CONNECTED SECURITY

Δυναμική και Προσαρμόσιμη Ασφάλεια σε περιβάλλον Multicloud

*Άρθρο του **Σταύρου Καραγκιούλογλου**, Dipl.-Ing*
Managing Partner United-Telecom AE-
Partner Juniper Networks
e-mail: s.kara@united-telecom.gr

Οι σύγχρονες επιχειρήσεις ανταγωνίζονται μέσω των δυνατοτήτων που τους προσφέρει η χρήση των κινητών και διαδικτυακών εφαρμογών που χρησιμοποιούν για B2C ή B2B. Η ανάγκη για γρήγορο ρυθμό ανάπτυξης ή και βελτιστοποίησης των εφαρμογών, ασκεί τεράστια πίεση στις ομάδες πληροφορικής καθώς σχεδόν όλοι θεωρούν ότι αυτές οι απαιτήσεις μπορούν να ικανοποιηθούν άμεσα αν όχι και ακαριαία.

Παλαιότερα, οι ομάδες πληροφορικής δημιουργούσαν εφαρμογές βάσει έργου και οι όποιες εγκαταστάσεις σχεδιάζονταν και υλοποιούνταν για βδομάδες ή και μήνες ενώ οι όποιες αναβαθμίσεις ήταν νέα έργα και γίνονταν σπανιότερα, ίσως π.χ. μία φορά το χρόνο.

Αυτή η προσέγγιση όμως δεν μπορεί να λειτουργήσει πλέον όταν μια εφαρμογή θεωρείται δεδομένο ότι θα πρέπει να παραμένει διαθέσιμη, αποτελεσματική και ασφαλής ενώ παράλληλα και ταυτόχρονα θα πρέπει να ενημερώνεται πολύ πιο συχνά - σε ορισμένες περιπτώσεις ακόμα και αρκετές φορές την ημέρα!

Η φύση των σύγχρονων εφαρμογών και η ευέλικτη διαδικασία ανάπτυξής τους απαιτούν συχνά on-demand επέκταση και βελτιστοποίηση της χωρητικότητας στις πλατφόρμες υπολογιστών που τις υποστηρίζουν/φιλοξενούν. Αυτό αυτομάτως σημαίνει τη δημιουργία ενός πλήρους συνόλου υποκείμενων υπηρεσιών συνδεσιμότητας δικτύου που χρειάζονται οι εφαρμογές με αμεσότητα, με ευελιξία πλατφορμών και πρωτίστως με δυναμική ασφάλεια ανά πάσα στιγμή.

Τα παραπάνω οδήγησαν στην ανάδειξη νέων υποδομών με δυναμική και προσαρμόσιμη ασφάλεια σε περιβάλλον Multicloud. Η εικόνα 1 δείχνει ένα τέτοιο περιβάλλον.

Η πρόκληση

Στα παραδοσιακά συστήματα, οι πολιτικές α-

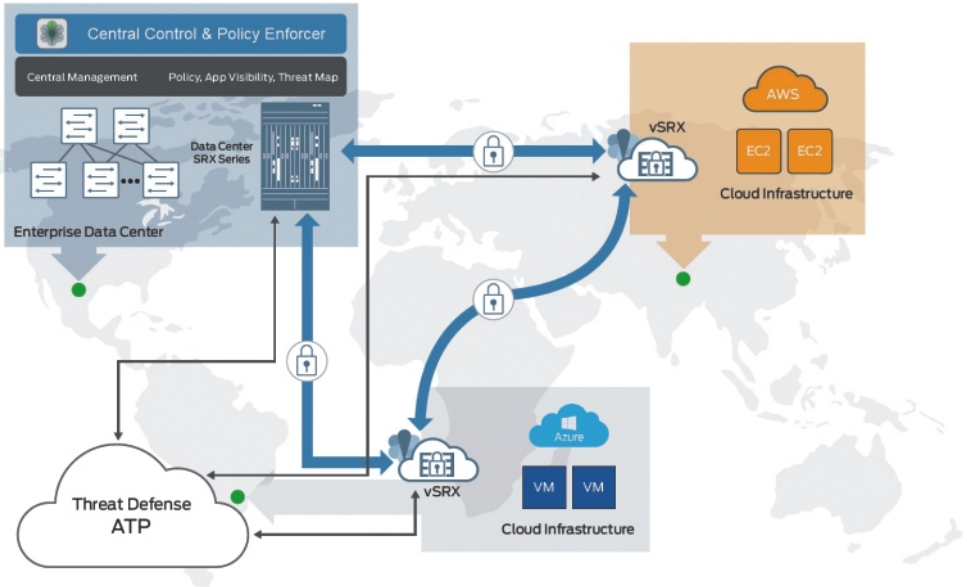
σφάλειας δεν προσαρμόζονται δυναμικά στις συνεχώς μεταβαλλόμενες απαιτήσεις ασφάλειας των εργασιακών ροών. Εξαιτίας αυτού οι πολιτικές αυτές πρέπει να διαμορφώνονται και να προσαρμόζονται για κάθε πιθανή δυνατότητα ανάπτυξης ξεχωριστά και χειροκίνητα στις φυσικές, private και public cloud υποδομές.

Οι παραδοσιακές πολιτικές firewall που βασίζονται σε μεγάλο βαθμό στις διευθύνσεις IP, δεν έχουν υποστεί κάποια σημαντική βελτίωση εδώ και μια δεκαετία και δυστυχώς, δεν είναι πλέον και πολύ αποτελεσματικές στο σημερινό cloud κόσμο που χρησιμοποιεί εκτεταμένα το cloud ή ταυτόχρονα και πολλά cloud (Multicloud). Στην νέα εποχή της πληροφορικής οι διευθύνσεις IP αλλάζουν, δημιουργούνται και τερματίζονται συνεχώς καθώς ακολουθούν τον κύκλο ζωής των δυναμικών ιδεατών υπολογιστικών οντοτήτων (dynamic virtual instances).

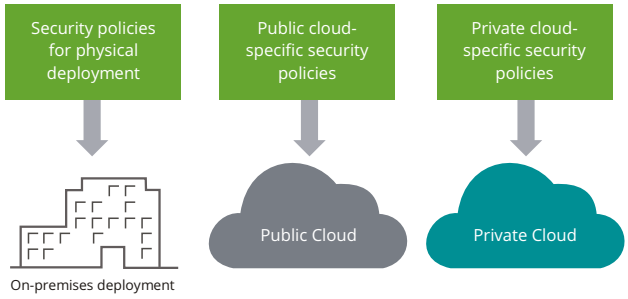
Ως συνέπεια της κατάστασης αυτής, για να διαχειριστούν οι επιχειρήσεις τις προκλήσεις ασφάλειας της εποχής του Multicloud, πρέπει να μπορούν να προσαρμόζουν δυναμικά τις πολιτικές ασφαλείας σε διαφορετικά workflows και επιλογές ανάπτυξης, χρησιμοποιώντας ένα μοναδικό και ενιαίο αλλά ευέλικτο μοντέλο πολιτικής Multicloud.

Επιπλέον, κάθε περιβάλλον cloud έχει τα δικά του δομικά στοιχεία, όπως π.χ. στα Amazon Web Services (AWS) ή στο VMware NSX που χρησιμοποιούν σημάνσεις (tags) είναι δύσκολο αυτές να ενσωματωθούν στις πολιτικές των κλασικών firewalls χρησιμοποιώντας παραδοσιακές διαδικασίες και εργαλεία. Το αποτέλεσμα είναι ότι για πρακτικούς λόγους ή και για λόγους ταχύτητας η ευελιξία και η ασφάλεια των επιχειρήσεων περιορίζεται ξοδεύοντας χρόνο και πόρους για ειδικές κατασκευές κάθε φορά. Η εικόνα 2 δείχνει ακριβώς αυτόν τον κατακερματισμό των πολιτικών ασφάλειας.

Ο στατικός και ανελαστικός χαρακτήρας των μέτρων και των ενεργειών πολιτικής ασφάλειας είναι άλλη μία πρόκληση στην αποτελεσματική ανταπόκριση σε διαφορετικά workflows ασφάλειας. Στις παραδοσιακές πολιτικές firewall, όταν το δίκτυο δέχεται επίθεση, ο διαχειριστής ασφαλείας πρέπει κυριολεκτικά να κοσκινίσει χιλιάδες κανόνες, απενεργοποιώντας τους περιττούς, ώστε να απομονώσει την πηγή του συμβάντος. Ομοίως, χρειάζεται να πειραματιστεί με ρυθμίσεις πολιτικής που θα καθορίζουν το καλύτερο δυνατό επίπεδο ασφάλειας ώστε να επιτυγχάνονται συνθήκες συγκεκριμένης απόδοσης δικτύου, τις οποίες θα αλλάζει ανάλογα με



Εικόνα 1: Ασφαλές Δίκτυο σε περιβάλλον Multicloud με ενιαία τεχνολογία NGFW παντού



Εικόνα 2: Ο κατακερματισμένος τρόπος: Οι πολιτικές ασφαλείας εφαρμόζονται ξεχωριστά ανά τομέα υποδομής

τις επιχειρηματικές ανάγκες.

Η χειροκίνητη πραγματοποίηση αυτών των αλλαγών σε μια μεγάλη βάση κανόνων και μάλιστα σε ένα κατακερματισμένο περιβάλλον είναι χρονοβόρα και εξαιρετικά αναποτελεσματική - δεν είναι δε καθόλου ιδανική για άμεσες λύσεις ή επαναλαμβανόμενες καταστάσεις.

Λύση: Πολιτικές Ασφαλείας Χρηστών

Όταν ένα δίκτυο δέχεται επίθεση, η ανάγκη για ταχεία απομόνωση της απειλής και η λήψη διορθωτικών μέτρων είναι κρίσιμη και απαιτείται μία λύση με ισχυρά ασφαλή workflows. Μια τέτοια λύση μπορεί υλοποιηθεί χρησιμοποιώντας δυναμικές ομάδες πρόσβασης (Dynamic Access Group - DAG) που αποτελεί ένα ενοποιημένο και «διαισθητικό» μοντέλο πολιτικής κάνοντας χρήση των Metadata. Αυτή η λύση μπορεί να μεταφερθεί σε όλα τα συστήματα στο φυσικό Data Center και στα Clouds, δίνοντας στους διαχειριστές ασφαλείας την πλήρη εικόνα όλων των υποδομών και συνολικό έλεγχο των λειτουργιών και των εφαρμογών στο Multicloud.

Οι προκλήσεις που περιγράφονται πιο πάνω μπορούν να αντιμετωπιστούν με μία ολοκληρωμένη λύση Πολιτικών Ασφάλειας Χρηστών, που αναπτύσσει πολιτικές ασφάλειας με βάση τα Metadata που προέρχονται από το δίκτυο και έχει ισχυρές δυνατότητες και ικανότητες δυναμικής δράσης και επέμβασης.

Η λύση αυτή περιλαμβάνει κατά κανόνα τα ακόλουθα δύο στοιχεία:

- Software Defined Services Gateway (φυσικό ή ιδεατό μηχάνημα) με ενσωματωμένο τείχος προστασίας επόμενης γενιάς (NGFW), με Unified Threat Management (UTM), με προστασία από Zero-Day Attacks, με Advanced Threat Protection (ATP) και με Role Based Access Control (RBAC).
- Centralized Policy Management και σύστημα επιβολής πολιτικών (Policy Enforcer).

Αυτή η υποδομή εξασφαλίζει:

- Ολική λειτουργικότητα firewall με IPsec/SSL-VPN και πλούσιες υπηρεσίες δικτύωσης όπως Network Address Translation (NAT) και routing
- Intrusion Prevention System (IPS) για ανίχνευση και αποκλεισμό εισβολών στο δίκτυο
- Εφαρμογή προστασίας βάσει ρόλου των χρηστών με σκοπό την ανάλυση, καταγραφή και επιβολή ελέγχου πρόσβασης βάσει των χαρακτηριστικών των ρόλων ή και βάσει των ομάδων χρηστών
- Έλεγχο εφαρμογών και ορατότητα με ενσωματωμένο Application Security που παρέχει ανάλυση σε επίπεδο εφαρμογής, ιεράρχηση και αποκλεισμούς για επωφελή χρήση των εφαρμογών
- Antivirus, antispam, Web και content filtering με UTM για προστασία από ιούς, ανεπιθύμητα μηνύματα, κακόβουλα URL και βλαβερό περιεχόμενο
- Προσαρμοστικότητα σε όλα τα cloud περιβάλλοντα για λειτουργικά Linux KVM, VMware, AWS και Azure πλατφόρμες
- Κεντροποιημένη, ολική διαχείριση για ανάπτυξη, παρακολούθηση και διαμόρφωση λειτουργιών ασφαλείας και πολιτικών σε όλες τις φυσικές και ιδεατές μορφές firewall στο δίκτυο (Centralized Policy Management)
- Κεντροποιημένη νοημοσύνη για την ανάπτυ-

ξη και επιβολή πολιτικών ασφαλείας στις υποδομές δικτύου (Policy Enforcement)

- Λεπτομερείς αναλύσεις, χάρτες απειλών και αρχεία καταγραφής συμβάντων, παρέχοντας μία ολική ορατότητα στα μέτρα ασφαλείας του δικτύου
- Δυνατότητα χρήσης των Metadata για την δημιουργία Πολιτικών Ασφάλειας Χρηστών χρησιμοποιώντας την λειτουργία επιβολής δυναμικών επεμβάσεων στις πολιτικές ασφάλειας (Dynamic Policy Actions - DPA).

Η εικόνα 3 δείχνει τον νέο αυτοματοποιημένο τρόπο δυναμικής ασφάλειας στο δίκτυο, όπου τα Metadata που συγκεντρώνονται προσδιορίζουν και επηρεάζουν την δημιουργία, προσαρμογή και ενεργοποίηση των Πολιτικών Ασφάλειας Χρηστών που μεταφέρονται στα μηχανικά και ιδεατά NGFW του όλου δικτύου με ροές Dynamic Address Groups (DAG).

Τεστάρετε τη γνώση σας στο Cloud Security*

1. Ποιος είναι υπεύθυνος για την ασφάλεια στο Cloud;
   A. Ο cloud provider
   B. Ο πελάτης cloud
   Γ. Και οι δύο

2. Αλήθεια ή Ψέμα;
   Οι cloud providers είναι υπεύθυνοι για την ασφάλεια της κίνησης μεταξύ των διαφορετικών clouds, ενώ ο πελάτης είναι υπεύθυνος για την ασφάλεια της κίνησης μεταξύ των data centers και του cloud

3. Οι περισσότερες ..... που έχουν συμβεί στους servers του public cloud ήταν από λάθος του cloud πελάτη.

** Οι απαντήσεις στο τέλος του άρθρου*

Μοντέλο Πολιτικών Ασφάλειας Χρηστών αξιοποιώντας τα Metadata

Τα Metadata μπορούν να περιγραφούν ως ένα ευρετήριο ζευγών τιμών κλειδιών που συλλέγονται από μια λίστα πιθανών τιμών και συσχετίζουν ορισμένα χαρακτηριστικά με τα endpoints. Οι περισσότερες εφαρμογές cloud (VMware NSX, Juniper Contrail® Platform, Amazon AWS κ.λπ.) χρησιμοποιούν εγγενή Metadata που παράγουν οι ίδιες. Η δυνατότητα αξιοποίησης των Metadata στις πολιτικές ασφαλείας ενισχύει σημαντικά τις παραδοσιακές πολιτικές ασφαλείας που χρησιμοποιούν ήδη στατικά αναγνωριστικά όπως διευθύνσεις IP κλπ.

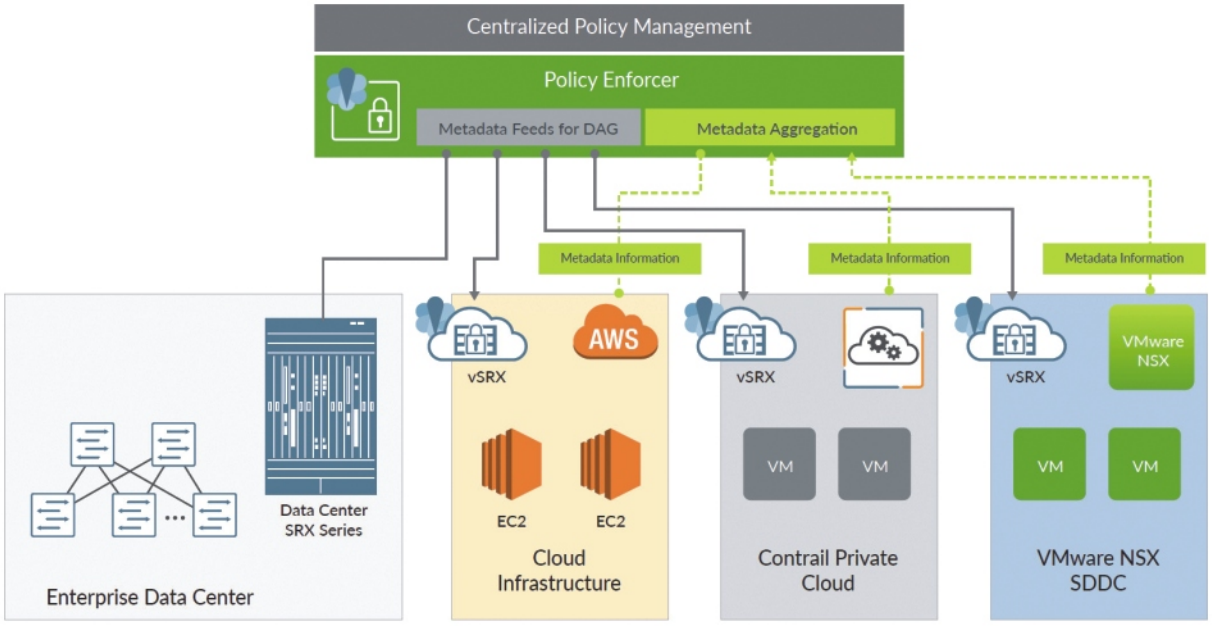
Το Policy Enforcement, που είναι μέρος της Κεντρικής Διαχείρισης Πολιτικών (Central Policy Management) μπορεί να διαμορφώσει και να προσαρμόσει όλα τα NGFW του δικτύου σε ολόκληρη την επιχείρηση με την ίδια ενιαία πολιτική εφαρμόζοντας σήμανση (tagging) βάσει Metadata - χωρίς να απαιτείται κάποια σημαντική προσαρμογή, ώστε να καταστήσει αυτόματα και άμεσα όλη την υποδομή συμβατή με τις δυναμικές απαιτήσεις του πολλαπλών clouds.

Η εικόνα 4 δείχνει την μετάλλαξη του μοντέλου από τον κατακερματισμένο τρόπο της εικόνας 2 στον νέο ενοποιημένο τρόπο.

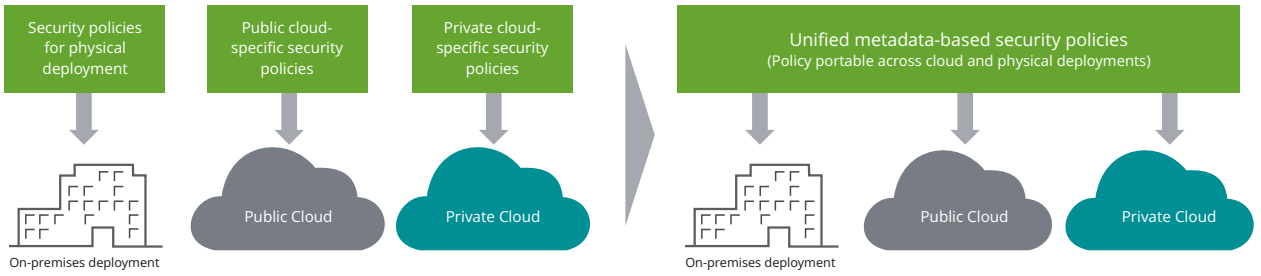
Συμπερασματικά

Αξιοποιώντας τις ικανότητες του Connected Security, επιτυγχάνονται ταυτόχρονα πέντε στόχοι:

1. Εφαρμόζεται μία και ενιαία πολιτική ασφάλειας σε όλες τις υποδομές, ανεξάρτητα από το αν είναι αυτές μηχανικές (appliance) ή ιδεατές στο cloud
2. Αυτοματοποιείται η διαδικασία δημιουργίας, προσαρμογής και ενεργοποίησης των πολιτικών ασφάλειας στις υποδομές με ροές Dynamic Address Groups (DAG)
3. Αξιοποιούνται τα Metadata των υποδομών για τις προσαρμογές σε πραγματικό χρόνο ώστε να τηρείται το επίπεδο ασφάλειας (SLA) ανά πάσα στιγμή χρησιμοποιώντας δυναμικές δράσεις και επεμβάσεις μέσω Dynamic Policy Actions (DPA)
4. Μειώνεται δραστικά ο χρόνος αντίδρασης, προσαρμογής και λήψης μέτρων σε περί-



Εικόνα 3: Ο αυτοματοποιημένος τρόπος: Συγκέντρωση Metadata, δημιουργία και ενεργοποίηση Πολιτικών Ασφάλειας Χρηστών με ροές Dynamic Address Groups (DAG) σε όλα τα NGFW του δικτύου



Εικόνα 4: Εξέλιξη ενοποιημένου μοντέλου πολιτικής ασφάλειας βασισμένο στα Metadata

πτωση συμβάντων ασφάλειας δίνοντας κάλυψη ασφάλειας από άκρο σε άκρο - και μεταξύ των clouds

5. Επιταχύνεται δραστικά η διαδικασία ετοιμασίας ασφαλών και δυναμικά προσαρμόσιμων υποδομών πληροφορικής και δικτύων για την επιχείρηση, μειώνοντας ταυτόχρονα τα λειτουργικά έξοδα και συμπερασματικά ενισχύεται η ανταγωνιστικότητά της.

Λίγα λόγια για τον αρθρογράφο

Ο κ. **Σταύρος Καραγκιούλογλου** κατάγεται από την Κωνσταντινούπολη και αποφοίτησε από το Γερμανο-Αυστριακό Κολλέγιο St.Georg. Στη συνέχεια σπούδασε Διπλ. Ηλεκτρολόγος-Μηχανολόγος Μηχανικός με ειδικότητα στα δίκτυα τηλεπικοινωνιών στο Technical University RWTH AACHEN Γερμανίας, όπου πήρε και το μεταπτυχιακό του με εργασία την εφαρμογή real-time τηλεματικής στον έλεγχο οδικής κυκλοφορίας. Είναι παντρεμένος και πατέρας δύο παιδιών. Στην τηλεπικοινωνιακή αγορά έχει εμπειρία 30 χρόνια, εκ των οποίων τα περισσότερα στη SIEMENS - στους τομείς εφαρμογής, πωλήσεων και marketing τηλεπικοινωνιακών προϊόντων και υπηρεσιών, όπου κατείχε καίριες θέσεις, μεταξύ αυτών και τη θέση του Διευθυντή Πωλήσεων Τηλεπικοινωνιακών Συστημάτων, Προϊόντων και Εφαρμογών. Το 2003 ίδρυσε και μετέχει ενεργά ως Διευθύνων Σύμβουλος στην διοίκηση της UNITED TELECOM AE, μία εταιρία που δραστηριοποιείται εντατικά στην παροχή και την ασφάλεια των κινητών, ασύρματων και σταθερών επιχειρησιακών δικτύων υπολογιστών, τηλεφωνίας και πολυμέσων δημόσιας και ιδιωτικής χρήσης καθώς και στην ασφάλεια των ηλεκτρονικών συναλλαγών, των δεδομένων και του Cloud.

Απαντήσεις στο test: Η γνώση σας για το Cloud Security

1. Γ. *Είναι υπεύθυνοι και ο cloud provider αλλά και ο πελάτης. Ισχύει το μοντέλο της Διαμοιρασμένης Ευθύνης στο οποίο η ασφάλεια είναι μία ευθύνη που μοιράζεται και στα δύο μέρη. Ο cloud service provider είναι κατά βάση υπεύθυνος να προστατεύει τη φυσική υποδομή και το λογισμικό πάνω στο οποίο «κάθεται» το cloud, ενώ οι πελάτες που ανεβάζουν εφαρμογές στο cloud είναι υπεύθυνοι για την ασφάλεια των άυλων περιουσιακών τους στοιχείων που τρέχουν στο cloud, όπως δικτύωση, workloads και δεδομένα.*

2. Λάθος. *Οι πελάτες του cloud είναι υπεύθυνοι να ασφαλίσουν την κίνηση και από και προς το cloud καθώς επίσης και την κίνηση μεταξύ διαφορετικών cloud περιβαλλόντων αν κάνουν τέτοια χρήση. Ένα ασφαλές Multicloud περιβάλλον διαθέτει ισχυρή προστασία από το campus έως τα υποκαταστήματα, ανάμεσα στις υποδομές cloud και φυσικά και στο data center.*

3. Παραβιάσεις. *Ο συντριπτικός αριθμός των παραβιάσεων ασφαλείας στο cloud μπορεί να αποφευχθεί και οφείλεται σε πελάτες του cloud που δεν ακολουθούν τις βέλτιστες πρακτικές προγραμματισμού configuration και ασφάλειας. Στην πραγματικότητα, η ερευνητική Gartner, Inc. προβλέπει ότι «ήδη έως και το 2022, τουλάχιστον το 95% των αστοχιών ασφαλείας στο cloud θα είναι σφάλμα του πελάτη», βλ. "Is the Cloud Secure", Smarter with Gartner, March 27, 2018.*

Εάν επιθυμείτε το COMMUNICATION SOLUTIONS να δημοσιεύσει περισσότερα άρθρα για **Security** επικοινωνήστε μαζί μας στο: **info@comsol.gr**