τα κενά ασφαλείας που ανακάλυψαν στην πορεία. Μόλις το 13% των οργανισμών δηλώνουν ευχαριστημένοι με το καθεστώς ασφαλείας των cloud τους ενώ το 43% των οικονομικών οργανισμών και το 39% όσων συμπεριλαμβάνουν e-commerce λειτουργίες ομολογούν ότι αντιμετωπίζουν μεγάλες καθυστερήσεις ανάμεσα στις ειδοποιήσεις, την αξιολόγηση και την αντιμετώπιση απειλών, (mean time to detection -MTTD) οι οποίες τους κοστίζουν ιδιαίτερα και όχι μόνο σε χρήμα αλλά και αξιοπιστία και πελατολόγιο.

Από την «τέλεια» καταιγίδα στην κιβωτό

Και όλο αυτό συμβαίνει με το τέλειο timing. Όταν ο ανταγωνισμός στον αγώνα δρόμου για τον ψηφιακό μετασχηματισμό δεν επιτρέπει σε κανέναν να «παγώσει» ή να αναστείλει -πόσο μάλλον να ακυρώσει- το cloud deployment, για να το ξαναδεί με την διάσταση της ασφάλειας στις βασικές συνιστώσες του. Και καθώς η διαλειτουργικότητα των APIs και των υβριδικών cloud αρχιτεκτονικών είναι πλέον βασικοί enablers σε σχεδόν κάθε κομμάτι της επιχειρηματικότητας. Γι' αυτό η «by design» και εξαρχής πρόβλεψη για την ασφάλεια στο cloud προκύπτει τώρα ιδιαίτερα σημαντική και μάλιστα σε κάθε κύκλο της ανάπτυξης στο υπολογιστικό νέφος. Στη σχεδίαση της στρατηγικής μετάβασης σε αυτό, στην υλοποίηση, στην προσαρμογή, στην ανάπτυξη χάρη σε αυτό και στη συνεχή βελτιστοποίηση της. Γιατί η μέχρι τώρα εμπειρία έδειξε ότι τα εργαλεία ασφαλείας δεν μπορούν να προστεθούν αργότερα «αν -όταν και εφόσον» προκύψει πρόβλημα. Τουλάχιστον όχι με τρόπο πραγματικά αποδοτικό.

Σε ένα επιχειρηματικό περιβάλλον όπου όλο και συχνότερα οι όροι «virtual machines» και «serverless

ΟΙ «ΠΡΟΓΝΩΣΕΙΣ» ΓΙΑ ΤΟ ΕΛΛΗΝΙΚΟ ΝΕΦΟΣ

Τις παραπάνω ανάγκες επιβεβαιώνουν στελέχη και στο ελληνικό επιχειρηματικό περιβάλλον. Το netweek απευθύνθηκε στην εμπειρία στελεχών στις δύο πλευρές του προβλήματος- την κυβερνοασφάλεια και το cloud αντίστοιχα- και οι απαντήσεις τους είναι διαφωτιστικές.



Γιάννης Ηλιάδης Διευθυντής Υποδομών Πληροφορικής, Τειρεσίας Α.Ε. Πρόεδρος Επιτροπής Ελέγχου, ISC2 Hellenic Chapter

ΤΟ ΒΛΕΜΜΑ ΣΤΑ ΣΥΝΝΕΦΑ, ΤΑ ΠΟΔΙΑ ΣΤΗ ΓΗ

Η Gartner είχε δίκιο, για ακόμη μία φορά. Οι ταχύτατες ψηφιακές εξελίξεις των τελευταίων πέντε ετών οδήγησαν πολλές οικογένειες Cloud-only προϊόντων στις τελευταίες δύο φάσεις του Gartner Hype Cycle (καμπύλη διαφώτισης, επίπεδο παραγωγικότητας). Τώρα πια, γνωρίζουμε. Βάσει διεθνών μελετών των τελευταίων μηνών, το 76% των οργανισμών αυξάνουν τους προϋπολογισμούς για ασφάλεια SaaS (CSA), ενώ το 96% των οργανισμών εκφράζουν ανησυχία για την ασφάλεια στο δημόσιο Cloud (ISC2). Γίνονται οι οργανισμοί πιο ανθεκτικοί στις επιθέσεις ή καλλιεργούν μια ψευδαίσθηση ασφάλειας; Αναλύουμε σε πέντε πυλώνες.

- **Πυλώνας 1:** Υψηλή εμπιστοσύνη, χαμηλή ετοιμότητα; Το 79% των οργανισμών θεωρεί επαρκές το σύνολο των μέτρων ασφάλειας SaaS που έχουν λάβει (CSA) [1], ενώ μόλις το 4% των οργανισμών διαθέτει ώριμη ετοιμότητα να αντιμετωπίσει τους τρέχοντες κυβερνοκινδύνους που προέρχονται από το Cloud (Cisco).
- **Πυλώνας 2:** Χάσμα δεξιοτήτων, όχι πλήθους επαγγελματιών. Το κύριο πρόβλημα δεν είναι πλέον η έλλειψη προσωπικού, αλλά η έλλειψη κρίσιμων δεξιοτήτων (ISC2) [2], καθώς το 59% των οργανισμών δηλώνει σοβαρές ελλείψεις δεξιοτήτων στους τομείς ασφάλειας Cloud και Τεχνητής Νοημοσύνης. Στην Ελλάδα, ο συνήθης τρόπος κάλυψης του κενού αυτού είναι η εξωτερική βοήθεια (outsourcing, team augmentation κτλ).
- **Πυλώνας 3:** Το Cloud ως γεννήτρια νέων απειλών. Το Cloud αποτέλεσε την αναγκαία συνθήκη για παγκόσμια αξιοποίηση της Τεχνητής Νοημοσύνης. Το 42% των οργανισμών έχει βιώσει επιθέσεις κοινωνικής μηχανικής βελτιστοποιημένες με Τεχνητή Νοημοσύνη (Cisco) [3], ενώ μόνο το 34% των οργανισμών προλαβαίνουν να διορθώνουν τις ευπάθειες του λογισμικού που αναπτύσσεται με GenAI (Palo Alto).
- **Πυλώνας 4:** Το Cloud ως καταλύτης ωρίμανσης μέτρων ασφάλειας. Το Cloud επιτάχυνε την ανάπτυξη της ομομορφικής κρυπτογράφησης (Cloud Security Alliance) [5] δίνοντας δυνατότητες συνεπεξεργασίας δεδομένων με διατήρηση της ιδωτικότητάς τους. Η ραγδαία αύξηση 41% σε επιθέσεις προς APIs (Palo Alto) [4] προερχόμενες από Cloud (agentic AI) οδήγησε κανονιστικούς φορείς στην έκδοση σχετικών οδηγιών προστασίας (NIST SP 800-228). Επιπρόσθετα, η αύξηση του attack surface λόγω Cloud έχει οδηγήσει στη δημιουργία ελάχιστων απαιτούμενων ρυθμίσεων ασφάλειας (π.χ. CISA ScuBA) και δημιούργησε την νέα κατηγορία μέτρων ασφαλείας CNAPP [7], τα οποία συνοψίζουν το επίπεδο ασφάλειας των Cloud tenants (IaaS/PaaS) και διαχειρίζονται κεντρικά τα επιμέρους μέτρα ασφαλείας.
- **Πυλώνας 5:** Το Cloud και τα ευρωπαϊκά κανονιστικά πλαίσια. Τον Νοέμβριο 2025, οι ευρωπαϊκοί εποπτικοί φορείς EBA, EIOPA, ESMA όρισαν τους κύριους Cloud Providers ως «κρίσιμους τρίτους παρόχους» για τον ευρωπαϊκό χρηματοπιστωτικό τομέα, εντάσσοντάς τους πλέον στο Ευρωπαϊκό πλαίσιο άμεσης εποπτείας DORA και υποχρεώνοντάς τους σε ενισχυμένο εποπτικό καθεστώς.

Συμπέρασμα: Η σύγχρονη ασφάλεια Cloud επιτάσσει να διαμορφώνουμε τα σωστά επίπεδα εμπιστοσύνης στα μέτρα ασφάλειας που υιοθετούμε, να επενδύουμε στην ανάπτυξη σχετικών δεξιοτήτων των αρμόδιων στελεχών, να παραμένουμε σε επαγρύπνηση για τις νέες απειλές που γεννώνται μέσα στους κόλπους του Cloud, να αξιοποιούμε στο έπακρο τα νέα μέτρα ασφάλειας που δημιουργούνται χάριν του Cloud και να είμαστε ενήμεροι για τις μεταβαλλόμενες υποχρεώσεις που απορρέ-

functions» ακούγονται στις αίθουσες συσκέψεων ανώτερων στελεχών και η «ευζωία» των data ταυτίζεται με αυτή των οργανισμών τους το «αργότερα» συνήθως πλησιάζει επικίνδυνα το «πολύ αργά». Δεν είναι ζήτημα απόφασης, αλλά καθαρά ρυθμού εξέλιξης των διαδικασιών που εξελίσσονται και αυτοματοποιούνται με ταχύτητες που δεν είχαμε ξαναδεί.

Η Gartner επιβεβαιώνει τις ανάγκες που το cloud δημιουργεί για «by design» εργαλεία κυβερνοασφάλειας και στην έκθεση της με τίτλο « Market Guide for Cloud-Native Application Protection Platforms» που δημοσιεύθηκε το περασμένο καλοκαίρι προβλέπει ότι το πρόβλημα της ασφάλειας στο cloud ενεργοποιεί την σχετική αγορά cloud-native application protection platforms (CNAPP). Έτσι προβλέπει ότι ως το 2029, το 40% των οργανισμών που εφαρμόζουν επιτυχημένα zero trust λειτουργία στις υπηρεσίες τους σε περιβάλλοντα cloud θα εξαρτώνται απόλυτα από τις ικανότητες ελέγχου και παρακολούθησης των CNAPP, ενώ στο ίδιο διάστημα πάνω από τις μισές επιχειρήσεις θα λειτουργούν σε containers που θα κάνουν απαραίτητα ενισχυμένα και ενοποιημένα πρωτόκολλα ασφαλείας για εφαρμογές, αλλά και αποθήκευση δεδομένων στο cloud.

Αυτό που μάλιστα τονίζει η έκθεση είναι ότι αυτό δεν αφορά μόνο τις multicloud ή της «εκ του προχείρου» στρατηγικές, αλλά φαίνεται πως κάθε υλοποίηση κάποιας cloud στρατηγικής αργά ή γρήγορα έρχεται αντιμέτωπη με το ζήτημα της ασφάλειας, ανεξαρτήτως μάλιστα provider, αν και όπως αναφέρει κάποιοι προσφέρουν καλύτερα security control panels, dashboards και δυναμικό reporting από άλλους. Τα οποία γίνονται ζωτικής σημασίας ειδικά για μεγάλες επιχειρήσεις που κληρονομούν ανομοιογενείς υποδομές μετά από συγχωνεύσεις και εξαγορές.

ουν από κανονιστικά πλαίσια και εποπτικούς φορείς. Καθώς ετοιμαζόμαστε να αντιμετωπίσουμε τις αυριανές απειλές, πρέπει να επιβεβαιώνουμε συνεχώς ότι δεν χρησιμοποιούμε χθεσινά όπλα. Η αιθεροβασία των πρώτων ετών αξιοποίησης Cloud (την περίοδο Covid) έχει παρέλθει ανεπιστρεπτί. Το Cloud είναι η νέα πραγματικότητα και το βλέμμα μας πρέπει να είναι στραμμένο προς αυτό. Όμως τα πόδια μας πρέπει να πατούν γερά στη Γη.



Πέτρος Λιβάνιος, Cloud Platform Manager, Coca-Cola HBC

«CLOUD SECURITY BY DESIGN: ΒΑΖΟΝΤΑΣ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΣΧΕΔΙΑΣΜΟ ΑΠΟ ΤΗΝ ΑΡΧΗ»

Η μετάβαση στο cloud έχει πλέον περάσει από τη φάση της επιλογής στη φάση της αναγκαιότητας. Παρόλα αυτά, η επιτυχία ενός cloud migration δεν κρίνεται μόνο από την τεχνική υλοποίηση, αλλά κυρίως από τον τρόπο που ενσωματώνεται η ασφάλεια στη συνολική αρχιτεκτονική. Το "security by design" δεν είναι πια αρχή· είναι πρακτική που καθορίζει την ανθεκτικότητα και τη βιωσιμότητα ενός οργανισμού.

Οι μεγαλύτεροι κίνδυνοι σε ένα cloud migration προέρχονται συχνά από ανθρώπινες παραδοχές και όχι από την ίδια την τεχνολογία. Η λάθος εντύπωση ότι το cloud "είναι από μόνο του ασφαλές" οδηγεί σε κενά: ανεπαρκή μοντέλα πρόσβασης, μη ενεργοποιημένες πολιτικές, ανεπαρκές logging και αδύναμη διακυβέρνηση. Σε ένα περιβάλλον όπου οι υπηρεσίες πολλαπλασιάζονται γρήγορα, οποιαδήποτε αμέλεια επεκτείνεται και γίνεται κίνδυνος μεγάλης κλίμακας.

Ένας δεύτερος κρίσιμος παράγοντας είναι η πολυπλοκότητα. Αρχιτεκτονικές που συνδυάζουν πολλαπλά επίπεδα – όπως multi-cloud ή υβριδικά περιβάλλοντα με on-premise τεχνολογίες – παρουσιάζουν αυξημένους κινδύνους, επειδή απαιτούν συνεπή πολιτική ασφαλείας και συνεχή εναρμόνιση κανόνων. Η ετερογένεια αυτών των μοντέλων δυσκολεύει τη διαχείριση ταυτοτήτων, τον έλεγχο πρόσβασης και την τυποποίηση ασφαλιστικών μέτρων. Αντίθετα, όσο πιο ενιαίο και κεντρικοποιημένο είναι το μοντέλο, τόσο πιο εύκολο είναι να επιβληθούν σταθερές αρχές ασφαλείας.

Παράλληλα, η λανθασμένη ή ανεπαρκής κατανόηση του shared responsibility model συνεχίζει να αποτελεί πηγή κινδύνων. Πολλοί οργανισμοί υποτιμούν ότι σημαντικό μέρος της προστασίας – από την ταυτοποίηση χρηστών μέχρι την παρακολούθηση και την ανάκτηση δεδομένων – παραμένει δική τους ευθύνη. Η σύγχυση αυτή δημιουργεί αδύναμα σημεία που μπορεί να αξιοποιηθούν από επιτιθέμενους. Σήμερα, πρακτικές όπως identity-first security και Zero Trust έχουν γίνει πλέον αυτονόητες. Δεν αποτελούν "προχωρημένη στρατηγική", αλλά τη βάση κάθε σύγχρονης αρχιτεκτονικής. Η πραγματική αξία και διαφοροποίηση βρίσκεται πλέον στα επόμενα επίπεδα.

- Τυποποίηση και αυτοματοποίηση: Η αυτοματοποίηση παίζει αποφασιστικό ρόλο στη μείωση των κινδύνων. Όταν τα πάντα – από την ανάπτυξη υποδομών έως την εφαρμογή πολιτικών ασφαλείας – υλοποιούνται μέσω Infrastructure as Code, μειώνονται τα λάθη, αυξάνεται η ταχύτητα και η ασφάλεια γίνεται μέρος του ίδιου του lifecycle. Χωρίς αυτοματοποίηση, κάθε κενό διαχείρισης αργά ή γρήγορα θα δημιουργήσει πρόβλημα.
- Ενιαίο governance και συνεχής ορατότητα: Σε σύνθετες αρχιτεκτονικές, το μεγαλύτερο ρίσκο είναι η ασυνέχεια. Ενιαίες πολιτικές tagging, παρακολούθησης, logging και cost control βοηθούν να υπάρχει καθαρή εικόνα σε πραγματικό χρόνο. Όσο πιο πολυδιάστατο είναι το περιβάλλον – εφαρμογές, βάσεις, data services, AVS, containers – τόσο πιο απαραίτητο γίνεται ένα governance μοντέλο που δεν βασίζεται στην "καλή θέληση", αλλά σε συγκεκριμένους κανόνες που εφαρμόζονται με συνέπεια.
- Ενσωματωμένη ανθεκτικότητα από την πρώτη μέρα: Backup, cyber-resilience και disaster recovery δεν πρέπει να μπαίνουν "μετά". Η εμπειρία δείχνει ότι όταν η ανθεκτικότητα σχεδιάζεται εξαρχής, μειώνονται τα ρίσκα, οι χρόνοι αποκατάστασης και το λειτουργικό κόστος. Η ύπαρξη αυτοματοποιημένων μηχανισμών ανάκτησης και προστασίας δεδομένων διασφαλίζει ότι ο οργανισμός μπορεί να συνεχίσει τη λειτουργία του ακόμη και σε συνθήκες κρίσης.

Τελικά, η ασφάλεια στο cloud δεν είναι ένα έργο που τελειώνει. Είναι μια κουλτούρα. Όσο νωρίτερα θεμελιωθεί, τόσο πιο σταθερή και ασφαλής είναι η βάση πάνω στην οποία αναπτύσσεται ο οργανισμός. **NW**