HOW s@fe is your Business

Συνέδριο “How S@fe is your Business”

Σημαντικότερα ευρήματα

Με αφορμή την επιτυχή διοργάνωση του συνεδρίου “How S@fe is your Business” το οποίο έλαβε χώρα στο Συνεδριακό Κέντρο Φιλοξένια στις 2 Φεβρουαρίου 2017, το Κυπριακό Εμπορικό και Βιομηχανικό Επιμελητήριο (ΚΕΒΕ) και το Ινστιτούτο Νευροεπιστήμης και Τεχνολογίας Κύπρου (CNTI), ως συνδιοργανωτές του συνεδρίου, θα θέλαμε να ευχαριστήσουμε όλους όσους παραβρέθηκαν και συμμετείχαν στις ενδιαφέρουσες τοποθετήσεις που αναπτύχθηκαν από τους ομιλητές στην προσπάθεια καταγραφής της υπάρχουσας κατάστασης αναφορικά με την ασφάλεια των επιχειρήσεων στη ψηφιακή εποχή.

Το συνέδριο στέφθηκε με απόλυτη επιτυχία καθώς κατόρθωσε να συγκεντρώσει μία πολυτομεακή ομάδα εμπειρογνωμόνων με εμπειρία και γνώση στον ευρύτερο τομέα της ασφάλειας πληροφοριών οι οποίοι επιχείρησαν να σκιαγραφήσουν τους ψηφιακούς κινδύνους στους οποίους εκτίθενται καθημερινά οι επιχειρήσεις. Μέσα από τις παρουσιάσεις προτάθηκαν λύσεις οι οποίες θα συνεισφέρουν στην αύξηση του επιπέδου ασφαλείας των δεδομένων της επιχείρησης σε μία εποχή όπου τουλάχιστον το 43% των Μικρομεσαίων Επιχειρήσεων στοχοποιείται από κυβερνοεπιθέσεις.

Παρακάτω, καταγράφονται τα σημαντικότερα πορίσματα από το συνέδριο

- Η αξιοποίηση της ψηφιακής τεχνολογίας αποτελεί αναπόσπαστο στοιχείο για μία επιχείρηση η οποία προσβλέπει στη βιωσιμότητά της και την αύξηση του κέρδους της
- Οι δυνατότητες που παρέχει η ψηφιακή τεχνολογία στις επιχειρήσεις συνοδεύονται από πολλαπλούς και διαρκώς εξελίξιμους κινδύνους που καθιστούν τις επιχειρήσεις ευάλωτες
- Η λίστα των πιθανών κινδύνων και απειλών είναι ανεξάντλητη και περιλαμβάνει μεταξύ άλλων: Ransomware, Cryptolockers, Denial-of-service attacks (DoS), Phishing scams, Spam
- Η κυβερνοαπειλή μπορεί να προέρχεται από εξωτερικές πηγές (π.χ. χάκερς) ή ακόμη και από εργαζόμενους εντός της ίδιας της επιχείρησης
- Τα κίνητρα των κυβερνοεπιθέσεων ποικίλουν όπως επίσης και το είδος των πληροφοριών που επιδιώκει ο δράστης να προσπελάσει: πληροφορίες σχετικά με αναδυόμενες τεχνολογίες, τραπεζικές κάρτες, επιχειρηματικές συμφωνίες, προσωπικά δεδομένα πελατών και συνεργατών
- Η άμυνα των επιχειρήσεων απέναντι στις διαρκώς ανελισσόμενες ψηφιακές απειλές περιλαμβάνει μεταξύ άλλων: στρατηγική για την προστασία των πληροφοριών, εκπαίδευση και ευαισθητοποίηση των υπαλλήλων, πρότυπα ασφαλείας, ανεξάρτητο εσωτερικό τμήμα ασφάλειας κεντρικών συστημάτων πληροφορικής, εγκατάσταση τεχνικού εξοπλισμού (π.χ. antivirus, breach detection systems, access control systems), αγορά υπηρεσιών από επιχειρήσεις εξειδικευμένες στην παροχή λύσεων κυβερνοασφάλειας

CYPRUS CHAMBER OF COMMERCE AND INDUSTRY

CNTI

PLATINUM SPONSOR

ODYSSEY

pwc

HELLENIC BANK

GOLD SPONSOR

cyta

MEDIA SPONSOR

ΚΥΠΕ CNA

HOW s@fe is your Business

• Η Διεύθυνση των Επιχειρήσεων πρέπει να ενημερωθεί για τις επιπτώσεις από τις κυβερνοεπιθέσεις και ειδικότερα για τις πιθανές συνέπειες από μία επίθεση εντός της επιχείρησης έτσι ώστε να ευαισθητοποιηθούν για την ανάγκη λήψης αποφάσεων για προστασία των πληροφοριών της

• Οι πιθανές επιπτώσεις από μία κυβερνοεπίθεση περιλαμβάνουν μεταξύ άλλων: οικονομικές απώλειες, απώλεια κερδών, υποκλοπή προσωπικών δεδομένων πελατών, υποκλοπή εμπιστευτικών πληροφοριών που πωλούνται σε ανταγωνιστές, ζημιά στη δημόσια εικόνα και την υπόληψη της επιχείρησης

• Οι πληροφορίες που υποκλέπτονται συχνά πωλούνται μέσω του DarkWeb σε δυνητικούς ενδιαφερόμενους

• Οι κυβερνοεπιθέσεις έχουν ως στόχο την απόκτηση εμπιστευτικών πληροφοριών. Όλες οι επιχειρήσεις διαθέτουν πληροφορίες. Συνεπώς, όλοι οι επιχειρήσεις είναι δυνητικά θύματα κυβερνοεπίθεσης

• Είναι καθόλα δυνατός ο μετριασμός των κινδύνων και η αποτελεσματική διαχείριση / αντιμετώπιση όλων των απειλών νοούμενο ότι η Επιχείρηση λαμβάνει τα κατάλληλα μέτρα

• Η επιχείρηση οφείλει να μελετήσει και να επικεντρωθεί σε εκείνες τις απειλές που παρουσιάζουν τη μεγαλύτερη συχνότητα και πιθανότητα εκδήλωσης και συνάμα τον μεγαλύτερο αντίκτυπο στην επιχείρηση

• Οι τεχνικές λύσεις δεν είναι επαρκείς για την ασφάλεια των δεδομένων μίας επιχείρησης. Πρέπει να συνοδεύονται από την εκπαίδευση των εργαζομένων σε ζητήματα κυβερνοασφάλειας

• Η εκπαίδευση των εργαζομένων θα πρέπει να έχει δυναμικό και όχι στατικό χαρακτήρα, να προσφέρεται ανά τακτά διαστήματα και να προετοιμάζει τους εργαζόμενους στην αναγνώριση, εντοπισμό, αποφυγή και διαχείριση περιστατικών κυβερνοεπίθεσης

• Η δημιουργία κουλτούρας κυβερνοασφάλειας για όλους τους εργαζόμενους εντός της επιχείρησης συγκαταλέγεται στις αναγκαίες ενέργειες στις οποίες πρέπει να προβεί μία επιχείρηση για την προστασία των δεδομένων της

• Η Πληροφορική (IT) ΔΕΝ ταυτίζεται με την Ασφάλεια Δικτύων και Πληροφοριών (Information Security) όπως ακριβώς η ασφάλεια της επιχείρησης ΔΕΝ εξασφαλίζεται μόνο από ένα ειδικό στην Πληροφορική

• Ο άνθρωπος είναι ο πλέον αδύνατος κρίκος στην αλυσίδα της κυβερνοασφάλειας

• Είναι πολύ πιο εύκολο να ξεγελάσεις ένα εργαζόμενο για να σου εξασφαλίσει πρόσβαση σε εμπιστευτικές πληροφορίες από το να προσπαθήσεις να παρεισφρήσεις στο σύστημα αξιοποιώντας εξειδικευμένες γνώσεις υπολογιστών

Ιδιαίτερες ευχαριστίες απευθύνονται στους χορηγούς του Συνεδρίου, Ελληνική Τράπεζα, PwC και εταιρεία Odyssey καθώς επίσης στη CYTA αλλά και στο ΚΥΠΕ.

CYPRUS CHAMBER OF COMMERCE AND INDUSTRY

CNTI

PLATINUM SPONSOR

ODYSSEY

pwc

HELLENIC BANK

GOLD SPONSOR

cyta

MEDIA SPONSOR

ΚΥΠΕ CNA