

Insider

ΦΙΛΙΠΠΟΣ ΧΑΤΖΗΖΑΧΑΡΙΑΣ
ΥΦΥΠΟΥΡΓΟΣ ΕΡΕΥΝΑΣ, ΚΑΙΝΟΤΟΜΙΑΣ
ΚΑΙ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΣΕ ΠΟΡΕΙΑ ΔΗΜΙΟΥΡΓΙΑΣ
ΚΑΙ Η ΚΥΠΡΙΑΚΗ
«SILICON VALEY»

ΑΦΙΕΡΩΜΑ
INTERNATIONAL
BANKING
ΟΙ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΤΑ
ΠΡΟΪΟΝΤΑ ΠΟΥ
ΠΡΟΣΦΕΡΟΝΤΑΙ

ΟΙ 30 ΠΟΥ
«ΧΡΥΣΟΠΛΗΡΩΣΕ»
Η ΚΥΒΕΡΝΗΣΗ
ΤΟ 2022

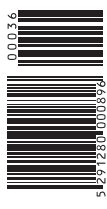
ΘΑΝΟΣ ΜΙΧΑΗΛΙΔΗΣ

ΕΞΕΤΑΖΟΥΜΕ ΝΕΕΣ ΕΠΕΝΔΥΣΕΙΣ ΞΕΝΟΔΟΧΕΙΩΝ ΣΕ ΚΥΠΡΟ ΚΑΙ ΕΞΩΤΕΡΙΚΟ

Ο CEO ΤΩΝ ΘΑΝΟΣ HOTELS & RESORTS ΜΙΛΑ ΓΙΑ ΤΑ ΕΠΕΝΔΥΤΙΚΑ ΣΧΕΔΙΑ ΤΟΥ ΟΜΙΛΟΥ ΤΟΥ ΚΑΙ ΑΝΑΛΥΕΙ ΤΙΣ ΠΡΟΤΕΡΑΙΟΤΗΤΕΣ ΤΟΥ ΜΕΤΑ ΤΗΝ ΑΝΑΛΗΨΗ ΤΗΣ ΠΡΟΕΔΡΙΑΣ ΤΟΥ ΠΑΣΥΣΕ

ΑΦΙΕΡΩΜΑ

Η ΤΕΧΝΟΛΟΓΙΑ ΣΤΗ ΝΕΑ ΕΠΟΧΗ



ΧΟΡΗΓΟΣ ΑΦΙΕΡΩΜΑΤΟΣ



Η ΤΕΧΝΟΛΟΓΙΑ ΣΤΗ ΝΕΑ ΕΠΟΧΗ

ΠΕΡΙΕΧΟΜΕΝΑ

54 - ODYSSEY

79 - LOGICOM

80 - ATL SOLUTIONS & DELL
TECHNOLOGIES

82 - eBOS TECHNOLOGIES

84 - EY

86 - IRON MOUNTAIN

88 - KPMG ΚΥΠΡΟΥ

90 - ΗΛΙΑΣ ΝΕΟΚΛΕΟΥΣ
& ΣΙΑ ΔΕΠΕ

92 - PRIMETEL

94 - PwC

96 - SOFTONE TECHNOLOGIES

ΤΟ ΨΗΦΙΑΚΟ FAST FORWARD ΚΑΙ ΤΑ ΟΦΕΛΗ ΣΕ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ ΝΟΙΚΟΚΥΡΙΑ

ΤΟ ΨΗΦΙΑΚΟ FAST FORWARD ΣΤΟ ΟΠΟΙΟ ΕΒΑΛΕ ΤΗΝ ΚΥΠΡΟ ΚΑΙ ΟΛΟ ΤΟΝ ΠΛΑΝΗΤΗ Η ΠΑΝΔΗΜΙΑ ΑΝΕΔΕΙΞΕ ΕΝΑ ΝΕΟ ΜΟΝΤΕΛΟ ΛΕΙΤΟΥΡΓΙΑΣ ΤΗΣ ΟΙΚΟΝΟΜΙΑΣ, ΤΟΥ ΚΡΑΤΟΥΣ ΚΑΙ ΤΗΣ ΙΔΙΑΣ ΤΗΣ ΚΟΙΝΩΝΙΑΣ, ΤΟ ΟΠΟΙΟ ΕΧΕΙ ΣΤΟ ΕΠΙΚΕΝΤΡΟ ΤΗΝ ΨΗΦΙΑΚΗ ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΤΗΝ ΙΣΟΤΙΜΗ ΠΡΟΣΒΑΣΗ ΣΕ ΓΡΗΓΟΡΕΣ ΚΑΙ ΑΞΙΟΠΙΣΤΕΣ ΥΠΟΔΟΜΕΣ. ΤΑ ΤΕΛΕΥΤΑΙΑ ΧΡΟΝΙΑ, ΤΟ 5G, ΤΟ INTERNET OF THINGS, Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΚΑΙ Η ΕΙΚΟΝΙΚΗ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ ΕΓΙΝΑΝ ΜΕΡΟΣ ΤΗΣ ΖΩΗΣ ΚΑΙ ΚΥΒΕΡΝΗΣΗ ΚΑΙ ΙΔΙΩΤΙΚΟΣ ΤΟΜΕΑ ΚΑΝΟΥΝ ΕΝΕΡΓΕΙΕΣ ΩΣΤΕ ΝΑ ΜΗΝ ΕΙΝΑΙ Η ΚΥΠΡΟΣ ΟΥΡΑΓΟΣ ΤΩΝ ΕΞΕΛΙΞΕΩΝ. ΣΕ ΕΙΔΙΚΟ ΑΦΙΕΡΩΜΑ ΤΟΥ INSIDER ΑΝΑΛΥΟΥΜΕ ΜΕΣΩ ΑΡΘΡΟΓΡΑΦΙΑΣ ΚΑΙ ΣΥΝΕΝΤΕΥΞΕΩΝ ΤΗΝ ΕΠΙΔΡΑΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΣΤΟΝ ΑΝΘΡΩΠΟ, ΣΤΗΝ ΚΟΙΝΩΝΙΑ ΚΑΙ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ. ΠΑΡΑΛΛΗΛΑ, ΠΡΩΤΑΓΩΝΙΣΤΕΣ ΤΟΥ ΚΛΑΔΟΥ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΣΤΗΝ ΚΥΠΡΟ ΜΑΣ ΠΑΡΟΥΣΙΑΖΟΥΝ ΤΙΣ ΚΑΙΝΟΤΟΜΕΣ ΥΠΗΡΕΣΙΕΣ ΚΑΙ ΤΑ ΠΡΟΪΟΝΤΑ ΠΟΥ ΠΑΡΕΧΟΥΝ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ ΣΤΟΥΣ ΚΑΤΑΝΑΛΩΤΕΣ.

ΧΟΡΗΓΟΣ





ΔΙΑΣΦΑΛΙΖΟΝΤΑΣ ΤΟ ΜΕΛΛΟΝ ΤΩΝ ΟΡΓΑΝΙΣΜΩΝ

Η ΡΑΓΔΑΙΑ ΑΥΞΗΣΗ ΤΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΣΤΗΝ ΚΥΠΡΟ, ΜΕΣΑ ΑΠΟ ΤΑ ΜΑΤΙΑ ΤΩΝ ΕΙΔΙΚΩΝ

Ενώ η αύξηση των κυβερνοεπιθέσεων αποτελεί ένα παγκόσμιο φαινόμενο με σοβαρές επιπτώσεις σε διάφορους τομείς της οικονομίας αλλά και της κοινωνίας στο σύνολό της, η Κύπρος δεν αποτελεί εξαίρεση, με τις κυβερνοεπιθέσεις στο νησί να αυξάνονται ραγδαία το τελευταίο εξάμηνο. Κι ενώ διάφορα περιστατικά έχουν έρθει στο φως της δημοσιότητας προκαλώντας ανησυχία στους οργανισμούς, υπάρχουν ακόμη πολλές περιπτώσεις που δεν έχουν γίνει γνωστές, σε τοπικό και σε παγκόσμιο επίπεδο.

Η αύξηση σε αριθμούς

Σύμφωνα με το Security Operation Center της Odyssey, το οποίο εδώ και 20 χρόνια παρέχει υπηρεσίες Managed Detection and Response και εξυπηρετεί πελάτες 24 ώρες το 24ωρο, 7 ημέρες τη εβδομάδα, και 365 ημέρες τον χρόνο από όλες τις γεωγραφικές περιοχές του κό-

σμου, οι πρόσφατες στατιστικές αναφορές για την κυβερνοασφάλεια στην Κύπρο αναδεικνύουν ανησυχητικές τάσεις και σημαντική αύξηση σε ορισμένους τύπους κυβερνοεπιθέσεων κατά το τελευταίο εξάμηνο. Σύμφωνα με τον Αντώνη Πράγκα, Assistant Manager Managed Detection & Response της Odyssey, προβλέπεται ότι αυτή η ανοδική τάση θα συνεχιστεί και θα ενταθεί, υπογραμμίζοντας την επείγουσα ανάγκη για ισχυρά μέτρα κυβερνοασφάλειας προκειμένου να προστατευθούν οι οργανισμοί από επερχόμενες απειλές.

Συγκεκριμένα, οι επιθέσεις με την μεγαλύτερη αύξηση το τελευταίο εξάμηνο στην Κύπρο είναι οι επιθέσεις τύπου Ransomware που έχουν αυξηθεί κατά 125%, προκαλώντας αναστάτωση στις επιχειρήσεις καθώς κρυπτογραφούν κρίσιμα δεδομένα και ζητούν λύτρα, απειλώντας με διαρροή στο dark web. Η δεύτερη πιο ανησυχητική αύξηση κατά 101% αφορά τις δραστηριότητες που σχετίζο-

νται με τη μη εξουσιοδοτημένη χρήση λογισμικού, που οφείλεται στη μεγάλη επιτυχία των επιθέσεων στην εφοδιαστική αλυσίδα, είτε μέσω τρίτων προμηθευτών είτε μέσω χρηστών με πρόσβαση σε συστήματα ενός οργανισμού. Τέλος, οι επιθέσεις Man-in-the-Middle (MITM) έχουν επίσης αυξηθεί κατά 58% και αποτελούν μια παραδοσιακή μέθοδο επίθεσης, καθώς ο επιτιθέμενος εισβάλλει στην επικοινωνία και παραβιάζει την ασφάλεια των δεδομένων που ανταλλάσσονται.

Πίσω από την ραγδαία αύξηση

Οι λόγοι πίσω από την ραγδαία αυτή αύξηση οφειλονται στην νέα ψηφιακή εποχή που μαζί με τα ωφέλη που προσφέρει, συνοδεύεται -όπως και κάθε αλλαγή- και με προκλήσεις που δεν είναι άλλες από τα ψηφιακά ρίσκα, τα οποία καλούνται να αντιμετωπίσουν οι οργανισμοί. Βασικοί παράγοντες τονίζει ο Ανδρέας Κωνσταντινίδης, Manager Professional Services, της Odyssey

αποτελούν ο ψηφιακός μετασχηματισμός, η μεταφορά στο cloud καθώς και το μοντέλο υβριδικής εργασίας, τα οποία έχουν αλλάξει το ψηφιακό μας οικοσύστημα, επεκτείνοντας την ψηφιακή μας περιμετρο προκαλώντας έτσι αναπόφευκτα, νέα σημεία ευπάθειας. Αυτό έχει δημιουργήσει ένα πιο επικίνδυνο και διευρυμένο τοπίο απειλών, προσφέροντας νέες ευκαιρίες για τους hackers, καθιστώντας όλους τους οργανισμούς πιθανούς στόχους, ανεξαρτήτου μεγέθους και τομέα δραστηριότητας.

Πως μπορούν να προστατευτούν οι οργανισμοί

Η κυβερνοασφάλεια δεν είναι μόνο θέμα που αφορά το τμήμα πληροφορικής αλλά πρέπει να εντάσσεται στην γενική στρατηγική των οργανισμών. Η μεγαλύτερη πρόκληση που έχει να αντιμετωπίσει η χώρα μας, τονίζει ο Στέλιος Χαραλάμπους, Manager, Advisory Services, της Odyssey, είναι η άγνοια στην ανώτερη διοίκηση πολλών οργανισμών τόσο της σημαντικότητας ύπαρξης στρατηγικής για την κυβερνοασφάλεια όσο και για τον αποτελεσματικό τρόπο προσέγγισης της.

Είναι σημαντικό να κατανοήσουμε ότι η κυβερνοασφάλεια δεν αφορά μόνο την εφαρμογή μιας ενιαίας τεχνολογίας ή τη διεξαγωγή εκπαιδευτικών σεμιναρίων. Χωρίς 24ωρη παρακολούθηση, οι οργανισμοί δεν μπορούν να γνωρίζουν εάν δέχονται επίθεση ή εάν η ασφάλεια των δεδομένων τους διακυβεύεται. Είναι σημαντικό να υπάρχουν συστήματα και διαδικασίες που μπορούν να ανιχνεύουν και να ανταποκρίνονται σε απειλές σε πραγματικό χρόνο.

Επομένως για να μπορέσει μια στρατηγική να είναι αποτελεσματική και εφαρμόσιμη θα πρέπει να βασίζεται σε όλες τις λειτουργικές πτυχές του οργανισμού: Άνθρωποι, Διαδικασίες και Τεχνολογία. Το ευρύ φάσμα υπηρεσιών και λύσεων που προσφέρουμε στην Odyssey σε συνδυασμό με τα 20 χρόνια εμπειρίας μας στον τομέα

της κυβερνοασφάλειας, έχουν ως στόχο, συνδυαστικά, να μπορούμε να παρέχουμε τις απαραίτητες λύσεις που θα επιτρέψουν την αποτελεσματική διαχείριση των ψηφιακών κινδύνων.

Odyssey, ο στρατηγικός σας συνεργάτης στην κυβερνοασφάλεια

Η Odyssey, για περισσότερες από δύο δεκαετίες αποτελεί ηγέτη στον τομέα της Κυβερνοασφάλειας υποστηρίζοντας οργανισμούς παγκοσμίως δίνοντας τη δυνατότητα να μπορούν να προβλέπουν, να ανταποκρίνονται, να ανακρίπτονται γρήγορα και να προσαρμόζονται σε αναδυόμενες απειλές και ευπάθειες που υπάρχουν στο επεκτεινόμενο και απρόβλεπτο τοπίο απειλών.

Η ολιστική προσέγγιση της Odyssey συνδυάζει την πλατφόρμα ClearSkies™, Managed Detection & Response (MDR), Advisory Services, Integrated Solutions και Cloud Security. Κάθε ένας από τους πέντε πυλώνες, είτε σε συνδυασμό μεταξύ τους είτε ο καθένας μόνος του, στηρίζει τους οργανισμούς να εξελιχθούν με ασφάλεια στην ψηφιακή εποχή και να διαφυλάξουν την επιχειρησιακή τους συνέχεια.

Η εταιρεία είναι επίσης πιστοποιημένη με ISO 27001, ISO 9001, ISO 22301 και SOC 2@ Type 2, καθώς και διαπιστευμένη ως Qualified Security Assessor (QSA) από το Payment Card Industry Security Standards Council. Η Odyssey έχει λάβει πολυάριθμα διεθνή βραβεία και διακρίσεις και έχει αναγνωριστεί από την Gartner, στο Magic Quadrant του 2021, για το προϊόν της ClearSkies™, ως ένα από τα 20 καλύτερα παγκοσμίως στην κατηγορία Security Information and Event Management. Παράλληλα, έχει διακριθεί ανάμεσα στις κορυφαίες εταιρείες στον κόσμο όσον αφορά το καλύτερο εργασιακό περιβάλλον, με το πιστοποιητικό Great Place to Work, για τρία συνεχή έτη.





WE EMPOWER YOU TO BUILD A CYBER RESILIENT ORGANIZATION



20+

years of
experience & expertise

32+

countries with
trusted customers

150+

highly skilled
professionals

4.

offices in Cyprus (HQ),
Greece, MENA, UK



The attack surface is expanding and evolving at a much faster pace than ever before. As organizations become more and more reliant on technology and third-party technology providers, the complexity and dependency on the IT ecosystem are significantly increasing. It's a matter of time before an organisation suffers from a breach, which might result in data loss, systems outages and reputational damage.

This is why organizations need to shift from a cyber defence posture to a cyber resilient position to be able to anticipate, withstand, adapt to adverse conditions and quickly recover from disruptive attacks.

Cybersecurity is no longer a technology issue; it's a business issue.

To address this challenge, cybersecurity is becoming a critical part of the board's agenda and is being integrated into the organization's overall business strategy.

It's time to revisit and rethink your Cybersecurity Strategy.

Eleftherios Antoniadou
Founder & CTO, Odyssey