NetFAX

Συνεργασία Uni Systems - My Buddy για ανάπτυξη εφαρμογών Τεχνητής Νοημοσύνης

Η ανάπτυξη εφαρμογών Τεχνητής Νοημοσύνης (ΤΝ) βρίσκεται στο επίκεντρο της συνεργασίας της Uni Systems με την My Buddy, την εταιρεία ανάπτυξης της ομώνυμης καινοτόμας πλατφόρμας που προσφέρει μια νέα προσέγγιση στην ανάπτυξη εφαρμογών μέσω χιλιάδων εύκολων και ευέλικτων ενσωματώσεων. Στόχος της συνεργασίας των Uni Systems και My Buddy είναι η ανάπτυξη εφαρμογών και ολοκληρωμένων λύσεων ΤΝ με συνδυασμό χιλιάδων μοντέλων, βάσεων δεδομένων τύπου vector και περισσότερων από 250 προενσωματωμένων εργαλείων. Οι λύσεις που αφορούν στη μετατροπή φωνής σε κείμενο, οι έξυπνοι βοηθοί και η προηγμένη ανάλυση αγορών αποτελούν τη βάση της δραστηριότητας παρέχοντας τη δυνατότητα στις επιχειρήσεις ευρέως φάσματος της αγοράς να εκμεταλλευτούν τα οφέλη τεχνολογιών όπως τα Large Language Models (LLMs), Vision-Language Models (VLMs) και Automatic Speech Recognition (ASR). Να σημειωθεί ότι αν και οι εφαρμογές αξιοποιούν πλούτο δεδομένων, διασφαλίζεται απολύτως η συμμόρφωσή τους με τα πρότυπα SOC 2 και GDPR. Η αυτοματοποίηση των διαδικασιών με ταυτόχρονη μείωση λειτουργικών εξόδων, η καλύτερη κατανόηση των συμπεριφορών και των αναγκών των πελατών που οδηγούν στη βελτιστοποίηση των προσφερόμενων υπηρεσιών, και κατ' επέκταση στη βελτίωση της εμπειρίας χρήσης και εξυπηρέτησης, συγκαταλέγονται στα κύρια οφέλη των εφαρμογών ΤΝ που σχεδιάζουν οι δύο εταιρείες.

Η ΕΥ ανέλαβε το έργο για το ΠΣ της Ανεξάρτητης Αρχής Πιστολιπτικής Ικανότητας

Η ΕΥ ανέλαβε την υλοποίηση του έργου με αντικείμενο την «Ανάπτυξη Πληροφοριακού Συστήματος της Ανεξάρτητης Αρχής Πιστολιπτικής Αξιολόγησης». Η αξία της σύμβασης που υπεγράφη στις 18 Οκτωβρίου μεταξύ του αναδόχου και της Κοινωνίας της Πληροφορίας ανέρχεται στα 2,24 εκατ. ευρώ συμπεριλαμβανομένου του ΦΠΑ. Αντικείμενο του έργου είναι η ανάπτυξη ενός πληροφοριακού συστήματος το οποίο θα περιλαμβάνει μια κεντρική βάση δεδομένων οικονομικής συμπεριφοράς από φορείς του δημόσιου τομέα και μια ενιαία κλίμακα αξιολόγησης πιστολιπτικής ικανότητας για την παραγωγή και χορήγηση πιστολιπτικής βαθμολόγησης στα φυσικά και νομικά πρόσωπα σε σχέση με οφειλές τους προς το Δημόσιο. Το πληροφοριακό σύστημα θα διαλειτουργεί με άλλα ηλεκτρονικά συστήματα (δημόσια και ιδιωτικά, όπως Τειρεσίας κ.α), με σκοπό την ανταλλαγή βαθμολογιών πιστολιπτικής ικανότητας και τη δημιουργία ενιαίας βαθμολόγησης για την αξιολόγηση της πιστολιπτικής ικανότητας φυσικών και νομικών προσώπων.

SPACE HELLAS: ΕΚΤΗ ΤΙΜΗΤΙΚΗ ΥΠΟΤΡΟΦΙΑ «ΔΗΜΗΤΡΗΣ ΜΑΝΩΛΟΠΟΥΛΟΣ»

Η Space Hellas ανακοίνωσε την έναρξη του 6ου ετήσιου προγράμματος των τιμητικών υποτροφιών «Δημήτρης Μανωλόπουλος», εις μνήμην του ιδρυτή της. Οι υποτροφίες είναι δύο, έξι χιλιάδες ευρώ η κάθε μία και θα απονεμηθούν σε αποφοίτους δημόσιων ανώτατων εκπαιδευτικών ιδρυμάτων της Ελλάδας ή ισότιμων ανώτατων εκπαιδευτικών ιδρυμάτων του εξωτερικού, οι οποίοι θα εγγραφούν το ακαδημαϊκό έτος 2024-2025, σε ελληνικά δημόσια Πανεπιστήμια, για μεταπτυχιακές ή διδακτορικές σπουδές, στην περιοχή των τεχνολογιών πληροφορικής και επικοινωνιών και κατά προτίμηση σε τομείς σχετικούς με δίκτυα επικοινωνιών, κυβερνοασφάλεια (Cyber Security) και τεχνητή νοημοσύνη (AI). Καταληκτική ημερομηνία της υποβολής των αιτήσεων και των απαραίτητων δικαιολογητικών ορίζεται η 29η Νοεμβρίου 2024, ημέρα Παρασκευή και ώρα 17:00.

ΣΥΜΜΕΤΟΧΗ ΤΗΣ HP ΚΑΙ ΤΗΣ DIGIMARK ΣΤΗΝ XENIA 2024

Η Digimark ανακοινώνει την συμμετοχή της μαζί με την HP στην έκθεση-θεσμό της τουριστικής βιομηχανίας Xenia, η οποία θα πραγματοποιηθεί στο Metropolitan Expo στις 23-25 Νοεμβρίου 2024 Στο Hall1 – Περίπτερο D26/E24, η Digimark σε συνεργασία με την HP θα παρουσιάσουν λύσεις τεχνολογίας για τον τουριστικό κλάδο. Οι επισκέπτες της έκθεσης που θα περάσουν από το περίπτερο της εταιρείας θα έχουν τη δυνατότητα να ανακαλύψουν καινοτόμα προϊόντα και λύσεις HP όπως POS (Point Of Sales systems), εκτυπωτές, πολυμηχανήματα και προϊόντα Computing με εξελιγμένο Security, λύσεις DaaS καθώς και συστήματα Video Conferencing της POLY, ενός brand της HP. Επιπρόσθετα, θα δουν λύσεις για αδιάκοπη συνδεσιμότητα Internet σε απομακρυσμένες και μη περιοχές με τεχνολογίες 5G και Satellite που προσφέρει η Digimark στις επιχειρήσεις του κλάδου.

Cisco Webex Contact Center από την BEWISE: Η επόμενη γενιά επικοινωνίας στην εξυπηρέτηση πελατών για τις σύγχρονες επιχειρήσεις.

Στη σύγχρονη κοινωνία της πληροφορικής, οι επιχειρήσεις αναζητούν λύσεις που προσφέρουν ευελιξία και καινοτομία. Το Webex Contact Center, μια cloud-based λύση της Cisco, έρχεται να καλύψει τις ανάγκες τους και να βελτιώσει την εμπειρία επικοινωνίας με τους πελάτες τους, ώστε να προσαρμοστούν στον ψηφιακό μετασχηματισμό.
Σε αντίθεση με παραδοσιακές λύσεις, όπως το on-premise Cisco Unified Contact Center Express (UCCX), το Webex Contact Center προσφέρει έναν πιο ευέλικτο και οικονομικό τρόπο διαχείρισης επικοινωνιών. Ας εξετάσουμε πώς το Webex Contact Center ενισχύει την εμπειρία εξυπηρέτησης πελατών, καθώς και γιατί αποτελεί τη βέλτιστη λύση για επιχειρήσεις που επιθυμούν να αναβαθμιστούν ψηφιακά.

Πλεονεκτήματα του Webex Contact Center για τις σύγχρονες επιχειρήσεις

Άμεση Προσβασιμότητα & Ευελιξία
Το Webex Contact Center λειτουργεί σε cloud περιβάλλον, προσφέροντας άμεση προσβασιμότητα και ευελιξία, καθώς οι επιχειρήσεις δεν χρειάζεται να επενδύσουν σε φυσική υποδομή. Η cloud-based φύση του επιτρέπει στις εταιρείες να κλιμακώσουν τη χρήση τους εύκολα, ανάλογα με τις ανάγκες, χωρίς τα υψηλά κόστη αναβάθμισης ή συντήρησης των on-premise λύσεων.

Πολυκαναλική υποστήριξη
Στον σημερινό κόσμο, οι πελάτες μας έχουν την δυνατότητα να επικοινωνούν με μια επιχείρηση μέσω πολλαπλών καναλιών, όπως: κλήση, email, chat, social media κ.λπ. Το Webex Contact Center υποστηρίζει αυτήν την πολυκαναλική προσέγγιση από μία ενιαία πλατφόρμα, επιτρέποντας στους εκπροσώπους της εκάστοτε επιχείρησης να διαχειρίζονται όλα τα αιτήματα των πελατών ανεξάρτητα από το κανάλι επικοινωνίας που αυτή προήλθε. Αυτό προσφέρει μεγαλύτερη αποτελεσματικότητα στην εξυπηρέτηση και μειώνει τον χρόνο απόκρισης.

Ευκολία στη χρήση
Μέσω του Webex Contact Center, οι εργαζόμενοι μπορούν να δουλεύουν από οπουδήποτε, κάτι που ανταποκρίνεται στην αυξανόμενη τάση της απομακρυσμένης εργασίας. Πρόκειται για μια εξαιρετικά απλή και εύκολη πλατφόρμα στη χρήση, ανεξάρτητα από την τεχνική κατάρτιση του χρήστη. Τα οφέλη είναι πολλά και για τους διαχειριστές και τους υπεύθυνους ομάδων καθώς μπορούν ανά πάσα στιγμή να έχουν πλήρη έλεγχο και εποπτεία σε πραγματικό χρόνο, ανεξαρτήτως τοποθεσίας για την εξυπηρέτηση των αιτημάτων και την παραγωγικότητα των agents.

Ενσωμάτωση τεχνητής νοημοσύνης (AI) και analytics
Ένα από τα μεγάλα πλεονεκτήματα του Webex Contact Center είναι η ενσωμάτωση τεχνητής νοημοσύνης και αναλύσεων. Μέσω εργαλείων AI, οι επιχειρήσεις μπορούν να αυτοματοποιήσουν απλές διαδικασίες, να αναλύσουν τη συμπεριφορά των πελατών και να βελτιώσουν την εμπειρία εξυπηρέτησης, καθιστώντας την πιο προσωποποιημένη και αποδοτική.

Ενσωματωμένες Λύσεις Recording και Reporting
Το Webex Contact Center διαθέτει ενσωματωμένες δυνατότητες καταγραφής κλήσεων (recording) και αναφορών (reporting) με οπτικοποίηση, χωρίς την ανάγκη χρήσης τρίτων εφαρμογών. Αυτό σημαίνει ότι οι επιχειρήσεις έχουν άμεση πρόσβαση σε καταγραφές και αναλύσεις των επιδόσεών τους, ενώ μπορούν να προβάλλουν τα δεδομένα μέσω γραφημάτων και διαγραμμάτων. Αντίθετα, στο UCCX, οι δυνατότητες αυτές δεν είναι ενσωματωμένες και συχνά απαιτούν τρίτες λύσεις, προσθέτοντας κόστος και πολυπλοκότητα στη διαχείριση.

Γιατί το Webex Contact Center Υπερέχει σε Σχέση με το On-Premise UCCX

Το παραδοσιακό UCCX απαιτεί φυσική υποδομή, περιορίζοντας τις δυνατότητες κλιμάκωσης και την ευελιξία των επιχειρήσεων. Η μετάβαση στο Webex Contact Center, το οποίο λειτουργεί πλήρως στο cloud, προσφέρει έναν πιο οικονομικό και ευέλικτο τρόπο για τη διαχείριση επικοινωνιών. **Η μείωση των επενδύσεων σε υλικό και η δυνατότητα απομακρυσμένης εργασίας** επιτρέπουν στις **επιχειρήσεις να ανταποκρίνονται γρηγορότερα στις απαιτήσεις των πελατών** και να διαχειρίζονται καλύτερα τους πόρους τους.
Παράλληλα, το Webex Contact Center προσφέρει **πλήρη συμμόρφωση με τα παγκόσμια πρότυπα ασφαλείας και συμμόρφωσης.** Η Cisco προσφέρει υψηλά επίπεδα ασφάλειας δεδομένων και επικοινωνιών, ενώ διασφαλίζει ότι οι λύσεις της είναι σε πλήρη συμμόρφωση με κανονισμούς όπως το GDPR. Σε αντίθεση με τις on-premise λύσεις όπως το UCCX, όπου η διαχείριση της ασφάλειας και της συμμόρφωσης απαιτεί σημαντικές επενδύσεις και επιπλέον ανθρώπινους πόρους, το Webex Contact Center **προσφέρει ενσωματωμένες λύσεις ασφαλείας που καλύπτουν όλες τις σύγχρονες απαιτήσεις.**

Η γνώμη του ειδικού

«Ως μηχανικός στις εγκαταστάσεις του **Cisco Webex Contact Center,** μπορώ να επιβεβαιώσω ότι η λύση αυτή έχει φέρει εξαιρετικά αποτελέσματα σε μεγάλες επιχειρήσεις, πρόσφατο παράδειγμα μεγάλη εταιρεία στο χώρο της λιανικής-χονδρικής, με την οποία συνεργαζόμαστε. Στο συγκεκριμένο έργο, το contact center διαχειρίζεται πάνω από 1000 κλήσεις την ημέρα για διάφορες υπηρεσίες και η ευελιξία που προσφέρει έχει βελτιώσει σημαντικά τη λειτουργία τους.
Οι χρήστες μπορούν να εργάζονται από οπουδήποτε, κάνοντας την εξυπηρέτηση των πελατών πιο αποτελεσματική, ενώ οι supervisors έχουν τη δυνατότητα να παρακολουθούν τη ροή των κλήσεων από μία και μόνο πλατφόρμα, χωρίς να χρειάζεται να χρησιμοποιούν διαφορετικές εφαρμογές. Μάλιστα, **η δυνατότητα "call back" έχει διασφαλίσει ότι καμία κλήση δεν μένει αναπάντητη,** καθώς όλες εξυπηρετούνται από κάποιον agent, ανεξάρτητα από τον φόρτο εργασίας.
Στο τμήμα του Help Desk, η πλατφόρμα λειτουργεί περισσότερο από 4 μήνες άψογα, αποδεικνύοντας την χρηστικότητα και την αξιοπιστία της λύσης. Η δυνατότητα παραμετροποίησης του Webex Contact Center έχει επιτρέψει στη διοίκηση να προσαρμόζει τη λειτουργία του κέντρου εξυπηρέτησης σε πραγματικό χρόνο, βελτιώνοντας συνεχώς την αλληλεπίδραση τόσο με τους χρήστες όσο και με τους πελάτες. Οι ανάγκες της επιχείρησης καλύπτονται πλήρως, καθιστώντας το Webex Contact Center μια εξαιρετική επιλογή για την αναβάθμιση της εξυπηρέτησης πελατών στον ψηφιακό κόσμο».

Βασίλης Τσούτσας, Senior UC Engineer στην BEWISE και Cisco Webex Contact Center Expert

Μάθετε περισσότερα

bewise.gr, +30 213 0 908 400

Η Bausch + Lomb Ελλάδος υιοθετεί τη λύση Einvoicing της Softone Impact

Η Bausch + Lomb Ελλάδος υιοθετεί τη λύση Einvoicing της Softone Impact για την αποτελεσματική διαχείριση των συναλλαγών της με το Δημόσιο στο πλαίσιο συμμόρφωσης της εταιρείας με τις απαιτήσεις της νομοθεσίας για την ηλεκτρονική αποστολή των παραστατικών στην ΑΑΔΕ. Μέσω της cloud εφαρμογής η εταιρεία εξασφαλίζει την ασφαλή και έγκαιρη αποστολή των τιμολογίων της στην ΑΑΔΕ και την πλήρη εναρμόνισή της με τους πλέον απαιτητικούς κανονισμούς. Συνδυάζοντας τεχνολογίες αιχμής και την τεχνογνωσία της Softone Impact, το Einvoicing παρέχει στην Bausch + Lomb τη δυνατότητα ενημέρωσης σε πραγματικό χρόνο για κάθε στάδιο της διαδικασίας – από την παραλαβή έως την έγκριση και την πληρωμή του τιμολογίου, ενισχύοντας τη διαφάνεια και την αποτελεσματικότητα των συναλλαγών. Η real-time διασύνδεση της υπηρεσίας με το υφιστάμενο λογισμικό σύστημα εταιρείας επιτρέπει την αυτοματοποιημένη αποστολή των παραστατικών στην πλατφόρμα myDATA τη στιγμή της έκδοσής τους, οδηγώντας ταυτόχρονα σε σημαντική μείωση του απαραίτητου κόστους για την προετοιμασία και την αποστολή των τιμολογίων σε έντυπη μορφή καθώς και του απαιτούμενου χρόνου παραλαβής και πληρωμής των παραστατικών από τη δημόσια υπηρεσία. Η Bausch + Lomb είναι μια σύγχρονη πολυεθνική φαρμακευτική εταιρεία που παράγει και εμπορεύεται ένα ευρύ φάσμα επώνυμων συνταγογραφούμενων και μη συνταγογραφούμενων φαρμάκων, συμπληρωμάτων διατροφής, και ιατροτεχνολογικών προϊόντων, σε περισσότερες από 100 χώρες.

Οκτώβριος: Ευρωπαϊκός Μήνας Κυβερνοασφάλειας

ΧΟΡΗΓΟΣ
LOGISEK

Προστατεύοντας τον ψηφιακό κόσμο

Με όρους εκτίμησης επικινδυνότητας, οι σημαντικότερες απειλές στον κυβερνοχώρο για την Ελλάδα σχετίζονται με τις οικονομικές απάτες, τη σεξουαλική εκμετάλλευση ανηλίκων, τα εξαρτώμενα από το διαδίκτυο εγκλήματα, τη διακίνηση ψευδών ειδήσεων, και τις «κυβερνοεπιθέσεις» με τη χρήση κακόβουλου λογισμικού κατά κρίσιμων υποδομών, στρατηγικών δικτύων και κυβερνητικών υπηρεσιών. Σημαντικός είναι ακόμα ο κίνδυνος από τις δραστηριότητες των δικτύων του οργανωμένου εγκλήματος και της τρομοκρατίας στο «σκοτεινό διαδίκτυο» (dark web), όπως το εμπόριο όπλων και ναρκωτικών, η προπαγάνδα, η ριζοσπαστικοποίηση, η στρατολόγηση μαχητών, η χρηματοδότηση τρομοκρατικών επιθέσεων κ.ά. Εξίσου βαρύνουσα είναι η απειλή από κυβερνοεπιθέσεις, όπως αυτή κατά των ΕΛΤΑ τον Δεκέμβριο του 2022, με κύρια μορφή τους το Ransomware, δηλαδή επίθεση με κακόβουλο λογισμικό με σκοπό τα λύτρα από τον κάτοχο της συσκευής του δικτύου της υπηρεσίας. Οι συγκεκριμένες επιθέσεις δεν πραγματοποιούνται ωστόσο μόνο εναντίον δημόσιων υπηρεσιών αλλά και κατά εταιρειών, ακόμα και ιδιωτών. Μια επίθεση DDoS μπορεί να στοχεύσει από το online τραπεζικό σύστημα μέχρι μια ηλεκτρονική πλατφόρμα παραγγελίας φαγητού, αλλά και ένα μέσο κοινωνικής δικτύωσης, ενώ η πιο απλή μορφή επίθεσης Ransomware γίνεται κατά ιδιώτη, όπου με κλείδωμα του υπολογιστή τού ζητούν ένα συγκεκριμένο χρηματικό ποσό ως αντάλλαγμα. Ο ανθρώπινος παράγοντας παραμένει μια κρίσιμη τρωτότητα τόσο για τις επιχειρήσεις όσο και για τα άτομα. Το 82% των παραβιάσεων κατά των επιχειρήσεων αφορούσε τον ανθρώπινο παράγοντα, μέσω ζητημάτων όπως το σφάλμα και η κοινωνική μηχανική (social engineering).

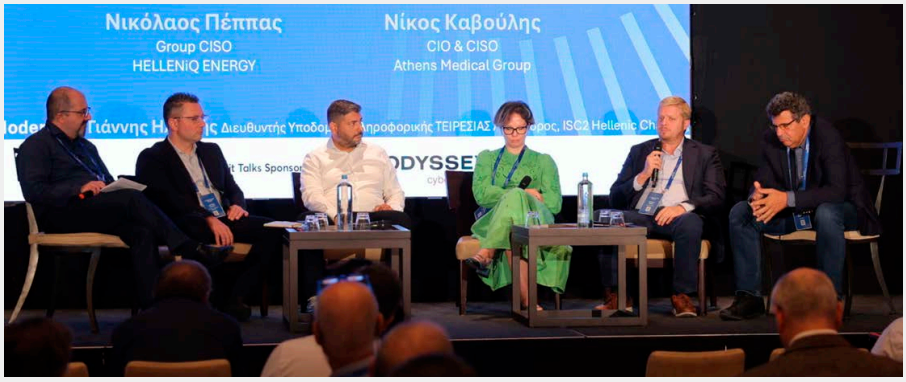
Η πλέον πρόσφατη θεσμική εξέλιξη στον τομέα της κυβερνοασφάλειας είναι η σύσταση, με τον Νόμο 5086/2024, της Εθνικής Αρχής Κυβερνοασφάλειας. Σκοπός της αρχής είναι η οργάνωση, ο συντονισμός, η εφαρμογή και ο έλεγχος ενός ολοκληρωμένου πλαισίου στρατηγικών, μέτρων και δράσεων για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, σε επίπεδο πρόληψης, προστασίας, αποτροπής, εντοπισμού, αντιμετώπισης, αποκατάστασης και ανάκαμψης από κυβερνοεπιθέσεις.

«Λύσεις που προσφέρουν σχεδόν απεριόριστες δυνατότητες για βελτιστοποίηση διαδικασιών, λήψη στοχευμένων αποφάσεων και παραγωγή καινοτομίας με τη δημιουργία νέων υπηρεσιών και προϊόντων.»

Γεώργιος Λεκάκος
Καθηγητής, Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας, Οικονομικό Πανεπιστήμιο Αθηνών - Πρόεδρος της Επιτροπής Αξιολόγησης

2nd Cyber Security summit
@ COSTA NAVARINO

Αντιμετωπίζοντας τους κινδύνους κυβερνοασφάλειας στην εφοδιαστική αλυσίδα



Στο πλαίσιο του 2nd Cyber Security Summit @ Costa Navarino πραγματοποιήθηκε το Summit Talk με τίτλο «Confronting with Supply Chain Cybersecurity Risks: we must do more than pray» στο οποίο, διακεκριμένοι επαγγελματίες του χώρου της κυβερνοασφάλειας αντάλλαξαν απόψεις για τις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στη διαχείριση των κινδύνων από την αλυσίδα προμηθευτών τους.

Τη συζήτηση συντόνισε ο Γιάννης Ηλιάδης, Διευθυντής Υποδομών Πληροφορικής στην ΤΕΙΡΕΣΙΑΣ και Πρόεδρος του ISC2 Hellenic Chapter, ενώ στο πάνελ συμμετείχαν οι Χρήστος Συγγελάκης, Group CISO και Group DPO στη Motor Oil GROUP, Λευτέρης Τζελέπης, CISO στη Steelmet, Δρ. Άννα Βαζιντάρη, ICT Manager στην Unisea Shipping Ltd., Νικόλαος Πέππας, Group CISO στη HELLENiQ ENERGY, και Νίκος Καβούλης, CIO και CISO στο Athens Medical Group.

Το θέμα της εφοδιαστικής αλυσίδας δεν είναι καινούριο στον τομέα της κυβερνοασφάλειας, αλλά όπως ανέφερε η Δρ. Άννα Βαζιντάρη, τα προβλήματα που υπάρχουν εντάθηκαν μετά την πανδημία του COVID-19. Επεσήμανε ότι η εξάρτηση των εταιρειών από το λογισμικό αυξάνει την επιφάνεια επίθεσης και δημιουργεί νέους κινδύνους για τις εταιρείες. Ιδιαίτερη αναφορά έκανε σε περιστατικό στον τομέα της ναυτιλίας το 2020-21, όπου μια κυβερνοεπίθεση σε συγκεκριμένο προμηθευτή προκάλεσε σοβαρά προβλήματα σε πολλές ναυτιλιακές εταιρείες.

Η εμπειρία αυτή έδειξε ότι τα προβλήματα με την εφοδιαστική αλυσίδα δεν είναι θεωρητικά, αλλά πραγματικά και με σοβαρές συνέπειες. Ακόμα, σχολιάζοντας τους νέους κανονισμούς ασφαλείας, σημείωσε ότι αποτελούν κρίσιμο μοχλό πίεσης για τη βελτίωση της κατάστασης στην Ναυτιλία.

Δεν υπάρχει μαγική συνταγή

Από την πλευρά του, Νικόλαος Πέππας, Group CISO της HELLENiQ ENERGY, υπογράμμισε την αύξηση του οικοσυστήματος των οργανισμών, το οποίο περιλαμβάνει πλέον πολλούς προμηθευτές. Όπως τόνισε, οι επιτιθέμενοι έχουν εντοπίσει την εφοδιαστική αλυσίδα ως έναν «δούρειο ίππο», ενώ επεσήμανε ότι δεν υπάρχει μια «μαγική» συνταγή για την αντιμετώπιση των κινδύνων και απαιτείται σημαντική επένδυση σε χρόνο, χρήμα και κόπο για την ανάπτυξη των κατάλληλων μέτρων ασφαλείας. Προέτρεψε τις εταιρείες να μειώσουν τον αριθμό των προμηθευτών τους και να επικεντρωθούν σε έναν αυστηρό και συνεχή έλεγχο καθ' όλη τη διάρκεια του κύκλου ζωής των συνεργασιών τους. Όπως τόνισε, σημαντική πρόκληση παραμένει η εξουσία που έχουν οι οργανισμοί να «κόψουν» έναν προμηθευτή που δεν πληροί τα κριτήρια ασφαλείας. Από την πλευρά του, ο Λευτέρης Τζελέπης ανέδειξε τη σημασία της ακριβούς κατανομής ευθυνών στη διαδικασία ελέγχου των προμηθευτών. Όπως υπογράμμισε, είναι σημαντικό να υπάρχει ένα εξειδικευμένο τμήμα εντός της εταιρείας που θα αναλάβει τη διαχείριση του ρίσκου. Όπως είπε, αν ένας βασικός προμηθευτής δημιουργήσει πρόβλημα κανείς δεν θα θυμάται μια αόριστη προειδοποίηση με αποτέλεσμα η ευθύνη να καταλήξει σε όλους. Επίσης, υπογράμμισε ότι πρέπει να γίνονται έγκαιροι έλεγχοι, ώστε όταν εντοπιστεί ένα πρόβλημα, η αντίδραση να είναι άμεση.

Τα κανονιστικά πλαίσια

Παίρνοντας τον λόγο ο Νίκος Καβούλης, CIO και CISO στο Athens Medical Group, αναφέρθηκε στα κανονιστικά πλαίσια και την αξία τους στη διαχείριση των κινδύνων. Με την εισαγωγή του NIS2 και άλλων νέων κανονισμών επεσήμανε ότι πλέον τα τμήματα ασφάλειας έχουν την εξουσία να επιβάλλουν τεχνικούς ελέγχους στους προμηθευτές τους, ενώ προσφέρεται και νομική κάλυψη στις εταιρείες. Ωστόσο, τόνισε ότι το 30-40% των εταιρειών δεν τηρούν όσα υπογράφουν και πρόσθεσε ότι η ευθύνη θα πρέπει να μεταβιβαστεί στις αρχές κυβερνοασφάλειας, ώστε να αναλάβουν τον έλεγχο των ελληνικών εταιρειών και να απαλλάξουν τις επιχειρήσεις από την υποχρέωση ελέγχου τρίτων. Τέλος, ο Χρήστος Συγγελάκης, Group CISO και Group DPO στη Motor Oil GROUP, έκλεισε τη συζήτηση, δίνοντας έμφαση στην ανάγκη για ρεαλισμό. Ενώ πολλοί ποντάρουν στις αναδυόμενες τεχνολογίες όπως η τεχνητή νοημοσύνη, ο κ. Συγγελάκης τόνισε ότι πρέπει πρώτα να σταθούμε στα πόδια μας και να μην βασιζόμαστε μόνο στις ελπίδες μας για την τεχνολογία. Σημείωσε ακόμα ότι πολλοί προμηθευτές λογισμικού και συσκευών ζητούν από τις επιχειρήσεις να τους εμπιστευτούν απόλυτα, ενώ προειδοποίησε ότι οι εταιρείες που παρέχουν ασφάλεια μπορεί να γίνουν πιο ελκυστικοί στόχοι από τους ίδιους τους πελάτες τους.

ΑΛΕΞΑΝΔΡΟΣ ΕΛΕΥΘΕΡΙΑΔΗΣ

«Μια επιτυχημένη υποβολή είναι αυτή που όχι μόνο αποδεικνύει την τεχνική αριστεία αλλά και παρουσιάζει τον αντίκτυπο του έργου στον πραγματικό κόσμο.»

Βασίλης Βασσάλος
Καθηγητής, Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

2nd Cyber Security summit
@ COSTA NAVARINO

NIS2: Η «καυτή» οδηγία που οδηγεί την κυβερνοασφάλεια σε ένα εντελώς νέο τοπίο

Η «καυτή» ευρωπαϊκή οδηγία που αλλάζει το τοπίο στην κυβερνοασφάλεια βρέθηκε στο επίκεντρο του discussion panel με τίτλο «Οδηγία NIS2 - Από τη θεωρία στην πράξη, τώρα!» που έλαβε χώρα κατά τη διάρκεια του 2d Cyber Security summit @ Costa Navarino. Στο εξαιρετικά ενδιαφέρον πάνελ συμμετείχαν οι: Γιάννης Αλεξάκης, Γενικός Διευθυντής της Εθνικής Αρχής Κυβερνοασφάλειας, Γιώργος Στεργιόπουλος, Επίκουρος Καθηγητής Ασφάλειας στο Πανεπιστήμιο Αιγαίου, Δημήτριος Πεππές, Διευθυντής στη Διεύθυνση Προστασίας Δεδομένων και Ασφάλειας Πληροφοριών του ΔΕΔΔΗΕ και Αργύρης Μακρυγεώργου, SecOps Business Development Manager, Greece, Hungary, Cyprus, Fortinet. Συντονιστής ήταν ο Δημήτρης Γκρίτζαλης, καθηγητής Κυβερνοασφάλειας στο Οικονομικό Πανεπιστήμιο Αθηνών (ΟΠΑ).

Κατά την τοποθέτησή του, ο κ. Αλεξάκης ανέφερε πως η νέα οδηγία «διαμορφώνει ένα εντελώς νέο τοπίο στον τομέα της κυβερνοσφάλειας», όπου η ζήτηση θα αυξηθεί ραγδαία σε ειδικούς. «Πλέον, με πολύ μεγάλη λεπτομέρεια, ορίζονται τα τεχνικά και νομοθετικά μέτρα και η πραγματικά πολύ μεγάλη διαφορά είναι ότι το βάρος απόδειξης της συμμόρφωσης πέφτει πλέον στους ίδιους τους οργανισμούς.

Με το NIS2 υπάρχει ανάγκη για ανάθεση ευθύνης και για διακριτούς ρόλους που να καλύπτουν τις απαιτήσεις, δήλωσε από την πλευρά του ο κ. Στεργιόπουλος, δηλώνοντας πως από πλευράς τεχνικών μέτρων υλοποίησης η οδηγία είναι «ευλογία» για τον CISO «διότι παίρνει το ρίσκο της ανάθεσης ευθύνης από προσωπική του επιλογή και το μεταφέρει στη διοίκηση».

«Ο πιο δύσκολα επιτεύξιμος παράγοντας στο δρόμο για την εναρμόνιση, είναι το ζήτημα της υλοποίησης των μηχανισμών που θέλουμε, κυρίως, να τοποθετήσουμε το οποίο εντάσσεται στο πλαίσιο του ευρύτερου ψηφιακού μετασχηματισμού που υλοποιείται στον ΔΕΔΔΗΕ. Αυτή τη στιγμή τρέχουν πάνω από 200 έργα Πληροφορικής στο Οργανισμό και η ενσωμάτωση της νέας θα δημιουργήσει μεγάλο φόρτο«», είπε ο από την πλευρά του ο κ. Πεππές.

Ερωτηθείς σχετικά για το ποιες θα πρέπει να είναι οι βασικές τεχνολογικές λύσεις που θα συνοδεύσουν την οδηγία ο κ. Μακρυγεώργου στάθηκε κυρίως στις επενδύσεις που θα πρέπει να γίνουν από επιχειρήσεις και οργανισμούς στο κομμάτι του automation, καθώς όπως είπε χαρακτηριστικά «οι reporting υποχρεώσεις θα είναι εκτενείς και επαναλαμβανόμενες». Στο τέλος της ενδιαφέρουσας συζήτησης ο κ. Γκρίτζαλης, επικαλούμενος την 38ετή πείρα του στα αμφιθέατρα, απευθύνθηκε στο κοινό του 2d Cyber Security summit @ Costa Navarino λέγοντας: «Επειδή όσο καλοί κι αν είστε επιστημονικά, όσο έμπειροι κι αν είστε επαγγελματικά, όσο επαρκείς διαθέσιμους πόρους κι αν διαθέτετε εκεί όπου θα είστε, δεδομένου αρκετού χρόνου, θα καταστείτε θύμα κυβερνοεπίθεσης με βεβαιότητα. Please get ready for it!».

ΣΤΑΘΗΣ ΒΑΣΙΛΟΠΟΥΛΟΣ

ONE TO ONE ΣΥΝΑΝΤΗΣΕΙΣ, WINE MASTERCLASS ΚΑΙ GOLF

Κορυφαίοι CISOs, ακαδημαϊκοί, ηγετικά στελέχη της αγοράς Πληροφορικής, εκπρόσωποι της κυβέρνησης και InfoSec experts έδωσαν το «παρών» στο δεύτερο Cyber Security summit @ Costa Navarino, το exclusive networking event που διοργάνωσε η Boussias Events, το περασμένο διήμερο, στο Costa Navarino. Στο επίκεντρο του event βρέθηκαν οι one-to-one επιχειρηματικές συναντήσεις CISOs και στελεχών προμηθευτών, οι οποίες έδωσαν την ευκαιρία για ανταλλαγή απόψεων, προτάσεων και λύσεων στις βασικές προκλήσεις που αντιμετωπίζουν σήμερα οι ελληνικές επιχειρήσεις που πρωτοστατούν στην ψηφιακή ασφάλεια. Το συνέδριο αποτέλεσε για ακόμα μια χρονιά το σημείο ετήσιας συγκέντρωσης και αλληλεπίδρασης των decision makers του Cyber Security στην Ελλάδα, που διαμορφώνει τη μελλοντική ατζέντα των ελληνικών επιχειρήσεων στη ψηφιακή ασφάλεια, αναδεικνύοντας τις προτεραιότητες, τις ανάγκες και τις λύσεις για τη συνεχή θωράκιση και προστασία των πληροφοριακών υποδομών από τις απειλές του σήμερα και του αύριο. Το πρόγραμμα του διημέρου περιλάμβανε επίσης, πλούσιο περιεχόμενο, ενδιαφέρουσες keynote ομιλίες, roundtable discussions, ψυχαγωγικές δραστηριότητες, όπως Golf experience, wine masterclass, olive oil tasting, Gala Dinner, lunches και cocktails που έδωσαν τη δυνατότητα για ουσιαστική επαφή σε ένα χαλαρό και ευχάριστο κλίμα.

BOUSSIAS events presents

22nd Bank Management conference

Powered by nexi

EARLY BIRD -10% UNTIL 25/10/24

26/11/24

Megaron Athens Concert Hall (Banquet Hall)

+ LIVE ONLINE

Foresight Digital Banking & Cyber-Resilience: Adapting & Disrupting the Expanding Digital Ecosystem

SPEAKERS

KEYNOTE SPEAKER

Panagiotis Kriaris
Unzer

THOUGHT LEADER INTERNATIONAL SPEAKER

Dr. Dimitrios Salampasis
Swinburne University of Technology

INTERNATIONAL SPEAKER

Kilian Thalhammer
Deutsche Bank AG

INTERNATIONAL SPEAKER

Tanja Imamovic
Raiffeisen Bank International

INTERNATIONAL SPEAKER

Margus Simson
Komercni Banka

INTERNATIONAL SPEAKER

Tommaso Jacopo Ulissi
Nexi Group

Stavroula Kampouridou
DIAS

Vassilis Panagiotidis
Hellenic Bank Association

- **Ioannis Tsikripis,** Bank of Greece
- **Dr. Nikolaos Kourogenis,** University of Piraeus
- **Dr. Andreas G. Koutoupis,** University of Thessaly
- **Zefi Nikolaou,** ASCO Greece
- **Stratos Molyviatis,** National Bank of Greece
- **Anestis Petridis,** Eurobank
- **Marios Tzitziras,** Piraeus Bank
- **Eleftherios Kororos,** National Bank of Greece
- **Aris Divaris,** National Bank of Greece
- **Nikos Papadoglou,** NEXI Greece
- **Stavros Balis,** Datatechnika
- **Effie Bitrou,** National Bank of Greece
- **Panagiotis Divriotis,** Alpha Bank
- **Katerina Glava,** Deloitte
- **Demie Goudoufa,** National Bank of Greece
- **Yiannos Ioannidis,** Alpha Bank
- **Fotis Kourmousis,** Hellenic Financial Stability Fund
- **Marina Krimba,** Eurobank
- **Antreas Ntousis,** Datatechnika
- **Fotis Panagiotopoulos,** Accenture Greece
- **Sophia Papastefanou,** Alpha Bank
- **Dimitris Stavropoulos,** Alpha Bank
- **Kostas Tovil,** tbi bank Greece
- **Dr. Akis Tsekouras,** Mastercard
- **George Tsiantos,** Fitch Ratings

JOIN NOW WITH -10%

LEARN MORE

POWERED BY nexi

GOLD SPONSOR

InTrust Information Technology Trust

IBM Platinum Partner

GRAND SPONSORS

AUSTRIACARD HOLDINGS

performance | Platinum Business Partner IBM

SPONSOR

Deloitte.

Google Cloud

Papakosmas Datatechnika

HONORARY SUPPORT

DIAS · HELLENIC BANK ASSOCIATION · HELLENIC

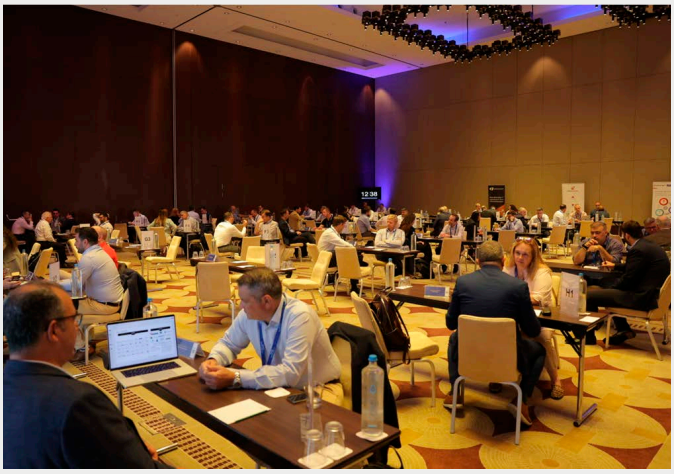
Subscriptions: Hara Katsarou, **T:** +30 210 661 7777 (ext. 233), **M:** +30 6951 007 127, **E:** xkatsarou@boussias.com
Sponsorships: Liza Antoniadi, **T:** +30 210 661 7777 (ext. 158), **M:** +30 6976 781 351, **E:** lantoniadi@boussias.com
Phaedra Baritaki, **T:** +30 210 661 7777 (ext. 192), **M:** +30 6980 182 723, **E:** pbaritaki@boussias.com
Content: Vicky Pavlatou, **M:** +30 6943 627 371, **E:** vpavlatou@boussias.com

Official Publication netweek

«Ανυπομονώ να δω τις ιδέες και τις καινοτομίες που θα οδηγήσουν σε θετικές αλλαγές στα εταιρικά περιβάλλοντα και την αγορά. Να δείξουμε ότι είμαστε σημαντικοί παίκτες και να αξιοποιήσουμε την παράδοση των καλών Ελλήνων μηχανικών.»

Δρ. Ματίνα Θωμαΐδου
VP, Head of Data Science, Dataseat (Verve)

2nd Cyber Security summit
@COSTA NAVARINO



Στο επίκεντρο βρέθηκαν οι επιχειρηματικές συναντήσεις CISOs και στελεχών προμηθευτών

Golf Experience

olive oil tasting

wine masterclass

Gala Dinner

Ευκαιρίες για networking

BOUSSIAS events presents

1st Secure Digital Governance Conference

Creating and maintaining a secure and resilient State

27/11/2024

Συνεδριακός Χώρος Εθνικής Ασφαλιστικής

Η ΣΥΜΜΕΤΟΧΗ ΕΙΝΑΙ ΕΛΕΥΘΕΡΗ ΓΙΑ ΤΑ ΣΤΕΛΕΧΗ ΥΠΟΥΡΓΕΙΩΝ, ΠΕΡΙΦΕΡΕΙΩΝ, ΔΗΜΩΝ ΚΑΙ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

Το **1st Secure Digital Governance Conference** με την Αιγίδα του **Υπουργείου Ψηφιακής Διακυβέρνησης** έρχεται για να εξετάσει το σημερινό στίγμα της χώρας σε ό,τι αφορά στον Ψηφιακό Μετασχηματισμό του κράτους, τους τρόπους που απαιτούνται για να καλύψουμε την απόσταση από τον ευρωπαϊκό μέσο όρο καθώς και τα επόμενα βήματα, έργα, συνέργειες και δράσεις που απαιτούνται, με σκοπό τη διατήρηση και την ενίσχυση του σημερινού ισχυρού momentum, σε συνδυασμό με την ανθεκτικότητα και απόκριση του κράτους σε Κυβερνοαπειλές.

ΑΠΕΥΘΥΝΕΤΑΙ ΣΕ:

- **Ανώτερα στελέχη του δημόσιου τομέα και των φορέων του.**
- **Policy makers - Policy Officers.**
- **Ανώτερα στελέχη επιχειρήσεων που είτε συνεργάζονται με το δημόσιο στην υλοποίηση έργων είτε του παρέχουν υπηρεσίες.**
- **Επιστήμονες, μηχανικοί, τεχνικοί, ελεύθεροι επαγγελματίες και στελέχη εταιριών, που έχουν σχέση με τον Ψηφιακό Μετασχηματισμό και την ασφάλεια του, υπό την ευρύτερη έννοιά του.**

JOIN NOW **LEARN MORE**

Συμμετοχές: Βίκυ Στάμου, **M:** 6947 145 105, **E:** vstamou@boussias.com
Χορηγίες: Λίζα Αντωνιάδη, **T:** 210 6617 777 (εσωτ. 158), **E:** lantoniadi@boussias.com
Φαίδρα Μπαριτάκη, **T:** 210 6617 777 (εσωτ. 192), **M:** 6980 182 723, **E:** pbaritaki@boussias.com

Official Publications
Manufacturing netweek

«Μία επιτυχημένη συμμετοχή χαρακτηρίζεται από τη σαφήνεια του σκοπού, την καινοτομία της προσέγγισης και τη μετρήσιμη επίδραση που φέρνει, αλλά και βαθιά κατανόηση των προβλημάτων που επιλύουν.»

Νίκος Μπάμπης
Chief AI Officer, avocado

Αντίστροφη μέτρηση για την εφαρμογή του NIS2

Από τον νέο χρόνο αναμένεται να ξεκινήσει σταδιακά η πλήρης εφαρμογή και στην Ελλάδα του NIS2, του νέου κανονισμού που εστιάζει και ρυθμίζει τα σχετικά με την κυβερνοασφάλεια θέματα σε άνω των 2000 κρίσιμων για την ομαλή εξυπηρέτηση του κοινωνικού συνόλου οργανισμούς και επιχειρήσεις. Αυτό επιβεβαιώθηκε στη διάρκεια ενημερωτικής συνάντησης της ηγεσίας της Εθνικής Αρχής Κυβερνοασφάλειας (ΕΑΚ) με τους διαπιστευμένους δημοσιογράφους, παρουσία και του πολιτικού προϊσταμένου τους, υπουργού Ψηφιακής Διακυβέρνησης, Δημήτρη Παπαστεργίου, ο οποίος δήλωσε ότι ο ευρωπαϊκός κανονισμός βρίσκεται πλέον σε φάση διαβούλευσης και ενημέρωσης των ενδιαφερομένων ως τις 2 Νοεμβρίου, για να ακολουθήσει η συζήτηση στη Βουλή και η ενσωμάτωσή του στην εθνική νομοθεσία, «πριν από αρκετές άλλες χώρες-μέλη».

Ο διοικητής της Αρχής, Μιχάλης Μπλέτσας (μιλώντας σε απευθείας σύνδεση από τη Βοστώνη, όπου βρίσκεται αυτές τις ημέρες) και οι δυο υποδιοικητές, Γιάννης Παυλόσογλου και Αντιγόνη Γιαννακάκη, ενημέρωσαν, διευκρίνισαν και απάντησαν σε πάμπολλες ερωτήσεις, δίνοντας μια σαφή και ρεαλιστική εικόνα τόσο του οδικού χάρτη για την εφαρμογή του NIS2, στις αρχές του επόμενου χρόνου, όσο και του ρόλου που καλείται να παίξει η ΕΑΚ σ' ό,τι αφορά αρχικά στην ενημέρωση και στη συνέχεια -μόλις ξεκινήσει η εφαρμογή- τον έλεγχο των κρίσιμων οργανισμών και επιχειρήσεων, ως προς τα προληπτικά μέτρα που έχουν λάβει.

Διευρύνεται το πεδίο

Όπως εξήγησε ο κ. Μπλέτσας, βάσει του ιδρυτικού της νόμου (από τις 14/02/24) αρμόδια για αυτόν τον έλεγχο -εκτός των άλλων καθηκόντων της- και την εποπτεία της εφαρμογής του από τους εμπλεκόμενους είναι η ΕΑΚ, η οποία επίσης ετοιμάζεται, αυξάνοντας το προσωπικό της (έφτασε ήδη, μέσω αποσπάσεων, τα 75 άτομα, έναντι οργανικής δύναμης 150) και οργανώνοντας δύναμη επιθεωρητών, για τον έλεγχο και τις αναγκαίες πιστοποιήσεις.

Οι ελεγχόμενοι οργανισμοί και επιχειρήσεις (μεσαίες, μεγάλες, αλλά και μικρότερες αναλόγως επικινδυνότητας και cyber-resilience, καθώς το πεδίο είναι ιδιαίτερα ευρύ, πλέον, σε σχέση με τις 170 ελεγχόμενες του προηγούμενου NIS) ανήκουν στους τομείς της υγείας, της ενέργειας, των μεταφορών, των τραπεζών, των υποδομών, της ύδρευσης και των ψηφιακών παρόχων, με νέες προσθήκες την κεντρική διοίκηση του κράτους και τους ΟΤΑ, τη διαχείριση υπηρεσιών ΤΠΕ, το διάστημα, τα λύματα και τη διαχείρισή τους, τα χημικά προϊόντα, τον κατασκευαστικό τομέα και, βεβαίως, τα τρόφιμα. Τα κριτήρια λαμβάνουν υπόψιν -πέραν του αντικειμένου- τον αριθμό εργαζομένων και τον κύκλο εργασιών.

Μητρώο και πρόστιμα

Όλες αυτές οι οντότητες είναι πλέον υποχρεωμένες όχι μόνο να εγγραφούν στους σχετικούς καταλόγους και το Μητρώο της Αρχής, αλλά και να της αναφέρουν εντός 24 ωρών κάθε περιστατικό παραβίασης ασφαλείας, ώστε να ληφθούν μέτρα και να προληφθούν δυσμενέστερες επιπτώσεις, με την επιβολή υψηλών προστίμων να επικρέμαται σε περίπτωση μη αναφοράς. Επίσης, διευρύνεται η ευθύνη από τον CISO στο σύνολο πλέον της εκτελεστικής ομάδας. Η εν εξελίξει διαβούλευση, πάντως, συνδυάζεται με εκτενή ενημέρωση όλων των ενδιαφερομένων πλευρών, μέσω των συλλογικών οργάνων και φορέων, ενώ η Αρχή ετοιμάζει και δικτυακή ενημέρωση.

ΓΙΑΝΝΗΣ ΡΙΖΟΠΟΥΛΟΣ

ΠΛΕΓΜΑ ΠΡΟΤΕΙΝΟΜΕΝΩΝ ΠΟΛΙΤΙΚΩΝ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΑΠΟ ΤΗ VODAFONE

Σε συνάντηση με τον Διοικητή της Εθνικής Αρχής Κυβερνοασφάλειας, Μιχάλη Μπλέτσα, η Vodafone παρουσίασε τις πρωτοβουλίες που έχει αναλάβει στον τομέα της κυβερνοασφάλειας, καθώς και τις προτάσεις πολιτικών που προέκυψαν σε συνεργασία με το Ελληνικό Ίδρυμα Ευρωπαϊκής και Εξωτερικής Πολιτικής (ΕΛΙΑΜΕΠ). Το συγκεκριμένο πλέγμα πολιτικών προέκυψε σε συνέχεια ερευνών κοινής γνώμης που διεξήχθησαν από την Metron Analysis για λογαριασμό της Vodafone Ελλάδας και σε συνεργασία με το ΕΛΙΑΜΕΠ, σχετικά με την αντίληψη των πολιτών και των επιχειρήσεων στην Ελλάδα για την ασφάλεια στο ψηφιακό περιβάλλον, αλλά και τη σχετική συζήτηση στρογγυλής τραπέζης που πραγματοποιήθηκε από το Κέντρο για την Κυβερνοασφάλεια του Οικονομικού Φόρουμ των Δελφών, παρουσία των εμπλεκόμενων φορέων. Το έργο αναδεικνύει τις δομικές παθογένειες για την κυβερνοασφάλεια στην Ελλάδα και προτείνει κατευθύνσεις μεταρρυθμίσεων που αφορούν, μεταξύ άλλων, στην αλλαγή του υφιστάμενου νομοθετικού πλαισίου για την προστασία και ενίσχυση της ανθεκτικότητας των κρίσιμων υποδομών, καθώς και την ευαισθητοποίηση της ελληνικής κοινωνίας σε θέματα ψηφιακής ασφάλειας. Πιο συγκεκριμένα, επισημάνθηκαν προβληματικά χαρακτηριστικά του οικοσυστήματος όπως ο κατακερματισμός της πολιτικής εσωτερικής ασφαλείας, η προβληματική συνεργασία μεταξύ ιδιωτικού και δημοσίου τομέα και η απουσία κουλτούρας ασφαλείας από το ανθρώπινο δυναμικό.

BOUSSIAS events presents

SUPER EARLY BIRD
-15% έως 22/11/24

8th InsurTech conference

Insurance's Extended Ecosystem: Digital Transformation - AI - Cyber-Resilience

29/01/2025

Athens

The Conference will refer to the broader network of Entities and Technologies that interact with the Insurance Industry potentially including policyholders, brokers, regulators, and various cutting-edge technologies such as IoT devices, AI, and blockchain platforms.

SPEAKERS

Prof. George Samakovitis
University of Greenwich, London, UK

Prof. Christos Xenakis
University of Piraeus

Dr Xenofon Liapakis
Intersalonica

Nikos Georgopoulos
Cromar Insurance Brokers, DPO Academy

Demetra-Ioanna Lychros
Hellenic Association of Insurance Intermediaries

Constantinos Roussis
Allianz European Reliance

Nikos Sofronas
Greek Institute for Insurance Education

Michael Tzortzoris
EADE, SEMA, Amt Insurance Brokers

- **Ioannis Aligizakis,** *Generali Hellas*
- **Ioannis Christaras,** *Groupama Asfalistiki*
- **Stavroula Karagianni,** *Allianz European Reliance (Greece & Cyprus)*
- **Panos Katertzis,** *Eurolife FFH*
- **Emilios Markou,** *Hellas Direct*
- **George Papasarantos,** *Generali*
- **Marios Sintichakis,** *INTERAMERICAN*
- **Panayiotis Sofocleous,** *Cyprus Insurance News*
- **Fannie Theofanidou,** *Radical Communications*
- **Petros Tsonis,** *Ethniki Asfalistiki*

JOIN NOW WITH -15%

LEARN MORE

HONORARY SUPPORTS

Subscriptions: Hara Katsarou **T:** +30 210 6617 777 (ext. 233) **M:** +30 6951 007 127, **E:** xkatsarou@boussias.com
Sponsorships: Liza Antoniadi **T:** +30 210 6617 777 (ext. 158), **M:** +30 6976 781 351, **E:** lantoniadi@boussias.com
Phaedra Baritaki, **T:** +30 210 6617 777 (ext. 192), **M:** +30 6980 18 2723, **E:** pbaritaki@boussias.com
Content: Vicky Pavlatou **M:** +30 6943 627 371, **E:** vpavlatou@boussias.com

Official Publication
netweek

«Μια επιτυχημένη συμμετοχή ξεχωρίζει όχι μόνο για την πρωτοπορία της, αλλά και για τον τρόπο που διαμορφώνει το μέλλον με υπευθυνότητα, προάγοντας ηθικά πρότυπα.»

Πάνος Μπάσιος
Digital, Data & Analytics Director, MSD Greece, Cyprus and Malta

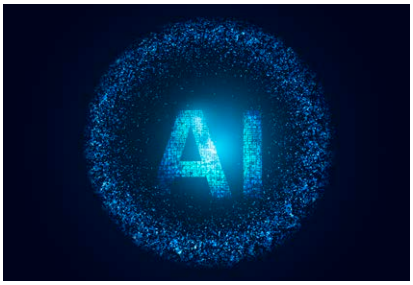
Η Dotsoft αναλαμβάνει έργο διαχείρισης κρίσεων και πολιτικής προστασίας στον Δήμο Σάμης

Η Dotsoft συνεργάζεται με τον δήμο Σάμης για την ανάπτυξη ενός σύγχρονου Κέντρου Επιχειρήσεων, εξοπλισμένου με καινοτόμες τεχνολογίες για τη διαχείριση κρίσεων και την πολιτική προστασία. Το νέο κέντρο θα έχει ενεργειακή αυτοτέλεια και θα χρησιμοποιεί τεχνολογίες Διαδικτύου των Πραγμάτων (IoT), διασφαλίζοντας την άμεση αντίδραση στις ανάγκες των δημοτών.

Η υλοποίηση του έργου περιλαμβάνει την εγκατάσταση δικτύου 60 αισθητήρων για την ανίχνευση πυρκαγιών, διάβρωσης και τη διαχείριση φυσικών πόρων. Οι αισθητήρες θα μεταδίδουν δεδομένα σε πραγματικό χρόνο σε μια ενιαία πλατφόρμα IoT, όπου θα αποθηκεύονται και θα αναλύονται, δίνοντας έτσι τη δυνατότητα για πρόληψη και άμεση ανταπόκριση σε πιθανά περιστατικά. Το Κέντρο Διαχείρισης Κρίσεων θα διαθέτει επίσης σύστημα Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης για την ανάλυση των δεδομένων, επιτρέποντας την αξιολόγηση κινδύνων και τη βέλτιστη λήψη αποφάσεων. Παράλληλα, θα δημιουργηθεί ψηφιακή πλατφόρμα ενημέρωσης των πολιτών, προσφέροντας αξιόπιστες πληροφορίες για την πρόληψη και αντιμετώπιση κινδύνων. Επιπλέον, το κέντρο θα εξοπλιστεί με σειρήνες προειδοποίησης, οθόνες πληροφόρησης, δορυφορικά τηλέφωνα και drones, ενώ τα οχήματα πολιτικής προστασίας θα διαθέτουν GPS για την άμεση παρακολούθησή τους. Στόχος του έργου είναι να ενισχύσει τις υποδομές του Δήμου στους τομείς της πολιτικής προστασίας και της ασφάλειας των δημοτών και των επισκεπτών. Οι παραπάνω δράσεις ενισχύουν τα μέτρα πρόληψης, παρακολούθησης, ελέγχου και προστασίας σε καταστάσεις έκτακτης ανάγκης όπως σεισμούς, πλημμύρες, πυρκαγιές, πανδημίες αλλά και έκτακτα καιρικά φαινόμενα. Το έργο χρηματοδοτείται από το Πρόγραμμα «ΑΝΤΩΝΗΣ ΤΡΙΤΣΗΣ» και αναμένεται να ολοκληρωθεί στα μέσα του 2025.

Μόλις μία στις 10 εταιρείες έχει υιοθετήσει πλήρως τη χρήση AI

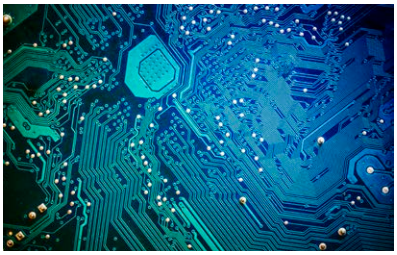
Τι δείχνει μελέτη της Salesforce



Πρόσφατη έρευνα της Salesforce αποκαλύπτει ότι, παρά την αναγνώριση της σημασίας της Τεχνητής Νοημοσύνης (AI) για τις επιχειρήσεις, μόλις το 11% των Chief Information Officers (CIO) έχει υιοθετήσει πλήρως αυτήν την τεχνολογία. Η έρευνα, που πραγματοποιήθηκε σε 150 CIO από εταιρείες με περισσότερους από 1.000 υπαλλήλους, υπογραμμίζει ότι το 84% των CIO θεωρεί την AI τόσο σημαντική όσο υπήρξε η άνοδος του διαδικτύου. Ωστόσο, σοβαρές ανησυχίες σχετικά με την ασφάλεια και την προστασία των δεδομένων εμποδίζουν την ευρύτερη υιοθέτησή της.
Η έρευνα επισημαίνει ότι οι CIO αντιμετωπίζουν αυξανόμενη πίεση να αναπτύξουν εξειδικευμένη γνώση γύρω από την AI, με το 61% να αναφέρει αυξημένες προσδοκίες σχετικά με τις γνώσεις τους. Παρά τη δυναμική της τεχνολογίας, το 67% των CIO ακολουθεί προσεκτική προσέγγιση, κυρίως λόγω των ανησυχιών που σχετίζονται με την ασφάλεια των δεδομένων και την αξιοπιστία τους. Επιπλέον, η κατανομή των πόρων παραμένει ένα σημαντικό ζήτημα. Παρόλο που οι εταιρείες επενδύουν περίπου το 20% του προϋπολογισμού τους σε δεδομένα και υποδομές, μόνο το 5% διατίθεται για την ανάπτυξη AI. Το 47% των CIO δηλώνει αβεβαιότητα σχετικά με το αν οι πόροι κατανέμονται σωστά, γεγονός που συνδέεται με την ανάγκη για αξιόπιστα και ασφαλή δεδομένα.

Ανέτοιμες οι εταιρείες

Παρά τις προκλήσεις, το 66% των CIO πιστεύει ότι η επένδυση στην AI θα αποδώσει. Ωστόσο, το 68% θεωρεί ότι οι επιχειρηματικοί εταίροι τους έχουν μη ρεαλιστικές προσδοκίες για το πότε θα επιτευχθεί αυτή η απόδοση, γεγονός που δημιουργεί επιπλέον πίεση. Ένα άλλο ενδιαφέρον εύρημα της έρευνας είναι ότι, ενώ οι εταιρείες αναγνωρίζουν τις δυνατότητες της AI, δεν είναι όλες εξίσου έτοιμες να την υιοθετήσουν. Για παράδειγμα, τα τμήματα εξυπηρέτησης πελατών, αν και έχουν τη μεγαλύτερη δυναμική για χρήση της AI, θεωρούνται τα λιγότερο προετοιμασμένα. Αντίθετα, οι ομάδες μάρκετινγκ είναι πρόθυμες να αγκαλιάσουν την AI, αλλά στερούνται των κατάλληλων δεξιοτήτων.
Συμπερασματικά, στην έρευνα γίνεται ξεκάθαρο πως ενώ η AI αναμένεται να διαμορφώσει το μέλλον των επιχειρήσεων, οι προκλήσεις στην υιοθέτηση της τεχνολογίας παραμένουν σοβαρές.



HUAWEI: ΑΝΗΣΥΧΙΕΣ ΓΙΑ ΠΙΘΑΝΗ ΠΑΡΑΒΙΑΣΗ ΕΞΑΓΩΓΙΚΩΝ ΠΕΡΙΟΡΙΣΜΩΝ

Η Taiwan Semiconductor Manufacturing Company (TSMC) ενημέρωσε τις αμερικανικές αρχές για την ύπαρξη ενός από τα τσιπ της σε προϊόν της Huawei, μετά από έρευνα της TechInsights. Ειδικότερα, η ανάλυση που πραγματοποιήθηκε αποκάλυψε την παρουσία του τσιπ σε ένα προϊόν της Huawei (το οποίο αποσυναρμολογήθηκε), προκαλώντας ανησυχίες για πιθανή παραβίαση των αμερικανικών εξαγωγικών περιορισμών που επιβλήθηκαν στην Huawei το 2019. Όπως αποκαλύπτει το Reuters, το προϊόν που ελέγχθηκε ήταν το Ascend 910B, το πιο εξελιγμένο AI τσιπ της Huawei. Η TSMC δήλωσε ότι δεν έχει προμηθεύσει τσιπ στη Huawei από τον Σεπτέμβριο του 2020, αλλά δεν είναι σαφές πώς το συγκεκριμένο τσιπ βρέθηκε στα χέρια της Huawei.
Η υπόθεση τονίζει τις δυσκολίες επιβολής των εξαγωγικών ελέγχων σε τεχνολογίες αιχμής και υπογραμμίζει την ανάγκη της Huawei για προηγμένα τσιπ. Από την πλευρά της, η αμερικανική κυβέρνηση εξετάζει το θέμα, αλλά δεν έχει επιβεβαιώσει αν υπάρχει κάποια έρευνα σε εξέλιξη.

ΑΡΧΙΣΥΝΤΑΚΤΗΣ:
Στάθης Βασιλόπουλος,
svasilopoulos@boussias.com

ΣΥΝΤΑΞΗ:
Αλέξανδρος Ελευθεριάδης,
aeleyftheriadis@boussias.com

Γιάννης Ριζόπουλος

ΔΙΑΦΗΜΙΣΗ:
Έλενα Δασκαλάκη
edaskalaki@boussias.com

ΣΕΛΙΔΟΠΟΙΗΣΗ:
Αλέξανδρος Εγγλέζος

ΔΙΕΥΘΥΝΟΥΣΑ ΣΥΜΒΟΥΛΟΣ:
Αντωνία Κατσουλιέρη

ΔΙΕΥΘΥΝΤΡΙΑ ΣΥΝΤΑΞΗΣ ΕΚΔΟΣΕΩΝ:
Κατερίνα Πολυμερίδου

GROUP ADVERTISING DIRECTOR: **Λήδα Πλατή**

GROUP SUBSCRIPTIONS DIRECTOR: **Αμαλία Ψιλούδη**

BOUSSIAS media

ΚΛΑΔΙΚΑ ΜΕΣΑ ΜΟΝ ΙΚΕ
Λ. Κηφισίας 125-127 -Τ.Κ. 115 24, Αθήνα
Κτίριο Cosmos Center **Τ:** 210 710 2452

Κόστος ετήσιας εταιρικής συνδρομής: 270€ + ΦΠΑ 24%

FIND US ON