έμφαση στη θέσπιση εταιρικής στρατηγικής και πολιτικών για όσους χρησιμοποιούν φορητές συσκευές στο εταιρικό περιβάλλον, αξιοποιώντας εφαρμογές ελέγχου, κρυπτογραφίας, patching, καθώς και πολύτιμα εργαλεία διαχείρισης φορητών συσκευών.



Η κα **Διονυσοπούλου Νατάσσα**, Brand Manager της εταιρείας **ITway**

Στη συνέχεια, η κα **Διονυσοπούλου Νατάσσα**, Brand Manager της εταιρείας **ITway**, μας παρουσίασε την προσέγγιση της McAfee σε σχέση με την "έξυπνη" ασφάλεια

που βασίζεται σε μια ολοκληρωμένη πλατφόρμα διασυνδεδεμένων εργαλείων και λειτουργιών, η οποία βελτιστοποιεί τις δυνατότητες προστασίας των δεδομένων στους Οργανισμούς. Η ενοποίηση όλων των απαραίτητων συστατικών για την ασφάλεια που επιτυγχάνει η πλατφόρμα της McAfee, απαντά με επιτυχία στις προκλήσεις που φέρνουν οι νέες απειλές, ενισχύοντας παράλληλα την αξία όλων των επιχειρη-

ματικών λειτουργιών, επισήμανε η ομιλήτρια.



Ο **Adrian Porcescu**,
Technical Consultant &
Trainer της **Kaspersky Lab**

Κλείνοντας την πρώτη ενότητα του συνεδρίου, ο κος **Adrian Porcescu**, Technical Consultant & Trainer της **Kaspersky Lab**, αφού ανέλυσε στους συνέδρους την εξέλιξη των απειλών και τη σύγχρονη πραγματικότητα, εκτίμησε ότι το κακόβουλο λογισμικό θα συνεχίσει να αναπτύσσεται ραγδαίως και οι ηλεκτρονικοί εγκληματίες θα στοχεύουν ολοένα και περισσότερο στις φορητές συσκευές με Android και Apple OS, ενώ παράλληλα θα ενταθούν οι επιθέσεις στις κρίσιμες και κυβερνητικές υποδομές. Ο ομιλητής παρουσίασε επίσης τις λύσεις που έχει αναπτύξει η kaspersky για να αντιμετωπίσει τις σύγχρονες απειλές με μία μόνο πλατφόρμα, που ενοποιεί όλα τα απαραίτητα εργαλεία τα οποία αντιμετωπίζουν με επιτυχία το τρίπτυχο των απαιτήσεων "προστασία - έλεγχος - διαχείριση".

2η Ενότητα: Η καινοτομία, κλειδί για την αποτελεσματική ασφάλεια

Στη δεύτερη ενότητα, στην οποία συντονιστής ήταν ο Αρχισυντάκτης του IT Security Professional, **Αμανατίδης Βλάσης**, δόθηκε έμφαση στις στρατηγικές που πρέπει να αναπτύξουν οι υπεύθυνοι των τμημάτων IT, προκειμένου να προστατεύσουν αποτελεσματικά τα κρίσιμα επιχειρηματικά δεδομένα, με βάση καινοτόμες ιδέες και προτάσεις.

Σε αυτά τα πλαίσια, ο κος **Θανάσης Παπαδόπουλος**, Country Manager της ITway, ανέλυσε στους συνέδρους



Ο κος **Θανάσης Παπαδόπουλος**,
Country Manager της
ITway

τις προκλήσεις σε σχέση με την ασφάλεια που αντιμετωπίζουμε στην Ελλάδα αλλά και σε όλη τη Νότια Ευρώπη, λαμβάνοντας υπόψη τις ιδιαιτερότητες της περιοχής που

έχουν προκύψει λόγω της οικονομικής κρίσης, παρουσιάζοντας παράλληλα τη στρατηγική και το πολύ μεγάλο φάσμα των καινοτόμων λύσεων και υπηρεσιών για την ασφάλεια των πληροφοριών, στην ευρύτερή της έννοια που διαθέτει ITway.



Ο κος **Chezki Gil**,
Territory Sales Manager,
East Mediterranean,
RSA

Στη συνέχεια, στο βήμα των ομιλητών ανέβηκε ο κος **Chezki Gil** (Territory Sales Manager, East Mediterranean, RSA) ο οποίος επικεντρώθηκε στην εξέλιξη των προηγμένων επιθέσεων

και πώς αυτές μπορούν να αντιμετωπιστούν από καινοτόμες λύσεις, όπως είναι η ολοκληρωμένη πλατφόρμα ελέγχου της ασφάλειας της RSA "Security Analytics" που επιτρέπει τη βέλτιστη δυνατή ορατότητα και αξιολόγηση των δεδομένων, καθώς και τη λύση των RSA Live Integrated Intelligence που μπορεί να ανακαλύψει κάθε «κρυφή παθογένεια».

Ο κος **Μιχάλης Σαμιωτάκης**, Technology Governance & Security, Assistant Manager στην **PwC**, στη δική του παρουσίαση τόνισε χαρακτηριστικά ότι «το cloud είναι εδώ και είναι η νέα εποχή!». Αυτό άλλωστε κατέδειξε η παγ-

REPORT

3ο Infocom Security



Ο κος **Μιχάλης Σαμιωτάκης**, Technology Governance & Security, Assistant Manager, **PwC**

κόσμια έρευνα για την Ασφάλεια Πληροφοριών που διεξήχθη από την PwC, όπου ειδικά για την Ελλάδα το 33% των συμμετεχόντων ανέδειξε μεταξύ άλλων ως πρώτη προτεραιότητα τη χάραξη μιας στρατηγικής για την ασφαλή μετάβαση σε αυτό. Ο ομιλητής, αφού στη συνέχεια παρουσίασε τις top 10 απειλές που αναδείχθηκαν από την έρευνα η οποία δημοσιεύθηκε πριν ένα μήνα από το Top Threats working Group του CSA - στο οποίο η PwC συμμετέχει ενεργά ως ένα από τα founding members - αναφέρθηκε στην αξιόπιστη λύση του Third Party Assurance, που είναι αναγνωρισμένο από το CSA και παρέχεται από όλους τους leading CSPs, σύμφωνα με την Gartner.



Ο κος **Πάνος Δημητρίου**, CTO & co-founder, **Encode**

Στη σύγχρονη προσέγγιση των Big Data Analytics και την άμυνα απέναντι στις προηγμένες επιθέσεις APT, με θεμέλιο πρωτοποριακές λύσεις και υπηρεσίες στην ασφάλεια, επικεντρώθηκε η παρουσίαση του κος **Πάνου Δημητρίου**, CTO & co-founder της **Encode**. Ο ομιλητής επισήμανε την ανάγκη επαναπροσδιορισμού του φαινομένου

των APT, λαμβάνοντας υπόψη την πολυπλοκότητα και ευελιξία του προβλήματος, όπως επίσης και τον ανθρώπινο παράγοντα που υπεισέρχεται σε αυτό. Τόνισε ακόμα την ανάγκη επανακαθορισμού της cyber στρατηγικής, με πυλώνα την ασφάλεια των Big Data Analytics και την έγκαιρη προειδοποίηση για τις ενδεχόμενες απειλές.



Ο κος **Συμεών Καλαματιανός**, Διευθυντής IT Risk Consulting στην **KPMG**

Ο κος **Συμεών Καλαματιανός**, Διευθυντής IT Risk Consulting στην **KPMG**, στα πλαίσια της δικής του παρουσίασης παρέθεσε πρόσφατες έρευνες της εταιρείας, που καταδεικνύουν την ασφάλεια ως την πλέον σημαντική πρόκληση που αντιμετωπίζουν οι Οργανισμοί στην υιοθέτηση ενός cloud περιβάλλοντος. Επίσης αναφέρθηκε στις αναφορές Service Organization Control (SOC) και πώς αυτές μπορούν να αξιοποιηθούν αποτελεσματικά. Παράλληλα, ανέπτυξε το πώς οι υπηρεσίες και η μεθοδολογία «IT Attestation» της **KPMG** μπορούν να βοηθήσουν αποτελεσματικά στην κατεύθυνση της διασφάλισης της προστασίας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων.

Την προσέγγιση της Trend Micro για την προστασία του Server Farm, μας παρουσίασε ο κος **Σωτήρης Δ. Σαράντος**, Σύμβουλος Δικτυακών Λύσεων της **Digital Sima**, προβάλλον-



Ο κος **Σωτήρης Δ. Σαράντος**, Σύμβουλος Δικτυακών Λύσεων της **Digital Sima**

τας τα βασικά πλεονεκτήματα της ενοποιημένης πλατφόρμας ασφαλείας «Trend Micro Deep Security» για την προστασία φυσικών, virtual και cloud υποδομών. Η συγκεκριμένη λύση συνδυάζει όλα τα απαραίτητα εργαλεία ασφαλείας για VMware περιβάλλοντα και παράλληλα ενισχύει την απόδοση των πόρων των υποδομών του Οργανισμού.



Ο κος **Ανέστης Δημόπουλος**, Αντιπρόεδρος του Δ.Σ. του **ISACA Athens Chapter**

Οι παρουσιάσεις της 2^{ης} ενότητας του συνεδρίου έκλεισαν με την ομιλία του Αντιπροέδρου του Δ.Σ. του **ISACA Athens Chapter**, κος **Ανέστης Δημόπουλος**, που ανέπτυξε τη μεθοδολογία για τη βελτιστοποίηση της αξιοποίησης των Big Data προς όφελος των επιχειρήσεων, ενώ παράλληλα προσέγγισε το κρίσιμο ζήτημα διαχείρισης των ρίσκων που προκύπτουν, θέτοντας και απαντώντας σε κρίσιμα ερωτήματα, όπως: Πού πρέπει να αποθηκεύουμε το μεγάλο όγκο δεδομένων; Πώς μπορούμε να τα προστατεύσουμε και να τα αξιοποιήσουμε με νόμιμο τρόπο και τι κάνουμε με τα «τοξικά» δεδομένα;

3η ενότητα: Προσαρμογή στις εξειδικευμένες ανάγκες

Στα πλαίσια της τρίτης ενότητας, που συντόνισε ο **Δρ. Βασίλης Βλάχος**, Καθηγητής Εφαρμογών του Τμήματος Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών στο ΤΕΙ Λάρισας, παρουσιάστηκαν από τους ομιλητές λύσεις που καλύπτουν συγκεκριμένες απαιτήσεις και προσαρμόζονται σε εξειδικευμένες ανάγκες στο επιχειρηματικό περιβάλλον. Την εναρκτική ομιλία στην 3^η ενότητα



Ο κος **Κώστας Κολοκοτρώνης**, Manager, Security Architecture Services της **Encode**

έκανε ο κος **Κώστας Κολοκοτρώνης**, Manager, Security Architecture Services της **Encode**, που επικεντρώθηκε στις διαδικασίες ελέγχου των διαχειριστών των IT υποδομών, αναφέροντας χαρακτηριστικά για τους διαχειριστές ότι: “...δεν μπορούμε να “ζήσουμε” χωρίς αυτούς, δεν μπορούμε να τους “περιορίσουμε” σε μεγάλο βαθμό, πρέπει όμως να βρούμε τρόπο ώστε να τους παρακολουθούμε στενά”. Η παραπάνω προσέγγιση σύμφωνα με τον ομιλητή, δεν είναι απλά μια βέλτιστη πρακτική, αλλά μια θεμελιώδης αρχή ασφάλειας.



Ο κος **Πάτροκλος Αργυρούδης (PhD)**, Ερευνητής Ασφάλειας Η/Υ, Υπεύθυνος Έρευνας και Ανάπτυξης της εταιρείας **Census**

Στην αξία της έρευνας ευπαθειών στις δοκιμές παρείσδυσης αναφέρθηκε στη συνέχεια ο κος **Πάτροκλος Αργυρούδης (PhD)**, Ερευνητής Ασφάλειας Η/Υ, Υπεύθυνος Έρευνας και Ανάπτυξης της εταιρείας **Cen-**

sus. Ο ομιλητής, αφού στην αρχή της παρουσίασής του προσδιόρισε τον ορισμό για την έρευνα ευπαθειών, στη συνέχεια περιέγραψε το πώς βελτιώνει μια δοκιμή παρείσδυσης η έρευνα ευπαθειών, κατά την οποία η ερευνητική ομάδα λειτουργεί παράλληλα με την ομάδα δοκιμών παρείσδυσης, εντοπίζει νέες αδυναμίες σε λογισμικό ή συστήματα που έχουν χαρακτηριστεί ως ενδιαφέροντα και τροφοδοτεί την ομάδα δοκιμών παρείσδυσης με νέα εργαλεία και exploits για συγκεκριμένες αδυναμίες. Έτσι η δοκιμή παρείσδυσης μπορεί πλέον να εξετάσει και το σενάριο στοχευμένης επίθεσης, το σενάριο εκμετάλλευσης αδυναμίας με 0-day exploits, την ορθή λειτουργία των proactive μηχανισμών ασφάλειας και την ετοιμότητα απέναντι σε μια αγνώστου φύσης απειλή.



Ο κος **Δημήτρης Παπίσης**, Senior Premier Field Engineer της **Microsoft Hellas**

Το παρόν και το μέλλον του PKI ανέπτυξε στην παρουσίασή του ο κος **Δημήτρης Παπίσης**, Senior Premier Field Engineer της **Microsoft Hellas**, παραθέτοντας τα χρόνια προβλήματα του PKI καθώς και τις λύσεις που προωθούνται για τη νέα εποχή. Οι αλλαγές που συντελούνται στο PKI, σύμφωνα με τον ομιλητή περιλαμβάνουν καινούριους αλγόριθμους (SHA-256 κ.λπ.), υποστήριξη clients (OS, browser, custom-made apps) αλλά και συνέχιση του παλαιού προτύπου για CAs (X.509) και συνδυασμό updates/CRLs/ OCSPs.

Η επόμενη παρουσίαση έγινε από κοινού από τον κος **Ανδρέα Λάλο**, Professional Services Director της **Besecure** και την κα **Amy Marion**, Marketing Director της **ObserveIT** και αφορούσε στις διαδικασίες του log analysis, παρουσιάζοντας τις σημαντικές προκλήσεις που υπάρχουν, όπως το μεγάλο όγκο και την



Ο κος **Ανδρέας Λάλος**, Professional Services Director της **Besecure**.



Η κα **Amy Marion**, Marketing Director της **ObserveIT**



Guy Eilon, South East Europe Regional Manager, **Websense** “Trends in the Threat Landscape”

πολυπλοκότητα των Log, καθώς και τις λύσεις που διαθέτει η **ObserveIT** και καλύπτουν σε μεγάλο βαθμό τις σύγχρονες απαιτήσεις για απομακρυσμένη παρακολούθηση, μείωση του κόστους συμμόρφωσης και άμεση “root cause ανάλυση”.

Εκπροσωπώντας την εταιρεία **Websense** και διαθέτοντας μεγάλη εμπειρία στον τομέα της ασφάλειας, ο κος **Guy Eilon** (South East Europe Regional Manager, **Websense**) είχε στη συνέχεια την ευκαιρία να προβάλει στους συνέδρους τα ποιοτικά και ποσοτικά χαρακτηριστικά των σύγχρονων απειλών

του διαδικτύου, επισημαίνοντας παράλληλα την ανάγκη για μείωση της πολυπλοκότητας των λύσεων ασφαλείας και την ενίσχυση του Total Cost of Ownership, στοιχεία που καλύπτονται πλήρως από τη λύση **TRITON** της **Websense** που μας παρουσίασε.

Η 3^η ενότητα του συνεδρίου έκλεισε με την ομιλία του κος **Γιώργου Σπηλιώτη** (Freelancer IT Consultant και ECC Certified Ethical Hacker), που παρουσίασε στους συνέδρους τα χαρακτηριστικά του “Two factor authentication” το οποίο προσφέρει αυξημένη ασφάλεια κατά τη

REPORT

3ο Infocom Security



Ο κος **Γιώργος Σπηλιώτης**, Freelancer IT Consultant και ECC Certified Ethical Hacker

διαπίστευση χρηστών, με περισσότερα του ενός αποδεικτικά - όπως συμβαίνει για παράδειγμα με τη χρήση των ATM (PIN + κάρτα). Κατά την παρουσίαση του κος Σπηλιώτης είχαμε επίσης την ευκαιρία να μάθουμε για τις μεθόδους υλοποίησης του TFA, καθώς και να δούμε αρκετά παραδείγματα χρήσης του σε cloud υπηρεσίες.

4η ενότητα: Νέας γενιάς Hacking και ο ιδιότυπος παγκόσμιος κυβερνοπόλεμος

Το 3ο Infocom Security έκλεισε με την τέταρτη ενότητα, κατά την οποία έμπειροι εισηγητές παρουσίασαν στους συνέδρους τα ποσοτικά και ποιοτικά χαρακτηριστικά των σύγχρονων ηλεκτρονικών εγκλημάτων και των μεθόδων των επιθέσεων που πραγματοποιούν με στόχο την υφαρπαγή δεδομένων ή την ακτιβιστική δράση, προβάλλοντας παράλληλα τεχνικές για την αντιμετώπιση αυτών των φαινομένων.

Στα πλαίσια λοιπόν της 4^{ης} ενότητας, ο κος **Κώστας Παπαδάτος**, COO & co-founder της **Encode**, μας παρουσίασε



Ο κος **Κώστας Παπαδάτος**, COO & co-founder της **Encode**

την “ανατομία” των σύγχρονων επιθέσεων με στόχο το οικονομικό όφελος, επισημαίνοντας τις μεγάλες αλλαγές που έχουν συντελεστεί στις μεθόδους που χρησιμοποιούν πλέ-

ον οι επιτιθέμενοι, εισάγοντας ακόμα και τον όρο “Malware as a Service” (Maas). Επίσης τόνισε την ανάγκη να ξεφύγουμε από τους παραδοσιακούς τρόπους ελέγχου και ασφάλειας, τονίζοντας ιδιαίτερα ότι η τεχνολογία από μόνη της δεν είναι αρκετή αλλά απαιτείται παράλληλα η εκπαίδευση όλων των χρηστών τραπεζικών online υπηρεσιών.



Ο κος **Χρήστος Βιδάκης**, Διευθυντής, IT Advisory, Risk and Management Consulting της KPMG

ΚPMG), θέτοντας στο επίκεντρο σημαντικά ζητήματα όπως είναι τα κίνητρα των δράσεων Hacking - αν δηλαδή έχουν ως αφετηρία κάποια ιδεολογία ή είναι απλά Business - ενώ παράλληλα μας παρουσίασε διάφορα σενάρια επίθεσης με τη χρήση εταιρικών πόρων (botnets). Επίσης παρακολουθήσαμε με ιδιαίτερο ενδιαφέρον μια επίδειξη που πραγματοποίησε ο κος Βιδάκης και αφορούσε σε σενάρια επίθεσης με την υποκλοπή κωδικών πρόσβασης, κλείνοντας την παρουσίασή του με το συμπέρασμα ότι απαιτούνται νέα αξιώματα ασφάλειας.

Στην παρουσίασή του ο κος **Μιχάλης Καλκαβούρας**, (Technology Consulting της Accenture), αφού επισήμανε ότι σήμερα οι επιθέσεις είναι πολλαπλές και μεταβάλλονται συνέχεια, τόνισε την ανάγκη να εντοπίζουμε και να ασφαλίζουμε τους πόρους του IT και όχι μόνο την περίμετρο, να δημιουργούμε μια ισχυρή κουλτούρα ασφάλειας στην επι-



Ο κος **Μιχάλης Καλκαβούρας**, Technology Consulting της Accenture

χείρηση, να δώσουμε μεγαλύτερη προσοχή στις εφαρμογές καθώς και στον έλεγχο της ταυτότητας του κάθε χρήστη και τέλος να αναπτύξουμε ακόμα περισσότερο την έννοια του «Cyber Situational Awareness».



Ο κος **Θανάσης Διόγος**, Security Engineer της **Microsoft Hellas**

Το συνέδριο έκλεισε με την ομιλία του κος **Θανάση Διόγους**, Security Engineer της **Microsoft Hellas**, που περιέγραψε - παρουσιάζοντας χαρακτηριστικά παραδείγματα -

το προφίλ και τους τρόπους δράσης των Anonymous μέσα από τα Social media, τα λεγόμενα “Online Riots” και επιθέσεις DDOS, ενώ παράλληλα επισήμανε τα νέα μοντέλα που απαιτούνται να υιοθετηθούν για την αντιμετώπιση των συγκεκριμένων φαινομένων. Ο ομιλητής έκλεισε “αποκαλύπτοντας” ότι το ΜΠΑ στο τίτλο της παρουσίασής του “Δεχόμαστε επίθεση; ΜΠΑ!” προέρχεται από το Μόνη Προηγμένη Απειλή, τονίζοντας ότι δεν υπάρχουν καθόλου περιθώρια εφησυχασμού.

Θα πρέπει επίσης να αναφέρουμε ότι κατά τη διάρκεια των εργασιών του συνεδρίου στην ολομέλεια, διοργανώθηκαν παράλληλα Security Labs από τις εταιρείες **Space Hellas**, **ODYSSEY CONSULTANTS** και **ESET HELLAS**, καθώς επίσης και από το **ISACA – Athens Chapter**.



Ιδιαίτερα πολύτιμη για την επιτυχία του Infocom Security 2013 ήταν η υποστήριξη των χορηγών – εταιριών του συνεδρίου.

Συγκεκριμένα, για ακόμα μια χρονιά Μεγάλος Χορηγός ήταν η **Encode**, ενώ Χρυσός Χορηγός ήταν οι **ITway**, **Odyssey Consultants** και **Space Hellas**.

Χορηγοί του συνεδρίου ήταν οι εταιρίες **Besecure**, **Census**, **Digital Sima**, **Eset Hellas**, **Intracom Telecom**, **IT Open Solutions**, **Kaspersky Lab**, **KPMG**, **McAfee**, **NSS & Sophos**, **PWC** και **RSA**.

Το συνέδριο υποστήριξαν επίσης οι εταιρίες **E-systems**, **HOL**, **Lighthouse**, **Phoenix Pro**, **PremiumIT** και **T&K** ενώ ιδιαίτερα σημαντική ήταν και η υποστήριξη του **ISACA Athens Chapter**, του **HEPIS** και των χορηγών επικοινωνίας. **iTSecurity**

