5ο Infocom Security
Mind the Risk. Be Proactive!

Με περισσότερους από 1500 συνέδρους, πάνω από 40 ομιλητές και 45 χορηγούς, το 5ο Συνέδριο Infocom Security επιβεβαίωσε την ανοδική πορεία της αγοράς της Ασφάλειας Πληροφοριών αλλά και το τεράστιο επιστημονικό και τεχνολογικό ενδιαφέρον που παρουσιάζει σήμερα ο συγκεκριμένος τομέας.

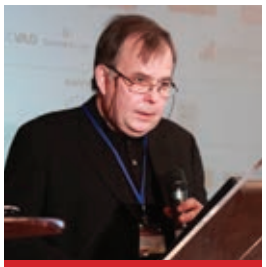
Η πολύ μεγάλη επιτυχία του **Infocom Security 2015** που διοργανώθηκε την **1η Απριλίου** για 5η συνεχόμενη χρονιά στο **Divani Caravel**, ισχυροποίησε ακόμα περισσότερο το τίτλο του «κορυφαίου event για την ασφάλεια πληροφοριών στην Ελλάδα». Το συνέδριο που διοργάνωσε όπως πάντα η εταιρία **Smart Press** και το περιοδικό **IT security professional**, προσέλκυσε φέτος πάνω από **1500 συνέδρους** και αποτέλεσε για ακόμα μια χρονιά το μεγάλο ετήσιο ραντεβού των ανθρώπων του χώρου της πληροφορικής, που ασχολούνται επαγγελματικά ή ενδιαφέρονται ακαδημαϊκά και επιστημονικά για το τομέα της ασφάλειας πληροφοριών. Σε ένα διαφορετικό και μεγαλύτερο χώρο από τις προηγούμενες διοργανώσεις, αλλά πάντα στο Divani Caravel, το φετινό συνέδριο είχε τη δυνατότητα να φιλοξενήσει στην αίθουσα της ολομέλειας περισσότερους συνέδρους, πιο πολλούς χορηγούς από κάθε άλλη φορά στον εκθεσιακό του χώρο, καθώς και αρκετά παράλληλα workshops, προσφέροντας μεγαλύτερη άνεση και περισσότερες διευκολύνσεις στους συμμετέχοντες και τους χορηγούς. Από όλες τις απόψεις ήταν μια αναβαθμισμένη και άκρως επιτυχημένη διοργάνωση που από τη μια πλευρά καταδεικνύει την πολύ μεγάλη ανταπόκριση του κόσμου της τεχνολογίας και της πληροφορικής για ένα ακόμα συνέδριο με το brand **Infocom** της Smart Press και παράλληλα επιβεβαιώνει το ιδιαίτερα μεγάλο ενδιαφέρον που υπάρχει για την αγορά και τις τεχνολογίες που συνοδεύουν την έννοια του Information Security, που πρώτο το περιοδικό IT Security Professional ανέδειξε σε αυτή την κλίμακα στην Ελλάδα.

Φυσικά, η μεγαλύτερη αξία και της φετινής διοργάνωσης του Infocom Security, ήταν το περιεχόμενο της θεματολογίας του συνεδρίου που για ακόμα μια φορά μέσα από τις παρουσιάσεις ειδικών από την Ελλάδα και το εξωτερικό, κατάφερε να αναδείξει συνολικά το περιβάλλον και τις απαιτήσεις γύρω από τον τομέα του Information Security και να ενημερώσει για τις επικαιροποιημένες τεχνολογίες, τις λύσεις, τις τεχνικές και τις στρατηγικές που εφαρμόζονται σήμερα. Κεντρικό μήνυμα του 5ου Infocom Security ήταν το **"Mind the Risk. Be Proactive!"** Θέλοντας έτσι, να τονίσει την σημερινή απαίτηση για την υιοθέτηση μεθόδων και διαδικασιών συνεχούς εκτίμησης των απειλών και των διαθέσιμων πόρων, καθώς επίσης και να δώσει έμφαση στην προστασία των κρίσιμων δεδομένων των επιχειρήσεων μέσα από μια πολιτική πρόληψης και επένδυσης σε τεχνολογίες, λύσεις, υπηρεσίες και πολιτικές ασφάλειας που δημιουργούν μια proactive προσέγγιση στην ψηφιακή ασφάλεια. Στην έναρξη του Συνεδρίου χαιρετισμό απηύθυνε ο Πρόεδρος της Οργανωτικής Επιτροπής **Κώστας Νόστης**, ο Πρόεδρος Δ.Σ. ΙΕΣΠ - ISACA Athens Chapter **Μιχάλης Σαμιωτάκης** , και ο Πρόεδρος του (ISC)² Hellenic Chapter, **Κώστας Παπαδάτος**.

1η ενότητα

The New Rules of Cyber Security

Κατά την 1η ενότητα του 5ου Infocom Security, οι ομιλητές περιέγραψαν κατά βάση το νέο τοπίο σχετικά με την ψηφιακή ασφάλεια και αναφέρθηκαν στους «νέους κανόνες του παιχνιδιού» μεταξύ επιτιθέμενων και επιχειρήσεων, χαρτογραφώντας τις τάσεις των απειλών σήμερα και τις διαφορετικές προσεγγίσεις που απαιτούνται για τη προστασία των πληροφοριών στο νέο οικοσύστημα.



Δρ. Λούις Μαρίνος

Ο πρώτος ομιλητής, ο Δρ. **Λούις Μαρίνος** - Network and Information Security, Research and Analysis Expert του **ENISA** - μέσα από την παρουσίαση του ανέλυσε το τοπίο των κυβερνοκινδύνων για το 2015 και αναφέρθηκε στις κορυφαίες απειλές που εντοπίστηκαν τα 2 προηγούμενα χρόνια σύμφωνα με έρευνες που έχει πραγματοποιήσει ο ENISA. Οι έρευνες αυτές, δείχνουν μεταξύ άλλων σημαντική άνοδο της διασποράς κακόβουλου κώδικα αλλά και των web based επιθέσεων. Ο ομιλητής, επισήμανε την ανάγκη για την όσο το δυνατόν βαθύτερη κατανόηση του είδους και των επιπτώσεων των εν δυνάμει απειλών απέναντι σε ένα οργανισμό, καθώς επίσης και την απαίτηση για ενίσχυση της γνώσης και των ικανοτήτων που θα επιτρέψουν να αντιμετωπιστούν οι απειλές, μέσα από τη συγκέντρωση και συσχέτιση πληροφοριών, αλλά και την οξοποίηση αυτοματοποιημένων εργαλείων.

Βασίλης Νικολόπουλος

Στη συνέχεια, ο **Βασίλης Νικολόπουλος** - Senior Security Consultant, για την **Check Point** στην Ελλάδα - αφού πρώτα ανέπτυξε προβληματισμούς που κάθε εταιρία πρέπει να λαμβάνει υπόψη, όπως για παράδειγμα, «το τι έχει να χάσει μια επιχείρηση» ή «ποιες θα είναι οι επιπτώσεις» από μια ενδεχόμενη επίθεση, περιέγραψε στη συνέχεια το πώς αρχικά σχεδιάζεται μια επίθεση αξιοποιώντας ευάλωτα σημεία που εμφανίζει το δίκτυο ενός οργανισμού. Ο ομιλητής, παρουσίασε επίσης την προσέγγιση της Checkpoint για την προστασία των πληροφοριών από γνωστές αλλά και άγνωστες απειλές, μια προσέγγιση που βασίζεται σε πολλαπλά επίπεδα ασφαλείας και περιλαμβάνει μηχανισμούς: IPS, Antivirus &Web URL φίλτρα, Anti-Bot και ένα πολύ σημαντικό εργαλείο, που είναι το Threat Emulation το οποίο αντιμετωπίζει προηγμένες επιθέσεις που προέρχονται από πολλά αρχεία.

Ελευθέριος Αντωνιάδης

Αιμιλία Ορφανίδου

Τη νέα πρόταση "Next Generation Security Information and Event Management" που μετουσιώνεται σε λύση μέσα από την πλατφόρμα ClearSkies, είχαν την ευκαιρία να παρουσιάσουν στους συνέδρους ο **Ελευθέριος Αντωνιάδης** και η **Αιμιλία Ορφανίδου** - Executive Director και Marketing Manager αντίστοιχα της εταιρείας **Odyssey Consultants**. Η συγκεκριμένη πλατφόρμα, που έχει αναπτύξει η ίδια η εταιρία, βασίζεται σε διεθνή πρότυπα και πρακτικές και συνεχίζει να εξελίσσεται και να αναβαθμίζεται συνεχώς όπως τόνισαν οι δύο ομιλητές. Μεταξύ πολλών πλεονεκτημάτων, η πλατφόρμα υποστηρίζει ελαχιστοποίηση των false positives, έγκαιρη ανάλυση και συσχέτιση των δεδομένων, συνεχή ανάλυση και αξιολόγηση των αναδυόμενων απειλών καθώς και μεγάλη ευελιξία που επιτρέπει στους οργανισμούς να προσαρμόσουν την υπηρεσία ανάλογα με τις ανάγκες και τους πόρους που διαθέτουν.

Ηλίας Χάντζος

Η αναφορά για την κατάσταση της ιδιωτικότητας στην Ευρώπη και οι συνέπειες της προστασίας της ιδιωτικότητας για καταναλωτές και επιχειρήσεις ήταν το θέμα που ανέπτυξε ο **Ηλίας Χάντζος** - Ανώτερος Διευθυντής, Κυβερνητικές Σχέσεις, Προστασία Κρίσιμων Υποδομών και Ιδιωτικότητας στην περιοχή EMEA, για την **Symantec**. Η ανάλυση του ομιλητή για το συγκεκριμένο θέμα βασίστηκε σε μια πρωτοποριακή έρευνα που έχει διενεργήσει η Symantec, από την οποία έχουν

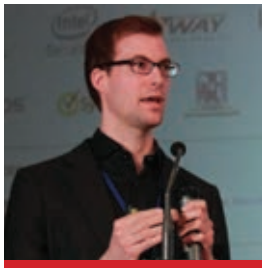
εξαχθεί σημαντικά συμπεράσματα, όπως ότι η ιδιωτικότητα συγκεντρώνει την προσοχή των καταναλωτών γιατί κατανοούν ότι τα δεδομένα έχουν αξία, οι εταιρείες τεχνολογίας δεν απολαμβάνουν την εμπιστοσύνη που είχαν στο παρελθόν και ότι η χρήση παραπληροφόρησης από τους χρήστες θέτει εν αμφιβόλω επιχειρηματικά μοντέλα που βασίζονται στην επεξεργασία πληροφοριών, ενώ ο καταναλωτής επιλέγει πλέον με κριτήριο και την ιδιωτικότητα. Ο ομιλητής τόνισε χαρακτηριστικά ότι η συζήτηση για την ιδιωτικότητα και τον ρόλο του κράτους έχει μόλις αρχίσει.


Δημήτρης Πατσός

Σε ένα άκρως επίκαιρο ζήτημα που θα μας απασχολεί συνέχεια, όπως αυτό της ασφάλειας στο mobile και το cloud επικεντρώθηκε κυρίως η παρουσίαση του **Δημήτρη Πατσού** - CTO της **ADACOM**. Ο ομιλητής επισήμανε χαρακτηριστικά, ότι η ατζέντα πλέον αλλάζει και ότι η προσπάθεια δημιουργίας μιας ασφαλούς εφαρμογής - που μπορεί να μοιάζει ως μια ακροβασία αν απαιτείται να ακολουθηθούν μια σειρά από πολλά βήματα - μπορεί πλέον να υλοποιηθεί με την αγορά έτοιμων λύσεων. Σύμφωνα με τα συμπεράσματα του ομιλητή, το cloud ήρθε για να μείνει απλά απαιτείται μια σωστή αντιμετώπιση από την αρχή, ενώ η επιλογή του τι θα πάει στο cloud πρέπει να γίνει με σωστά κριτήρια. Επίσης τόνισε ότι η ασφάλεια στο cloud μπορεί να οδηγήσει σε σημαντικές οικονομίες κλίμακας και ενίσχυση της επιχειρηματικής αποδοτικής λειτουργίας, ενώ το compliance πλέον εξελίσσεται σε ένα υποπροϊόν.


Νίκος Μουρτζίνος

Την σημασία του Threat-Centric Security που αποτελεί μια εντελώς νέα αρχιτεκτονική ασφάλειας εστιασμένη στις απειλές, ανέλυσε στη συνέχεια ο **Νίκος Μουρτζίνος**, Product Sales Specialist, **Cisco** Global Security Organization. Η νέα αυτή πρόταση προήλθε από το γεγονός ότι οι παραδοσιακές μέθοδοι που εστίαζαν στην περίμετρο δεν μπορούν πλέον να μας βοηθήσουν μιας και όλοι πλέον θέλουμε να δουλεύουμε από παντού και από οποιαδήποτε συσκευή, ενώ το δυναμικό τοπίο των απειλών έχει αλλάξει δραματικά. Όπως χαρακτηριστικά επισήμανε ο ομιλητής «δεν μπορείς να προστατέψεις κάτι που δεν γνωρίζεις ». Έτσι η προσέγγιση Threat-Centric Security, έχει ως θεμελιώδη λίθο το "superior network visibility" που επιτρέπει πλήρη ορατότητα κάθε υποδομής, αυτοματοποιημένα και σε κάθε χρονική στιγμή.


Jorn Lutters

Την ανάγκη επανασχεδιασμού της στρατηγικής ασφάλειας στο νέο περιβάλλον απειλών με την υποστήριξη σύγχρονων λύσεων, ανέδειξε ο **Jorn Lutters** - Pre-sales engineer της εταιρίας **Sophos** που ήταν καλεσμένος της εταιρίας **NSS**. Ο ομιλητής αναφέρθηκε στον επαγγελματισμό που διέπει πλέον τους ψηφιακούς εγκληματίες μέσα από συγκεκριμένα παραδείγματα και επισήμανε ταυτόχρονα ορισμένες σοβαρές δυσλειτουργίες σε συμβατικές μεθόδους ασφάλειας όπως είναι η πολυπλοκότητα, παρουσιάζοντας στη συνέχεια την οπτική της Sophos που δίνει ιδιαίτερη βαρύτητα στην απλότητα των λύσεων ψηφιακής ασφάλειας, μέσα από ολοκληρωμένες προτάσεις εύκολης διαχείρισης που επικαιροποιούνται συνεχώς και προσαρμόζονται ευέλικτα στις ανάγκες του κάθε οργανισμού.

Πάνος Δημητρίου

Κλείνοντας την 1η ενότητα του συνεδρίου, ο **Πάνος Δημητρίου** - CTO της **ENCODE** –παρουσίασε την προσέγγιση του "Continuous Cyber Situational Awareness" για την αντιμετώπιση των σύγχρονων στοχευμένων κυβερνοεπιθέσεων. Ο ομιλητής, τόνισε ότι τα περιστατικά επιθέσεων που βλέπουν το φως της δημοσιότητας είναι μόνο η κορυφή του παγόβουνου μιας και καθημερινά συμβαίνουν επιθέσεις με σημαντικές επιπτώσεις. Η προσέγγιση Continuous Cyber Situational Awareness, έχει τη δυνατότητα να πετύχει μεγαλύτερη αποτελεσματικότητα στην αντιμετώπιση αυτών των επιθέσεων, εντοπίζοντας την ύποπτη δραστηριότητα με «χειρουργική διερεύνηση» με μικρότερο κόστος και σε λιγότερο χρονικό διάστημα υλοποίησης από τις συμβατικές μεθόδους.

2η ενότητα

How to Be Proactive

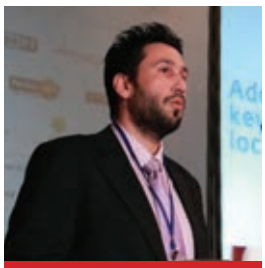
Αλέξανδρος Ντέτσικας, Παναγιώτης Καλαντζής

Η 2η ενότητα του συνεδρίου ξεκίνησε με την παρουσίαση των **Αλέξανδρου Ντέτσικα** και **Παναγιώτη Καλαντζή** - InfoSec Consultant Networking Solutions της **Space Hellas** – οι οποίοι ανέδειξαν μια proactive προσέγγιση ασφάλειας στα πλαίσια μιας έξυπνης στρατηγικής προστασίας των δεδομένων που βασίζεται στην ενοποίηση των πόρων της πληροφοριακής υποδομής ως σημεία προστασίας, στη συνεργασία των υπηρεσιών και υποδομών για την αντιμετώπιση απειλών καθώς και σε αυτοματοποιημένες τεχνολογίες για την αποτροπή των κινδύνων. Περιέγραψαν επίσης, την ολιστική προσέγγιση που υιοθετεί η Space Hellas και τα σημαντική οφέλη που προκύπτουν προς την κατεύθυνση της ασφάλειας, της βέλτιστης διαχείρισης ρίσκου και της μείωσης του κόστους και πολυπλοκότητας των διαδικασιών.

Δρ. Κωνσταντίνος Ελευθεριάνος

Εκπροσωπώντας τον **ΟΤΕ** και συγκεκριμένα το τμήμα Enterprise & Business Customers, ως Business Development Manager Marketing, ο Δρ. **Κωνσταντίνος Ελευθεριάνος** τόνισε κατά την παρουσίαση του στο συνέδριο, ότι οι παραδοσιακές μέθοδοι IT security δεν επαρκούν πλέον και επίσης επισήμανε η ασφάλεια εξελίσσεται σε ένα big data ζήτημα. Για αυτό και στον ΟΤΕ, έχουν αναπτύξει Managed Security Services που προσφέρουν πολλά πλεονεκτήματα με σημαντικότερο όλων τη δυνατότητα απόλυτης προσαρμογής των υπηρεσιών αυτών στις ανάγκες του κάθε οργανισμού. Ο ομιλητής, ενημέρωσε επίσης τους συνέδρους για την πλατφόρμα προστασίας από DDoS επιθέσεις που προσφέρει ο ΟΤΕ και παράλληλα παρουσίασε 3 case studies που αποδεικνύουν την αποτελεσματικότητα ασφάλειας που παρέχουν οι λύσεις του Οργανισμού.

Στη συνέχεια, ο **Γιάννης Παυλίδης** - Presales & Tech Support Engineer της **ESET Hellas** – αναφέρθηκε με αναλυτικά στοιχεία στα security incident και στα data breach των τελευταίων ετών καθώς και στις οικονομικές και άλλες επιπτώσεις που υπήρξαν από αυτά. Από τα όσα ανέφερε ο ομιλητής, ξεχώρισε η διαπίστωση ότι κορυφαία μέθοδο data breach για το 2014 ήταν η υποκλοπή κωδικών, καθώς και το ότι ο χρόνος για τη διαπίστωση ενός breach μπορεί να φθάσει να είναι ακόμα και αρκετοί μήνες. Επίσης, παρουσίασε το ESET Secure Authentication που προσφέρει πολλαπλά επίπεδα προστασίας με βάση two-factor authentication τεχνική, όπου σε αντίθεση με τον τυπικό έλεγχο ταυτότητας με κωδικό πρόσβασης χρησιμοποιεί δυο παράγοντες (δηλαδή κάτι που ο χρήστης γνωρίζει και κάτι που ο χρήστες κατέχει) αλλά και one-time password που υποστηρίζει διαφορετικούς κωδικούς κάθε φορά όπου μετά από κάθε χρήση τους «καίγονται».



Γιάννης Παυλίδης

Mehdi Bouzoubaa

Το πώς μπορούμε να εντοπίσουμε κακόβουλο λογισμικό σε κάθε συσκευή που εντάσσεται στο πληροφοριακό σύστημα ενός οργανισμούς, ήταν το θέμα που ανέπτυξε ο **Mehdi Bouzoubaa** - Sales Director EMEA της εταιρίας **Damballa**, που συμμετείχε στο συνέδριο ως καλεσμένος της εταιρίας **Avad**. Ο ομιλητής, παρουσίασε τη λύση FailSafe της Damballa, που σχεδιάστηκε να εντοπίζει με το βέλτιστο δυνατό τρόπο "μολυσμένα αρχεία" τα οποία επιβεβαιωμένα συνιστούν απειλή, καθώς και να κατηγοριοποιεί με προτεραιότητα και ανά επικινδυνότητα τα αρχεία αυτά. Το χαρακτηριστικό στοιχείο, που κάνει τις λύσεις της Damballa να ξεχωρίζουν, είναι η δυνατότητα απόλυτης ορατότητας μέσα στο οικοσύστημα των απειλών, η προηγμένη ικανότητα εντοπισμού απειλών μέσα από το Threat Discovery Center αλλά και η δυνατότητα εξαγωγής προβλέψεων και analytics σε σχέση με την ασφάλεια.

Ο επόμενος ομιλητής **Ανδρέας Αθανασούλιας** - Principal Security Consultant της **Uni Systems** – παρουσίασε ένα νέο μοντέλο ασφάλειας που προσφέρει η εταιρία που εκπροσωπεί και το οποίο βασίζεται σε μεγάλο βαθμό στην ελεγχόμενη και με ασφάλεια πρόσβαση των χρηστών (εσωτερι-


Ανδρέας Αθανασούλιας

κών και εξωτερικών) στους διαθέσιμους πόρους της εταιρίας μέσω μηχανισμών αναγνώρισης, αυθεντικοποιήσης και εξουσιοδότησης. Ο ομιλητής, ανάφερε μεταξύ άλλων οτι οι τεχνολογίες ασφάλειας πρέπει να είναι "proactive" υποστηρίζοντας risk assessment, two factor authentication, network & application access controls, DLP και APT Detection καθώς επίσης και reactive υποστηρίζοντας μεταξύ άλλων, Security Information & Event Management, κρυπτογράφηση APT Remediation.


Paolo Florian

Στην επόμενη παρουσίαση ο **Paolo Florian** - Sales Engineer της **McAfee**, Part of Intel Security – ως καλεσμένος της εταιρίας IT WAY είχε την ευκαιρία να ενημερώσει τους συνέδρους για την ενοποιημένη πλατφόρμα της Mcafee που επιτυγχάνει τη διασύνδεση μεταξύ μηχανισμών security risk management, threat intelligence, analytics και contest orchestration, προστατεύοντας έτσι ταυτόχρονα το περιεχόμενο, το δίκτυο και τα endpoint μιας επιχείρησης. Η ενοποιημένη αυτή αρχιτεκτονική νέας γενιάς προσφέρει υψηλή αποτελεσματικότητα ασφάλειας και διευκολύνει στη σωστή λήψη αποφάσεων. Διαθέτει επίσης ισχυρά εργαλεία προστασίας στα endpoint και τα δίκτυα και διακρίνεται για την απλοποίηση στη διαχείριση ασφάλειας, μειώνοντας σημαντικά τα λειτουργικά κόστη.


Αντώνης Καλοχριστιανάκης

Στο ιδιαίτερα κρίσιμο ζήτημα της αντιμετώπισης των προηγμένων απειλών που είναι γνωστές ως APTs αναφέρθηκε στη παρουσίαση του ο **Αντώνης Καλοχριστιανάκης** - Εμπορικός Διευθυντής της **Digital Sima**. Ο ομιλητής επισήμανε χαρακτηριστικά ότι το Antivirus δεν επαρκή πλέον για να καλύψει τις ανάγκες και ότι σύμφωνα με έρευνες σχεδόν το 88% του malware μεταμορφώνεται ώστε να παρακάμψει τα signature-based antivirus. Επίσης σήμερα, το κοινό κακόβουλο malware χρησιμοποιεί τις ίδιες προηγμένες τεχνικές APTs που χρησιμοποιούνται για επιθέσεις σε κρίσιμες υποδομές και πλέον κάθε οργανισμός κινδυνεύει από advanced threats! Η Digital Sima συνεργάζεται με την εταιρία WatchGuard παρέχοντας λύσεις που εντοπίζουν και αντιμετωπίζουν αποτελεσματικά τις προηγμένες επιθέσεις τύπου APTs


Angelo Gentili

Στη συνέχεια, ο **Angelo Gentili** - Business Development Manager της **PartnerNet** – παρουσίασε την οπτική της Cyberoam σχετικά με την ασφάλεια στο επιχειρηματικό περιβάλλον, αναπτύσσοντας μια προσέγγιση που βασίζεται σε ενοποιημένους και αυτοματοποιημένους μηχανισμούς προστασίας, καθώς επίσης και σε αναβαθμισμένες λειτουργίες παρακολούθησης και εξαγωγής αναφορών που επιτρέπουν την εναρμόνιση ασφάλειας, παραγωγικότητας και συμμόρφωσης. Μεταξύ άλλων, η Cyberoam προτείνει ένα μοντέλο που κατά βάση αναγνωρίζει και κατηγοριοποιεί τα κρίσιμα δεδομένα, τους διαθέσιμους πόρους, τα πιθανά ευάλωτα σημεία και τις απειλές.


Peter Galvin


Ανδρέας Λάλος

Μια εναλλακτική προσέγγιση στο θέμα της ασφαλούς online επικοινωνίας χρησιμοποιώντας ψηφιακά πιστοποιητικά που μειώνουν το κόστος, παρουσίασε ο **Ανδρέας Λάλος**, Professional Services Director της εταιρίας **BESECURE** και ο συνεργάτης του **Peter Galvin**, Technical Sales Consultant της **ENTRUST** Certificate Services. Οι λύσεις της Entrust όπως μας ανέφεραν οι δυο ομιλητές, προστατεύουν τις ταυτότητες παρέχοντας αυθεντικοποιήση για πολλές διεργασίες, κυρίως οικονομικές αλλά και πολλές άλλες, σε ανθρώπους, εφαρμογές, φορητές συσκευές, μηχανές και

servers. Η απλότητα και η ταχύτητα δημιουργίας των ψηφιακών πιστοποιητικών από τους administrators είναι ιδιαίτερα σημαντική, ενώ ιδιαίτερα εύκολη είναι και η διαχείριση όλων των πιστοποιητικών από το χρήστη.

Γιάννης Γκιόκας

Κλείνοντας τη 2η ενότητα ο **Γιάννης Γκιόκας**, CEO της **Crypteia Networks** ανέδειξε μεταξύ άλλων την ανάγκη για την υιοθέτηση του "Threat Intelligence" τονίζοντας ότι η έννοια του Security as a Service πρέπει να λειτουργεί σε πραγματικό χρόνο και να υποστηρίζει ευφυείς δράσεις. Ο ομιλητής υποστήριξε ότι η τάση του Security as a Service έχει αλλάξει σε μεγάλο βαθμό τον τρόπο με τον οποίο ελέγχονται τα πληροφοριακά συστήματα σήμερα. Η δημιουργία ενός ασφαλούς οικοσυστήματος όπως αυτό που μπορεί να υλοποιεί η Crypteia Networks έχει τη δυνατότητα να συλλέγει στοιχεία για απειλές από 23 διαφορετικές πηγές ταυτόχρονα, να επικαιροποιεί σε real-time τις database, να διατηρεί ιστορικά στοιχεία και να αξιολογεί κάθε νέο δεδομένο.

3η ενότητα

Building a Smart Protection Strategy

Bernard Montel

Στην εναρκτήρια ομιλία της 3ης ενότητας ο **Bernard Montel** - Regional PreSales Manager της **RSA** τα προϊόντα της οποίας διανέμει στη χώρα μας η IT WAY– παρουσίασε το μοντέλο Intelligence-Driven Security της RSA. Το συγκεκριμένο μοντέλο ασφάλειας, που βασίζεται στο τρίπτυχο ορατότητα – δράση – ανάλυση, προσφέρει μια σειρά από σημαντικά πλεονεκτήματα, όπως: ο καθορισμός των βέλτιστων προτεραιοτήτων, ενεργειών και διαθέσιμων πόρων, νέες δυνατότητες που βελτιώνουν την απόδοση σε βάθος χρόνου, άμεση ανταπόκριση στις όποιες αλλαγές μπορούν να συμβούν χωρίς την ανάγκη προσθήκης νέων προϊόντων καθώς και απόλυτη ευελιξία στην αξιοποίηση νέων τεχνολογιών και δυνατοτήτων που προκύπτουν.

Ντίνος Τσαΐρης, Θεοφάνης Σακελλαρίδης

Στη συνέχεια ο **Ντίνος Τσαΐρης**, Technical Support Manager της **Dataplex** και ο **Θεοφάνης Σακελλαρίδης**, IT Manager της εταιρίας **Νέα Οδός**, παρουσίασαν ένα case study που υλοποιήθηκε πρόσφατα και αναδεικνύει το πως μπορεί να «παντρευτεί» η ασφάλεια των δεδομένων με την ασφάλεια των Ελληνικών δρόμων. Το ιδιαίτερα αυτό απαιτητικό έργο υλοποιήθηκε αξιοποιώντας λύσεις της Checkpoint. Πρόκειται για ένα έργο με πολλές ιδιαιτερότητες και οι τεχνολογικές λύσεις που εφαρμόστηκαν πέτυχαν να ενοποιήσουν τη διαχείριση της ασφάλειας, τη διαχείριση των events και τη διαχείριση των Log προς όφελος της προστασίας των δεδομένων και της ενίσχυσης της λειτουργικότητας.

Το ιδιαίτερα σημαντικό ζήτημα του Data Classification σε σχέση με την ασφάλεια ανέλυσε στην παρουσίαση του ο **Wesley Budd** - Channel Manager, της Boldon James – A Qinetiq Company. Ο ομιλητής που ήταν καλεσμένος της εταιρίας **ADACOM** έδωσε έμφαση στην ανάγκη υιοθέτησης της ταξινόμησης των δεδομένων σε κάθε προσέγγιση


Wesley Budd

ασφάλειας, μιας και ενισχύει το awareness της προστασίας και παράλληλα υποστηρίζει πιο αποτελεσματικά τις διαδικασίες αρχειοθέτησης, μειώνοντας τις απαιτήσεις αποθήκευσης και κόστους. Επίσης, ενισχύει τη συμμόρφωση με τους κανονισμούς και τα πρότυπα, ενδυναμώνει την ασφάλεια στην εξ αποστάσεως εργασία καθώς και την απομακρυσμένη συνεργασία, ενώ παράλληλα διατηρεί σε υψηλά επίπεδα την επιχειρηματική βιωσιμότητα.


Αγγελική Φιλιπποπούλου

Επόμενη ομιλήτρια ήταν η **Αγγελική Φιλιπποπούλου** - Regional Sales Manager στην Ελλάδα για την **Fortinet** – η οποία ανέλυσε τα Managed Security Services που έχει αναπτύξει η Fortinet και που καλύπτουν αποδοτικά τις σύγχρονες προκλήσεις ασφάλειας, προσφέροντας σε μεγάλο βαθμό σημαντική εξοικονόμηση κόστους. Οι συγκεκριμένες λύσεις της Fortinet, που έχουν κατακτήσει πολλές διακρίσεις παγκοσμίως, ξεχωρίζουν για τη μεγάλη ταχύτητα απόδοσης και το υψηλό επίπεδο ασφάλειας ως απόρροια της μεγάλης εξειδικευμένης ομάδας έρευνας που εντοπίζουν άμεσα τις αναδυόμενες απειλές αλλά και των πολλών συνεργασιών που έχει αναπτύξει η εταιρία.

Emmanuel Roeseler Rivera

Την οπτική της IBM για τη διαχείριση ρίσκου και τη ψηφιακή ασφάλεια παρουσίασε στη συνέχεια ο **Emmanuel Roeseler Rivera** - Security Systems IMT Leader της **IBM** – επιβεβαιώνοντας την κοινή πεποίθηση ότι οι επιθέσεις είναι πλέον ιδιαίτερα στοχευμένες και οι επιτιθέμενοι περισσότερο οργανωμένοι, αφού μεταξύ άλλων αξιοποιούν ακόμα και στρατηγικές Business Intelligence. Στη συνέχεια, ο ομιλητής ανέδειξε την ανάγκη για ένα διαφορετικό τρόπο σκέψης σχετικά με τα θέματα ασφάλειας που θα βασίζεται στο τρίπτυχο: εντοπισμός – ανταπόκριση – αποτροπή, κάτι που η IBM εφαρμόζει, συμβουλεύοντας τους οργανισμούς να δίνουν προτεραιότητα και να εστιάζουν κυρίως στα πιο κρίσιμα δεδομένα τους αποκτώντας πλήρη ορατότητα και έλεγχο στο cloud και στο mobility.


Yaron Bielous

Στη συνέχεια ο **Yaron Bielous** - Head of Cloud Solutions and Enterprise Business της **Allot** που συνεργάζεται στη χώρα μας με την ADACOM– εστίασε την παρουσίαση του σε λύσεις ασφάλειας στο cloud που διαθέτει η εταιρία και προσφέρουν σημαντικά πλεονεκτήματα όπως λειτουργίες web analytics με κρυπτογράφηση, ισχυρό και proactive web intelligence με μεγάλη και λεπτομερή ανάλυση καθώς και ισχυρή DDoS προστασία. Ο ομιλητής αναφέρθηκε αναλυτικά στα οφέλη που προκύπτουν από την αξιοποίηση λύσεων cyber security της Allot όπως το φιλτράρισμα περιεχομένου για παράνομες διαδικτυακές υπηρεσίες, anti-malware προστασία αλλά και ισχυρή κρυπτογράφηση.


Παναγιώτης Πιέρρος


Μιχάλης Μίγγος

Μια ιδιαίτερα δυναμική παρουσίαση είχαμε την ευκαιρία να παρακολουθήσουμε στη συνέχεια από τον **Παναγιώτη Πιέρρο**, Managing Director και **Μιχάλη Μίγγο**, Technical Director της εταιρίας **TicTac Data Recovery**. Στην παρουσίαση των δυο εισηγητών καταγράφηκαν κάποιες πραγματικές ιστορίες απώλειας δεδομένων που αναδεικνύουν τις επιπτώσεις που υπάρχουν σε ανάλογα περιστατικά. Επίσης οι δυο ομιλητές επισήμαναν κάποιους σημαντικούς κανόνες που πρέπει να τηρούνται έτσι ώστε να προστατέψουμε την προσωπική και εταιρική μας ψηφιακή περιουσία. Ξεχωρίσαμε μεταξύ άλλων τη διαπίστωση ότι το 65% των μέσων αποθήκευσης αποσύρονται χωρίς να ληφθούν μέτρα ασφαλείας, ενώ τόνισαν χα-

ρακτηριστικά... ότι μπορούμε να προβλέψουμε πολλά όσον αφορά την απώλεια ή την αλλοίωση των δεδομένων αλλά δύσκολα προβλέπουμε τον παράγοντα άνθρωπο!

Νίκος Γεωργόπουλος

Μια εναλλακτική προσέγγιση που αφορούσε το "Cyber Insurance ως εργαλείο διαχείρισης κινδύνου" παρουσίασε ο **Νίκος Γεωργόπουλος** - Cyber Risks Advisor. Από τα πολλά ενδιαφέροντα θέματα που ανέπτυξε ο ομιλητής, ξεχωρίσαμε την αναφορά του στο γεγονός ότι τα δεδομένα υγείας θεωρούνται τα πλέον πολύτιμα από την ασφαλιστική αγορά. Επίσης ο ομιλητής ανέφερε ότι οι ζημίες από την απώλεια δεδομένων προέρχονται κατά 30 % από τον ανθρώπινο παράγοντα, από κακόβουλες ενέργειες και επιθέσεις το 41% και από συστήματα και διαδικασίες το 29 %. Η ασφάλιση των οικονομικών συνεπειών μια εταιρίας σε περίπτωση παραβίασης συστημάτων και απώλειας δεδομένων δεν είναι μια απλή κάλυψη και απαιτεί εξειδικευμένους ασφαλιστικούς διαμεσολαβητές τόνισε χαρακτηριστικά ο ομιλητής.

4η ενότητα

The Hacking Games

Mehmet Dagdevirenturk

Η 4η ενότητα του συνεδρίου ξεκίνησε με την παρουσίαση του καλεσμένου της εταιρίας CySoft, **Mehmet Dagdevirenturk** - Channel Development Technical Manager της **Trend Micro** – που μεταξύ άλλων ανέπτυξε μέσα από συγκεκριμένα παραδείγματα τις τεχνικές που ακολουθούνται στις στοχευμένες επιθέσεις σε πρόσωπα και οργανισμούς, μέσω ηλεκτρονικού ταχυδρομείου αξιοποιώντας μεθόδους social engineering. Επίσης, ενημέρωσε τους συνέδρους για τις λύσεις που προσφέρει η Trend Micro για την αντιμετώπιση αυτών των επιθέσεων και κυρίως για τη λύση Deep Discovery που είναι ειδικά σχεδιασμένη για να εντοπίζει και να μπλοκάρει emails με κακόβουλο περιεχόμενο.

Νικήτας Κλαδάκης

Στη συνέχεια ο **Νικήτας Κλαδάκης** - Information Security Manager, **NetBull** – αναφέρθηκε στις προηγμένες επιθέσεις τύπου APT και πως αυτές μπορούν να αντιμετωπιστούν. Συγκεκριμένα, παρουσίασε μια ολιστική 3D στρατηγική ασφάλειας που υλοποιείται από την εταιρία μέσα από την αρχιτεκτονική nSA και βασίζεται σε πολιτικές και διαδικασίες, σε συστήματα ασφάλειας πληροφοριών αλλά φυσικά και στον παράγοντα άνθρωπο. Η πρόταση αυτή εξασφαλίζει 24x7 παρακολούθηση ασφάλειας και προσφέρει προστασία ενάντια σε εσωτερικές και εξωτερικές απειλές βασισμένη σε threat intelligent και σε ένα security operation center.

Ο **Νίκος Τσαγκαράκης** - CEO/Director of Security Testing Services της **Census** – ανέπτυξε αναλυτικά 3 τρόπους με τους οποίους σήμερα οι hackers επιτίθενται σε έναν οργανισμό. Ο ομιλητής τόνισε χαρακτηριστικά ότι η λογική στο τομέα της ασφάλειας είναι «ότι δεν μπορεί να φτιαχτεί κάτι από τον άνθρωπο και το οποίο να είναι τέλειο» και αυτές οι ατέλειες, είναι τα λεγόμενα bugs στο χώρο των λογισμικών και είναι αυτά που εκμεταλλεύονται οι επιτιθέμενοι προκειμένου να

Νίκος Τσαγκαράκης

εισβάλουν στον οργανισμό. Συνεπώς η αρχή που προσπαθούν να μεταδώσουν τα στελέχη της Census είναι η αλλαγή νοοτροπίας στη κατεύθυνση ότι πρέπει να αντιμετωπίσουμε τις αδυναμίες εν τη γενέσει και να βρούμε τη λύση του προβλήματος εκεί που γεννιέται.

Jason Steer

Ο επόμενος ομιλητής ήταν ο **Jason Steer** - Chief Security Strategist EMEA της εταιρίας **FireEye** που στην Ελλάδα συνεργάζεται με την IT WAY. Ο ομιλητής στα πλαίσια της παρουσίασης του, ανέδειξε τις προκλήσεις που υπάρχουν σήμερα σχετικά με τις προηγμένες επιθέσεις, τους στόχους των hackers, τους ακτιβιστές και άλλες μορφές κινδύνων, τονίζοντας χαρακτηριστικά πως οι απειλές στον κυβερνοχώρο είναι πλέον ασύρματες και χρήζουν εξειδικευμένης αντιμετώπισης με νέα εργαλεία νέες τεχνολογίες που θα εντοπίζουν έγκαιρα και αξιόπιστα τις απειλές παρέχοντας την απαραίτητη ορατότητα για την αναγνώριση και αξιολόγηση του κινδύνου.

Dr. Κωνσταντίνος Παπαπαναγιώτου

Εκπροσωπώντας το **ISACA Athens Chapter** ο Dr. **Κωνσταντίνος Παπαπαναγιώτου** παρουσίασε ένα καινούργιο παγκόσμιο πρόγραμμα του ινστιτούτου, που είναι κάτι παραπάνω από μια πιστοποίηση και προκύπτει από την ανάγκη της μετεξέλιξης της ασφάλειας πληροφοριών σε Cyber Security. Πρόκειται για το πρόγραμμα Cybersecurity Nexus (CSX) που χαρακτηρίζεται ως μια «πλατφόρμα γνώσης» και μεταξύ άλλων έχει στόχο την ενίσχυση της τεχνογνωσίας, της καθοδήγησης, των ικανοτήτων και της διασύνδεσης των ανθρώπων που ασχολούνται με το χώρο της ασφάλειας πληροφοριών.

Ο επόμενος ομιλητής, ο **Χρήστος Βεντούρης**, εκπροσώπησε τον οργανισμό **(ISC)2 Hellenic Chapter** και ανέπτυξε

Χρήστος Βεντούρης

το θέμα "The two faces of Tor: Anonymity and Crime" αναλύοντας τις θετικές αλλά και αρνητικές πλευρές του δικτύου Tor το οποίο χρησιμοποιούν πάρα πολλοί επαγγελματίες και όχι μόνο, προκειμένου να διατηρήσουνε ορισμένες φορές την ανωνυμία τους στην επικοινωνία ή να προσπεράσουν τυχόν διαδικασίες λογοκρισίας στον οργανισμό ή στην χώρα που βρίσκονται.

Κωνσταντίνος Φίλης

Η 4η ενότητα και το συνέδριο έκλεισε με μια πολύ ενδιαφέρουσα παρουσίαση που έκανε ο **Κωνσταντίνος Φίλης** - R&D Senior Engineer της COSMOTE, και αφορούσε το ερευνητικό έργο NEMESYS που συμμετέχει η COSMOTE με άλλους φορείς και σχετίζεται με καινοτόμες τεχνικές προστασίας συσκευών και δικτύων κινητών επικοινωνιών από κακόβουλες επιθέσεις. Το συγκεκριμένο ερευνητικό έργο που ολοκληρώνεται σε 6 μήνες από τώρα είναι ιδιαίτερα σημαντικό μιας και παρατηρείται μια αυξητική τάση στη μόλυνση των φορητών συσκευών επικοινωνιών που χρήζει μια αποτελεσματικότερης αντιμετώπισης.

Τις περισσότερες παρουσιάσεις μπορείτε να τις δείτε στο site του συνεδρίου ***www.infocomsecurity.gr***

Οι Χορηγοί του Infocom Security 2015

Ιδιαίτερα σημαντική για την επιτυχία του συνεδρίου ήταν η υποστήριξη των χορηγών – εταιρειών, στελέχη των οποίων είχαν τη δυνατότητα στον εκθεσιακό χώρο του συνεδρίου να συζητήσουν με πολλούς από τους συνέδρους και να τους ενημερώσουν για τις δραστηριότητες που αναπτύσσουν.

Μεγάλος Χορηγός - Encode

Πλατινένιος Χορηγός - Checkpoint

Χρυσός Χορηγός - Adacom με Symantec, Allot, Boldon James

Χρυσός Χορηγός – Cisco

Χρυσός Χορηγός – Odyssey

Χρυσός Χορηγός – OTE-Cosmote

Χρυσός Χορηγός – Space Hellas

Αργυρός Χορηγός – Crypteia Networks

Census

Cysoft

ITWay & RSA

ITWay & McAfee

FireEye

Digital Sima

ESET Hellas

Ideal & Fortinet

Lexis & Fortinet

Netizen Security

Netbull

TICTAC

NSS & Sophos

PartnerNet

Unisystems

Avad & Damballa

PremiumIT

T&K - Avira

Εξέλιξη