ISSUE

Η απαίτηση της Ασφάλειας ως κομβικός παράγοντας υιοθέτησης του Cloud

Έρευνες παγκοσμίως μέχρι πριν κάποιο καιρό, έδειχναν ότι οι όποιες επιφυλάξεις για μετάβαση από τις παραδοσιακές υποδομές IT στο Cloud, αφορούσαν κατά κύριο λόγο τα θέματα ασφάλειας των δεδομένων. Σήμερα όμως έχουν ωριμάσει αρκετά οι συνθήκες ώστε αυτές οι επιφυλάξεις, αν όχι να έχουν εξαλειφθεί, τουλάχιστον να έχουν μειωθεί σημαντικά. Το Cloud δεν είναι απαραίτητα λιγότερο ή περισσότερο ασφαλές από το συμβατικό περιβάλλον IT ενός Οργανισμού. Η σημαντική διαφορετικότητα του όμως είναι αλήθεια ότι εγκυμονεί νέους κινδύνους για τα δεδομένα. Κίνδυνοι που εξαρτώνται από μια σειρά παραμέτρων όπως το είδος των δεδομένων, τους μηχανισμούς ασφαλείας και κυρίως ποιοι είναι αυτοί και ποιες υποδομές αξιοποιούν για την διαχείριση των δεδομένων σε περιβάλλον cloud. Το συμπέρασμα λοιπόν που εξάγουμε είναι ότι η μετάβαση στο cloud απαιτεί μια ταυτόχρονη επαναδιαμόρφωση της στρατηγικής για την ασφάλεια των δεδομένων, ερευνώντας μεταξύ άλλων τις διάφορες τεχνολογίες που έχουν αναπτυχθεί αλλά και το κανονιστικό πλαίσιο που υπάρχει. Σε συνέχεια λοιπόν του κεντρικού αφιερώματος του παρόντος τεύχους σχετικά με το cloud computing, απευθυνθήκαμε σε στελέχη εταιρειών που δραστηριοποιούνται ευρύτερα στο χώρο, προκειμένου να μας αναπτύξουν τη δική τους προσέγγιση για τις πολλές διαφορετικές παραμέτρους που συνθέτουν το θέμα της ασφάλειας στο Cloud.

Νίκος Μουρτζίνος

Product Sales Specialist, Cisco Security Ελλάδα, Κύπρος, Μάλτα, Ισραήλ, Πορτογαλία

Από το "Any-to-Any" στο "End-to-End"

Ο κόσμος του "Any-to-Any", δηλαδή η απρόσκοπτη επικοινωνία από και προς κάθε σημείο, συσκευή και άνθρωπο και το "Internet of Everything" είναι η εξέλιξη των δυνατοτήτων σύνδεσης και συνεργασίας που αναπτύσσεται ραγδαία, παρασύροντας κάθε μορφή εταιρικής αλλά και προσωπικής επικοινωνίας. Θα μπορούσαμε επίσης να περιγράψουμε αυτή την εξέλιξη ως τη σύνδεση συσκευών, cloud και εφαρμογών.

Αν και η εξέλιξη αυτή δεν ήταν απροσδόκητη, οι επιχειρήσεις σήμερα πιθανό να μην είναι προετοιμασμένες να συμμετέχουν στον κόσμο του "Any-to-Any", τουλάχιστον όσον αφορά στην ασφάλεια. Και αυτό, αφού η ουσία του είναι ότι κατευθυνόμαστε ταχύτατα στο σημείο όπου θα είναι όλο και λιγότερο πιθανό ο χρήστης να έχει πρόσβαση στην εργασία του μέσω του εταιρικού δικτύου. Οι συσκευές με πρόσβαση στο internet, συνδέονται πλέον από οπουδήποτε, σε κάθε σημείο του δικτύου και αναζητούν πρόσβαση σε εφαρμογές που μπορεί να "τρέχουν" οπουδήποτε, όπως ένα δημόσιο SaaS cloud, ένα ιδιωτικό ή ένα δημόσιο cloud.

Η πρόκληση της δημιουργίας ενός ασφαλούς πλαισίου για τις εφαρμογές, τις συσκευές και τους χρήστες, γίνεται πιο δύσκολη από την αναγνώριση του cloud ως το κατάλληλο μέσο για τη λειτουργία των εταιρικών συστημάτων. Σύμφωνα με την τελευταία έρευνα της Cisco, η παγκόσμια διακίνηση δεδομένων μέσω data center θα τετραπλασιαστεί στην επόμενη πενταετία, με τα cloud δεδομένα να αυξάνονται με τον ταχύτερο ρυθμό. Έως το 2016 η διακίνηση cloud δεδομένων θα αποτελεί τα 2/3 της συνολικής κίνησης.

Αποσπασματικές λύσεις ασφάλειας, όπως η εφαρμογή firewall στην άκρη του δικτύου, δεν προστατεύουν τα δεδομένα τα οποία βρίσκονται πλέον σε συνεχή κίνηση μεταξύ συσκευών, δικτύων και cloud. Ακόμα και μέσα στο data center, το virtualization αποτελεί πλέον τον κανόνα και όχι την εξαίρεση. Η αντιμετώπιση αυτών των προκλήσεων, σε συνέχεια του virtualization και του cloud, απαιτεί επανεξέταση των πολιτικών ασφάλειας, οι οποίες θα αντανακλούν τη νέα πραγματικότητα και θα ευθυγραμμιστούν με το σύγχρονο επιχειρηματικό μοντέλο.

Η Cisco θεωρεί το δίκτυο ως το κατάλληλο σημείο για την υλοποίηση της πολιτικής ασφάλειας και η στρατηγική που προτείνει θέτει το δίκτυο ως πλατφόρμα για την πολιτική και την εφαρμογή της και την ασφάλεια ως ένα ενιαίο σύνολο υπηρεσιών, που μπορούν να ενσωματωθούν στο data center και το router έως το switch και τις υπόλοιπες συσκευές, ως μια End-to-End πρόταση. Όλα τα παραπάνω με δυνατότητα ενιαίας διαχείρισης, καθώς και με υπηρεσίες ενημέρωσης για διαδικτυακούς κινδύνους, βασισμένες στο cloud. Η αρχιτεκτονική αυτή ονομάζεται Cisco SecureX Next Generation Security Architecture και παρέχει εξελιγμένη ασφάλεια σε κάθε χρήστη και συσκευή, όπου και αν βρίσκεται και οποιαδήποτε στιγμή. Προϊόντα, λύσεις και υπηρεσίες όπως το Cisco ASA 1000V Cloud Firewall, Cisco Intrusion Prevention, Cisco Cloud Email Security and Email Encryption, Cisco Cloud Web Security, Cisco Identity Services Engine, Cisco AnyConnect και το Cisco Security Intelligence Operations (SIO), το οποίο αποτελεί το μεγαλύτερο παγκοσμίως εργαλείο ενημέρωσης για διαδικτυακές απειλές, χρησιμοποιώντας περίπου 1 εκατομμύριο πηγές πληροφόρησης και δημιουργώντας σχεδόν 8 εκατομμύρια ενημερώσεις ανά ημέρα, συνθέτουν την πιο ολοκληρωμένη End-to-End πρόταση ασφάλειας για το cloud.

Επιπλέον, η πρόσφατη εξαγορά της εταιρείας "Cognitive Security", η οποία έχει αναπτύξει τεχνολογίες τεχνητής νοημοσύνης για τον εντοπισμό των απειλών μέσα και έξω από το δίκτυο, ενισχύει την προστασία από προηγμένες απειλές στον κυβερνοχώρο.

Κωνσταντίνος Ζαλαχώρης

Διευθύνων Σύμβουλος

Οι βέλτιστες πρακτικές για τη χρήση των cloud απο τις επιχειρήσεις ακόμα διαμορφώνονται

Τα τελευταία χρόνια αναπτύχθηκαν πολλές λύσεις για την προστασία των κρίσιμων για τη λειτουργία μιας επιχείρησης υποδομών, δεδομένων και πληροφοριών. Προστατευόμαστε από διαδικτυακές απειλές, πρέπει να διασφαλίσουμε την επιχειρησιακή συνέχεια, να διαχειριστούμε την πρόσβαση στα συστήματα, να αποτρέψουμε την υποκλοπή δεδομένων, να προστατέψουμε τους προσωπικούς υπολογιστές και τις κινητές συσκευές, να είμαστε συμβατοί

ISSUE

Η απαίτηση της Ασφάλειας ως κομβικός παράγοντας υιοθέτησης του Cloud

με διεθνείς και τοπικούς κανόνες, νόμους και στάνταρτ. Και πάνω που οι Διευθυντές Πληροφορικής και Επικοινωνιών πίστευαν ότι βρίσκονται σε καλό σημείο για την αντιμετώπιση των προβλημάτων ασφάλειας, η άφιξη του virtualization πρώτα και των clouds πιο πρόσφατα, δημιούργησαν νέα προβλήματα, ερωτηματικά και αμφιβολίες.

Οι απαιτήσεις για ασφάλεια δεν άλλαξαν αλλά άλλαξαν δραματικά τα περιβάλλοντα όπου οι πληροφορίες, απόλυτη αξία για την κάθε επιχείρηση, αποθηκεύονται, διακινούνται, μοιράζονται και γίνονται προσβάσιμες. Τα συστήματα των επιχειρήσεων, πραγματικά απόρθητα και απομονωμένα κάστρα κάποτε, επιτρέπουν πλέον πρόσβαση στα δεδομένα τους σε στελέχη, συνεργάτες , προμηθευτές και πελάτες ακόμα και σε social media. Και με την έλευση των cloud, οι επιχειρήσεις δυνητικά δεν γνωρίζουν ούτε που ακριβώς βρίσκονται τα πολύτιμα δεδομένα τους, ούτε έχουν τα κατάλληλα εργαλεία ώστε να ελέγξουν ότι όλες οι διαδικασίες που αφορούν τα δεδομένα τους ακολουθούν τις απαραίτητες πολιτικές ασφάλειας. Συνεχίζουν όμως να είναι υπόλογες απέναντι στο νόμο για πιθανή κακή χρήση ή διακίνηση προσωπικών δεδομένων και πρέπει οι ίδιες να εξασφαλίσουν ότι ο πάροχος των υπηρεσιών cloud διαχειρίζεται τα δεδομένα τους με τη δέουσα προσοχή. Ενδεικτικό είναι ότι μέχρι σήμερα μόνο έξι πάροχοι στην Αμερική έχουν καταφέρει να είναι συμβατοί με το FedRAMP στανταρντ, ώστε να παρέχουν πιο εύκολα υπηρεσίες cloud στο Αμερκάνικο δημόσιο.

Από τη μία λοιπόν τα αναμφισβήτητα πλεονεκτήματα του cloud, μείωση κόστους και ευελιξία και απο την άλλη "απώλεια» ελέγχου. Το συμπέρασμα; Οι βέλτιστες πρακτικές για τη χρήση των cloud απο τις επιχειρήσεις ακόμα διαμορφώνονται και η προσωπική εμπειρία χρήσης των υπηρεσιών ίσως είναι ο καλύτερος τρόπος για να μάθετε. Υπάρχουν αρκετοί κίνδυνοι στο cloud αλλά αυτοί μπορούν να αναλυθούν με τη βοήθεια των ειδικών ώστε η κάθε επιχείρηση να αποφασίσει για τα βήματα που θα ακολουθήσει. Αν δηλαδή θα προχωρήσει πρώτα με τα λιγότερο κρίσιμα συστήματα και σε δεύτερη φάση με τα πιο σημαντικά. Γιατί η εποχή του cloud έφτασε και είμαι σίγουρος ότι σύντομα δεν θα υπάρχει εταιρεία που να μην χρησιμοποιεί τέτοιες υπηρεσίες.

Γιώργος Ράικος

Γενικός Γραμματέας ISACA Athens Chapter, MSc, DipBA, CISA, CISM, Business & Executive Coach

Σταμάτης Πασσάς

Social Media Coordinator & Assistant Webmaster ISACA Athens Chapter, Ethnodata S.A. (NBG) - IT Compliance & Control Dept., MSc in Computer Studies, MBA

Cloud Security: Βέλτιστες Πρακτικές από τον ISACA®

Τα τελευταία χρόνια το cloud computing έχει γίνει κάτι περισσότερο από ένα ακόμα "IT buzzword", εγείροντας όπως είναι αναμενόμενο πολλά θέματα GRC.

Το 2009 η μελέτη White Paper-Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives του ISACA® αναφέρει ότι «πρόκειται για μια τάση των επιχειρήσεων που αναμένεται να έχει μια σημαντική επίδραση στον τρόπο που η κάθε μία λειτουργεί. Το cloud computing αναμένεται να αποκτήσει ακόμη μεγαλύτερη σημασία με το πέρασμα των ετών, καθώς η τεχνολογία και η σχετική αγορά παροχής υπηρεσιών ωριμάζουν συνεχώς. Σε περιόδους μείωσης του κόστους και οικονομικής ύφεσης, το cloud computing μπορεί να αποδειχθεί μία πιο αποδοτική προσέγγιση για την τεχνολογική υποστήριξη της επιχείρησης. Ωστόσο, η ασφάλεια και η προστασία των δεδομένων ακόμη θεωρούνται κρίσιμα ζητήματα κατά την υιοθέτηση των υπηρεσιών cloud computing».

Οι έλεγχοι ασφάλειας στο cloud δεν διαφοροποιούνται σημαντικά από τους αντίστοιχους ελέγχους των παραδοσιακών υλοποιήσεων. Παρά ταύτα, οι υλοποιήσεις στο cloud συνιστούν ιδιαίτερες προκλήσεις στους τομείς ασφάλειας των πληροφοριακών συστημάτων. Κάθε υλοποίηση στο cloud, ισορροπεί μετά βίας μεταξύ της έλλειψης άμεσου ελέγχου

των δεδομένων και της διατήρησης της απόλυτης ευθύνης για τη λειτουργία και τα δεδομένα από τον ανάδοχο.

Η διάθεση ενός Οργανισμού να αναλάβει μικρό ή μεγάλο ποσοστό ρίσκου, είναι μία πολύ σημαντική στρατηγική επιλογή, η οποία αντικατοπτρίζεται στην επιμέρους πολιτική ασφαλείας και τα διαφορετικά της τμήματα σε επίπεδο δικτύου, φυσικής ασφάλειας, λογικής ασφάλειας και ασφάλειας των εφαρμογών. Σύμφωνα με τις ISACA IT Governance Institute Guidelines, η χρηστή διαχείριση του ρίσκου, επιτάσσει την υιοθέτηση και την επιχειρησιακή ένταξη ενός μοντέλου αποτελεσματικής εταιρικής διακυβέρνησης, στην οποία οφείλει να αναφέρεται και η πολιτική και οι έλεγχοι για τη διαχείριση του κινδύνου και την ασφάλεια των δεδομένων. Κάτω από αυτό το πρίσμα, η συμμόρφωση με τις ρυθμιστικές αρχές και τις ισχύουσες νομικές διατάξεις, η επιβολή ελέγχων στον πάροχο του cloud - σύμφωνα με την εταιρική πολιτική ελέγχου και το σχετικό δικαίωμα ελέγχου, θα πρέπει να εξασφαλίζονται από τον Οργανισμό αναφορικά με την υλοποίηση του cloud.

Η υιοθέτηση κρυπτογραφικής τεχνολογίας, ελέγχου λογικών προσβάσεων, ταυτοποίησης χρηστών και ασφαλών απομακρυσμένων προσβάσεων και συνδέσεων, αποτυπώνονται και εφαρμόζονται ανελλιπώς, με σκοπό την περαιτέρω θωράκιση του συστήματος ασφαλείας.

Με βάση τα αποτελέσματα της μελέτης Cloud Computing Market Maturity Study Results που διεξήχθη από το CSA και τον ISACA® το 2012, για να ωριμάσει περαιτέρω το cloud computing ώστε οι επιχειρήσεις να λάβουν τα οφέλη που αυτό έχει υποσχεθεί – όπως είναι η συγκράτηση του κόστους (cost containment), η αμεσότητα (immediacy), η διαθεσιμότητα (availability), η επεκτασιμότητα (scalability), η απόδοση (efficiency) και η ελαστικότητα (resiliency), θα πρέπει να δοθεί λιγότερη έμφαση ως προς την τεχνολογική προσέγγιση και περισσότερη ως προς την κατανόηση μίας καινοτομίας που δρα καταλυτικά ως enabler σε μια επιχείρηση. Ο κίνδυνος που σχετίζεται με το cloud computing, θα πρέπει να αντιμετωπιστεί συνολικά σε επιχειρηματικό και επιχειρησιακό επίπεδο. Μπορεί ακόμη να αντιπροσωπεύει μία μοναδική ευκαιρία να επαναπροσδιοριστούν συνολικά τα IT controls και να διασφαλιστεί η κάθε επιχείρηση ως προς την προστασία δεδομένων, τη διαθεσιμότητα των συστημάτων και τη συμμόρφωση.

Η μεθοδολογία που ακολουθείται κατά την υλοποίηση ενός μοντέλου cloud θα πρέπει να είναι συμβατή και ευθυγραμμισμένη με την επιχειρησιακή στρατηγική, προκειμένου να αποδώσει τη μέγιστη προσδοκώμενη αξία σε σχέση με τα επενδυόμενα κεφάλαια και το ανθρώπινο δυναμικό που έχει δεσμευτεί. Η επιτυχία του εγχειρήματος είναι αποτέλεσμα πολλών συνιστωσών και η μεγιστοποίηση στη διάρκειά της είναι το τελικό ζητούμενο αποτέλεσμα.

Ο ISACA® καθοδηγώντας τις εξελίξεις και στο χώρο του cloud, ήδη θέτει μέσα από το paper "Cloud Governance: Questions Boards of Directors Need to Ask" τις πιο κρίσιμες ερωτήσεις στις οποίες θα πρέπει να έχει την απάντηση η Διοίκηση ενός Οργανισμού πριν «βγει στο cloud". Οι υλοποιήσεις του cloud παραμένουν μία πρόκληση για κάθε ειδικό ασφάλειας, αλλά η προστιθέμενη εμπειρία του παρελθόντος προσδίδει κάποιες καλές κατευθυντήριες γραμμές για να αποφύγει κανείς τους "επικίνδυνους υφάλους" και την αποτυχία που μπορεί να κοστίσει πολύ ακριβά.

Vladimir Udalov

Senior Corporate Marketing Manager

Πώς να προστατεύσετε τα δεδομένα σας στο cloud

Πολύ συχνά, όταν μιλάμε για τεχνολογίες cloud ο βασικός προβληματισμός των επιχειρήσεων είναι το αν είναι τελικά πιο επικίνδυνο να αποθηκεύονται δεδομένα στο cloud ή σε κάποιο φυσικό server. Η απάντηση είναι ότι αυτό εξαρτάται από τα μέτρα ψηφιακής ασφάλειας που χρησιμοποιούνται. Η πλειοψηφία των υπηρεσιών cloud είναι βασισμένη σε τεχνολογίες virtualization. Η χρήση συγκεκριμένων λύσεων antivirus που έχουν αναπτυχθεί για εικονικά περιβάλλοντα, αυξάνει τα επίπεδα προστασίας της υπηρεσίας cloud και επιτρέπει την ισορροπία ανάμεσα στην ασφάλεια και την αποδοτικότητα.

Υπάρχουν αρκετές προσεγγίσεις στο θέμα της ασφάλειας. Μια κλασική προσέγγιση είναι η εγκατάσταση antivirus προστασίας σε κάθε εικονικό server. Ωστόσο, αυτό συχνά ενδέχεται να αναιρεί όλα τα πλεονεκτήματα της virtualization – την αποδοτικότητα και τη δυνατότητα ελέγχου. Η εγκατάσταση μιας λύσης antivirus σε κάθε εικονικό μηχάνημα σημαίνει πως θα αναβαθμίζονται ξεχωριστά, χρησιμοποιώντας τις δικές τους μηχανές antivirus. Σε αυτήν την περίπτωση κάθε προϊόν λειτουργεί αυτόνομα, υπερφορτώνοντας το δίκτυο και τους υπολογιστικούς πόρους. Γι' αυτόν το λόγο έχουν εμφανιστεί στην αγορά συγκεκριμέ-

νες συγκεντρωτικές λύσεις για εικονικά περιβάλλοντα. Για την ώρα πάντως, πολύ λίγες από αυτές τις λύσεις είναι διαθέσιμες – στην πραγματικότητα μόνο ένα παρόμοιο προϊόν υπήρχε πριν την εμφάνιση του Kaspersky Security for Virtualization.

Η agent-less λύση ασφαλείας εξαφανίζει την ανάγκη για διπλούς πόρους σε κάθε virtual μηχάνημα, βοηθώντας τη βελτιστοποίηση της απόδοσης, τη μείωση του κόστους του hardware και της κατανάλωσης ενέργειας, καθώς και τη λεπτομερή καταγραφή των διαδικασιών ασφάλειας, σύμφωνα με τις απαιτήσεις του ελέγχου συμμόρφωσης. Έτσι, το Kaspersky Security for Virtualization υποστηρίζει την πλατφόρμα VMware ESXi, έχοντας σημαντικά λιγότερες απαιτήσεις από προϊόντα που εγκαθίστανται ξεχωριστά σε κάθε εικονικό μηχάνημα. Επιπλέον, η Kaspersky Lab ανακοίνωσε πρόσφατα τη δημιουργία του Kaspersky Security for Virtualization-Light Agent, ειδικά σχεδιασμένου για Citrix XenServer, Citrix XenDesktop και Microsoft Hyper-V. Η νέα τεχνολογία είναι πλήρως ενσωματωμένη στο Kaspersky Endpoint Security for Business, την εταιρική λύση-ορόσημο της εταιρείας.

Μερικές φορές τα εικονικά μηχανήματα απαιτούν αναβάθμιση όταν παραμένουν offline για αρκετό καιρό. Έτσι προκαλείται «συνωστισμός» που αφήνει απροστάτευτο το πρόσφατα ενεργοποιημένο μηχάνημα, ενώ οι αναβαθμίσεις«κατεβαίνουν». Αν η μηχανή antivirus «τρέχει» σε ξεχωριστό virtual μηχάνημα, θα είναι πάντα ενημερωμένη και το εικονικό μηχάνημα θα προστατεύεται αυτόματα, τη στιγμή που συνδέεται με το δίκτυο. Ο ανεξάρτητος server είναι μονίμως ενεργοποιημένος και παρακολουθεί το δίκτυο. Το προϊόν της Kaspersky Lab χρησιμοποιεί ένα συγκεκριμένο VMware interface – το vShield – το οποίο μεταβιβάζει αρχεία από εικονικά μηχανήματα για να ελεγχθούν από το Kaspersky Security for Virtualization.

Επιπλέον, το προϊόν της Kaspersky Lab προσφέρει ένα μοναδικό σύστημα προστασίας από εισβολές (IDS/IPS), προστασία εναντίον του κακόβουλου λογισμικού με τη χρήση σε πραγματικό χρόνο πληροφοριών για τις απειλές από το Kaspersky Security Network καθώς και το χαρακτηριστικό Shared Cache που βελτιώνει την απόδοση της προστασίας με την ανίχνευση παρόμοιων αρχείων στα εικονικά μηχανήματα, χωρίς να χρειάζεται η ξεχωριστή ανάλυση καθενός από αυτά. Αυτά τα χαρακτηριστικά, σε συνδυασμό με τα εργαλεία συγκεντρωτικής διαχείρισης βοηθούν τις εταιρείες να προστατεύουν με μεγαλύτερη ευκολία και αξιοπιστία τα δεδομένα τους στο cloud.

Η διαδικασία αδειοδότησης ενδέχεται να αποτελέσει σημαντικό πρόβλημα για τις εταιρείες. Πρέπει να σημειωθεί πως η αγορά του Kaspersky Security for Virtualization μπορεί να πραγματοποιηθεί με μία άδεια για τον κεντρικό επεξεργαστή που ελέγχει τα εικονικά μηχανήματα, επιτρέποντας την κάλυψη πολλών μηχανημάτων.

Γιώργος Καπανίρης
Business Development Director
NSS NETWORKSYSTEMSECURITY

Η Sophos δείχνει το δρόμο για ένα λαμπρό μέλλον στο cloud

Ενώ παντού γίνεται συζήτηση για το cloud, πολλά ερωτήματα παραμένουν εντελώς αναπάντητα για τις επιχειρήσεις και τους επαγγελματίες της πληροφορικής. Πρόσφατα στην Αθήνα έγινε το διεθνές συνέδριο της Sophos που φιλοξένησε περισσότερα από 600 άτομα από όλη την Ευρώπη, τη Μέση Ανατολή και την Αφρική. Είναι σαφές το ενδιαφέρον που υπάρχει από όλη την αγορά σχετικά με τη διαχείριση της ασφάλειας στο cloud για τερματικά (endpoint), πύλες (gateways) αλλά και φορητές συσκευές. Στο συνέδριο αντιμετωπίστηκε το θέμα της ασφάλειας στο cloud και παρουσιάστηκε μία νέα ιδέα διάθεσης της ασφάλειας ως υπηρεσίας στο cloud, κάτι που σίγουρα θα ενθουσιάσει την αγορά της πληροφορικής παγκοσμίως.

Ο στόχος της Sophos είναι να ενεργοποιήσει μέσω ειδικού περιβάλλοντος διαχείρισης στο Web το πλήρες χαρτοφυλάκιο των προϊόντων της, έτσι ώστε οι συνεργάτες να μπορούν να εξυπηρετούν τους πελάτες τους μέσω του Cloud. Το πρώτο στάδιο για να επιτευχθεί κάτι τέτοιο θα είναι η πλήρης προστασία των τερματικών (endpoint protection) χωρίς να απαιτείται τοπικός διακομιστής διαχείρισης για τη διαχείριση των πολιτικών ασφαλείας και των

αναφορών (reporting) στο χώρο του πελάτη, κάτι που θα μπορεί πλέον να γίνεται μέσω μίας κεντρικής εφαρμογής στο cloud. Στη συνέχεια θα δοθεί η δυνατότητα φιλτραρίσματος ιστοσελίδων, δικτυακής ασφάλειας και προστασίας κινητών συσκευών.

Να σημειωθεί ότι η Sophos θα συνεχίσει να υποστηρίζει όλα τα συστήματα προστασίας που προορίζονται για το χώρο του πελάτη για την ασφάλεια τερματικών και δεδομένων, αλλά και τα προϊόντα δικτυακής ασφάλειας. Το Sophos Cloud έρχεται για να προσφέρει μία πραγματικά συναρπαστική εναλλακτική προοπτική πλήρους διαχείρισης της ασφάλειας στο cloud, για πελάτες που θέλουν στρατηγικά να κινηθούν προς αυτήν την κατεύθυνση.

Αυτό που κάνει το Sophos Cloud πραγματικά μοναδικό είναι η καινοτόμος λειτουργία εξατομικευμένων πολιτικών και αναφορών. Αυτός είναι ένας πραγματικά εντελώς σύγχρονος τρόπος διαχείρισης της ασφάλειας από μία επιχείρηση που επικεντρώνεται προς το χρήστη και όχι τα μηχανήματα που χρησιμοποιεί (user security). Αφού οριστεί μία πολιτική για ένα χρήστη, αυτή θα τηρηθεί σε κάθε σύστημα που χρησιμοποιεί, όπου και να βρεθεί εντός ή εκτός της επιχείρησης, δίνοντας άμεση πληροφόρηση για τη δραστηριότητα και την προστασία του μέσω ενός ειδικού κέντρου ελέγχου (dashboard) του Sophos Cloud και του εξελιγμένου συστήματος αναφορών.

Το Sophos Cloud στοχεύει να είναι η πλατφόρμα του μέλλοντος για την παροχή ασφάλειας ως υπηρεσία σε όλα τα επίπεδα. Το Sophos Cloud θα περιλαμβάνει όλα όσα απαιτούνται για την προστασία τόσο των χρηστών όσο και όλων των συσκευών τους, καθώς και των δικτύων στα οποία συνδέονται. Τα επιπλέον υποσυστήματα ασφαλείας θα είναι διαθέσιμα ως add-ons, έτσι ώστε οι πελάτες να μπορούν να ενεργοποιήσουν αποκλειστικά την προστασία που χρειάζονται και στη συνέχεια εύκολα να μπορούν να ενεργοποιήσουν και επιπλέον υποσυστήματα προστασίας ανά πάσα στιγμή, αφού ελέγξουν πρώτα ότι τους καλύπτει η λειτουργικότητά τους (try-and-buy).

Είναι προφανές ότι η Sophos έχει προσεγγίσει το θέμα του cloud με ένα εντελώς διαφορετικό τρόπο, κάνοντας τη διαχείριση της ασφάλειας απλούστερη και πολύ πιο ''έξυπνη'', ενσωματώνοντας την πολύχρονη εμπειρία της, κάνοντας όμως τη διαχείριση της ασφάλειας απλούστερη από ποτέ. Η νέα κονσόλα διαχείρισης (management console) στο cloud έχει μια εντελώς νέα διεπαφή, πλήρως εκσυγχρονισμένη, εξασφαλίζοντας τη βέλτιστη πρακτική και απλοποιώντας ταυτόχρονα τα πράγματα για τους διαχειριστές.

Ήδη σε beta, το Sophos Endpoint Cloud έχει προγραμματιστεί για έναρξη στις ΗΠΑ και το Ηνωμένο Βασίλειο αυτό το καλοκαίρι - και σύντομα η υπηρεσία θα υποστηριχθεί παγκοσμίως.

Κωνσταντίνος Βαβούσης

Strategic Manager

TRUST-IT
IT Security Intelligence

Cloud Computing: Πλέον η ασφάλεια περνάει από το "σύννεφο"

Ένα από τα πιο δημοφιλή θέματα συζητήσεων στον κλάδο της πληροφορικής αποτελεί το cloud computing και η στροφή εταιρειών ακόμη και κυβερνήσεων προς αυτήν την κατεύθυνση. Οι εταιρείες παροχής υπηρεσιών cloud προσφέρουν έναν εναλλακτικό τρόπο διαχείρισης των λύσεων πληροφορικής με πολλά οφέλη, συμπεριλαμβανομένων της αυξημένης ευελιξίας και της σημαντικής μείωσης του κόστους. Μείωση, που στις μέρες μας φαντάζει σωτήρια. Τροχοπέδη όμως στην ένταξη των περισσότερων εταιρειών αποτελούσε μέχρι αρκετά πρόσφατα - και ακόμη απασχολεί αρκετούς - η ασφάλεια. Κατά πόσο δηλαδή διαφυλάσσονται ασφαλώς τα κρίσιμα εταιρικά - και όχι μόνο - δεδομένα των εταιρειών μας στο ''σύννεφο''. Αυτοί οι φόβοι επιδεινώνονταν κατά διαστήματα λόγω των εκάστοτε δυσλειτουργιών που προέκυπταν κατά κύριο λόγο σε κορυφαίες εταιρείες, όπως ακριβώς έγινε με την Amazon, όταν το καλοκαίρι του 2011 ένα κακόβουλο λογισμικό - παραλλαγή του SpyEye - εκμεταλλεύτηκε την υπηρεσία Simple Storage (Amazon S3).

Η ασφάλεια στο cloud αποτελεί ένα καυτό θέμα που ''καίει'' όλες τις εταιρείες παροχής υπηρεσιών cloud computing, με αρκετούς να έχουν καταφέρει με μεγάλη επιτυχία να λύσουν πρακτικά ζητήματα κυρίως σε ό,τι αφορά στην ασφάλεια και την εξασφάλιση των εταιρικών δεδομένων. Δεν είναι λίγες οι εταιρείες/ πάροχοι υπηρεσιών cloud οι οποίες έχουν καταφέρει να επεκτείνουν επιτυχώς τις πολιτικές ασφάλειας σε εφαρμογές που βρίσκονται πίσω από το εταιρικό firewall μιας επιχείρησης, αλλά και να ενδυναμώσουν εφαρμογές που βρίσκονται σε περιβάλλον cloud, προστατεύοντας παράλληλα το ηλεκτρονικό ταχυδρομείο και την αυθεντικοποίηση ταυτότητας χρηστών που αποτελούν πολύ σημαντικά στοιχεία για μια επιχείρηση η

ISSUE

Η απαίτηση της Ασφάλειας ως κομβικός παράγοντας υιοθέτησης του Cloud

οποία χρησιμοποιεί εκτεταμένα υπηρεσίες cloud.

Παρατηρούμε ολοένα και περισσότερες υπηρεσίες cloud να κάνουν την εμφάνισή τους και να χρησιμοποιούνται κατά κόρον από χρήστες τόσο σε προσωπικό όσο και σε εταιρικό επίπεδο. Χαρακτηριστικό παράδειγμα αποτελεί το Dropbox, το οποίο είναι μία από τις πιο διαδεδομένες και εξαιρετικά δημοφιλείς υπηρεσίες διαχείρισης δεδομένων στο "σύννεφο". Όπως αναφέραμε, τέτοιου είδους υπηρεσίες παρουσιάζουν αρκετά προβλήματα κατά κύριο λόγο σε θέματα ασφάλειας, τα οποία όμως σταδιακά αρχίζουν και εξαλείφονται εισάγοντας νέες μεθόδους για την ενίσχυση της ασφάλειας των παρεχόμενων υπηρεσιών, αλλά και δίνοντας συμβουλές στους χρήστες για πιο ασφαλή διαχείριση.

Αρκετές βελτιστοποιήσεις σε θέματα ασφάλειας έχουν καταφέρει να κερδίσουν την εμπιστοσύνη ολοένα και περισσότερων χρηστών, οι οποίοι με την πάροδο του χρόνου δείχνουν έστω και δειλά σημάδια μεγαλύτερης ευαισθητοποίησης σε σύγκριση με παλαιότερα, όσον αφορά στην ασφάλεια των δεδομένων τους. Πλέον υποστηρίζεται από ορισμένες υπηρεσίες επιτυχώς η ενεργοποίηση δύο σταδίων ελέγχου, που έχει να κάνει με την υποστήριξη επιλογής εισαγωγής όχι μόνο του κωδικού πρόσβασης του εκάστοτε χρήστη, αλλά και του κωδικού ασφάλειας προκειμένου να αποκτηθεί πρόσβαση στο λογαριασμό. Μια επίσης ισχυρή μέθοδος για την ασφάλεια των δεδομένων μας στο cloud αποτελεί σταθερά η κρυπτογράφηση. Οι υπηρεσίες cloud από μόνες τους δεν προσφέρουν κάποιο σοβαρό τρόπο κρυπτογράφησης, αλλά υπάρχουν πολλοί απλοί τρόποι που μπορούν να υιοθετηθούν από τον εκάστοτε χρήστη. Οι πιο προχωρημένοι χρήστες προτιμούν το TrueCrypt - φυσικά υπάρχουν και άλλες υπηρεσίες που είναι πιο φιλικές, όπως το BoxCryptor, ενώ οι λάτρεις των Linux μπορούν να χρησιμοποιήσουν το EncFS.

Ένα ενθαρρυντικό στοιχείο και για την ελληνική πραγματικότητα αποτελεί το γεγονός ότι ολοένα και περισσότεροι Οργανισμοί και επιχειρήσεις στρέφονται για λύσεις στο "σύννεφο", ανταποκρινόμενοι με ελάχιστη δυσπιστία στο ασφαλές πλέον τεχνολογικό κάλεσμα που ακούει στο όνομα cloud computing.

Χωρίς να παραβλέψουμε τον άπλετο χώρο για βελτιστοποιήσεις, μπορούμε να πούμε πλέον με ασφάλεια ότι το cloud computing αποτελεί μία από τις σημαντικότερες τάσεις στη διαχείριση και την αποθήκευση δεδομένων παγκοσμίως.

Πάνος Μητρόπουλος

General Manager

i.T.OpenSolutionS BUSINESS TECHNOLOGY

Websense Cloud Web & Email Security

Η ασφάλεια του διαδικτύου σήμερα, απαιτεί την πιο προηγμένη άμυνα -σε πραγματικό χρόνο- σε συνδυασμό με την ευκολία ανάπτυξης, μείωση λειτουργικού κόστους και την διαθεσιμότητα μιας Cloud υπηρεσίας ασφαλείας.

Οι Websense Cloud Web Security λύσεις αναλύουν το web περιεχόμενο και εντοπίζουν απειλές σε πραγματικό χρόνο μέσω του ACE (Advanced Classification Engine). Ειδικότερα, αναλύουν όλες τις εισερχόμενες και εξερχόμενες επικοινωνίες, μπλοκάρουν τις επιθέσεις από malware, ελέγχουν το botnet των επικοινωνιών και εντοπίζουν τις απειλές για την κλοπή στοιχείων. Επίσης ελέγχουν σε βάθος τα Social web applications (π.χ. Facebook, Twitter, LinkedIn, Youtube κλπ) καθώς και την κυκλοφορία HTTPS για την επικύρωση των προορισμών των web υπηρεσιών.

Η προστασία του email με την λύση Websense είναι απλή διαδικασία. Απλά, σημειώνουμε τα MX records στα datacenters της Websense και τα email καθαρίζονται πριν φτάσουν στο δίκτυο του οργανισμού, εξοικονομώντας bandwidth αφαιρώντας τα spam και τις απειλές στο cloud.

Πάνω από 89% των ανεπιθύμητων email περιέχουν συνδέσμους συχνά σε κακόβουλες τοποθεσίες (sites). Αυτό κάνει το ηλεκτρονικό ταχυδρομείο μια ανοιχτή πόρτα σε κλοπή δεδομένων. Στην πραγματικότητα, πολλές από τις μεγαλύτερες επιθέσεις στην IT ασφάλεια ενός οργανισμού, ξεκινούν από μείγμα τρωτών σημείων ηλεκτρονικού ταχυδρομείου και ιστοσελίδων. Οι λύσεις ασφαλείας ηλεκτρονικού ταχυδρομείου Cloud της Websense κλείνουν αυτή την πόρτα παρέχοντας απαράμιλλη προστασία ενάντια στις σύγχρονες στοχευμένες επιθέσεις, αναμειγνύοντας ένα από τα υψηλότερα επίπεδα προστασίας για τα εισερχόμενα και εξερχόμενα email.

Περιλαμβάνεται ενσωματωμένη κρυπτογράφηση που εξασφαλίζει την ασφάλεια του email χωρίς να θυσιάζεται η δυνατότητα να ελέγχει τα κρυπτογραφημένων email για κακόβουλο λογισμικό και παραβίαση του περιεχόμενου.

Γεώργιος Α. Κορέλλης
CEO

PhoenixPro
Built to Last.

Λύσεις ασφάλειας μέσα από το Cloud

Το απαιτητικό και ανταγωνιστικό περιβάλλον και οι δύσκολες συνθήκες στην αγορά, επιβάλλουν στις διοικήσεις εγρήγορση ως προς την ενεργή διαχείριση του ισολογισμού τους και συνεχή παρακολούθηση των πηγών κόστους και κινδύνων με ιδιαίτερη λεπτομέρεια.

Παράλληλα, οι αλλαγές στο εργασιακό καθεστώς, οι απολύσεις και οι μισθολογικές μειώσεις διαφοροποιούν με άκρως δραματικό τρόπο τη σχέση εργοδότη – υπαλλήλου, έχοντας διαλύσει την εμπιστοσύνη μεταξύ τους. Αν επιπλέον αναλογιστεί κανείς την αναπτυσσόμενη χρήση του διαδικτύου και των κινητών συσκευών και τη διαρκώς αυξανόμενη εξάρτηση των Οργανισμών από υπηρεσίες μέσω διαδικτύου, είναι φανερό πως θέματα ασφάλειας επιβάλλουν ακόμη μεγαλύτερη προσοχή και απαιτούν καινοτόμες προσεγγίσεις που προσδίδουν πραγματικό όφελος στις επιχειρήσεις.

Επομένως, τα κύρια κριτήρια που οι Διευθυντές Πληροφορικής και Ασφάλειας πρέπει να αξιολογούν σε σχέση με τις ανάγκες αγοράς, λειτουργίας και συντήρησης τεχνολογιών ασφάλειας σήμερα, είναι:

I. Αποτελεσματικότητα των τεχνολογιών που χρησιμοποιούνται – πρέπει να είμαστε προστατευμένοι!

2. Ταχύτητα υλοποίησης – η παραδοσιακή μέθοδος υλοποίησης με 4-34 εβδομάδες για υλοποίηση, δεν είναι πλέον αποδεκτή.

3. Δυνατότητα αναβάθμισης - σε αριθμό χρηστών ή επιπλέον λειτουργικότητα χωρίς νέο υλισμικό ή λογισμικό και χωρίς αλλαγές στην αρχιτεκτονική δικτύου του Οργανισμού.

4. Υποστήριξη ευρείας γκάμας κινητών συσκευών – τόσο σε σχέση με την ανάγκη για αύξηση της παραγωγικότητας, της υποστήριξης χρηστών που ταξιδεύουν (π.χ. στελέχη και πωλητές), αλλά και της νέας τάσης για Bring Your Own Device.

5. Τυποποίηση των πολιτικών ασφάλειας – για Οργανισμούς με πολλαπλά σημεία παρουσίας και χρήστες που κινούνται εκτός γραφείων, η τυποποίηση των τεχνικών πολιτικών ασφάλειας αποτελεί σημαντική πρόκληση, καθώς το παραμικρό λάθος, αβλεψία ή παράλειψη θέτουν σε κίνδυνο ολόκληρο το οικοσύστημα του Οργανισμού, λόγω του «πιο αδύναμου κρίκου». Επομένως, η υποδομή ασφάλειας πρέπει να διασφαλίζει ότι οι πολιτικές είναι κοινές και εφαρμόζονται πανομοιότυπα σε στατικά σημεία και σε κινητές συσκευές.

6. Χαμηλό κόστος ιδιοκτησίας – το συνολικό κόστος ιδιοκτησίας οποιασδήποτε τεχνολογίας και ιδιαίτερα εκείνων της ασφάλειας δεν περιορίζεται στις κεφαλαιουχικές δαπάνες αγοράς εξοπλισμού και λογισμικού, αλλά περιλαμβάνει έξοδα λειτουργίας και συντήρησης, όπως: χώρος στις καμπίνες, ηλεκτρικό ρεύμα, κλιματισμός, ηλεκτρογεννήτριες, UPS, συνδρομές λογισμικού, συνδρομές για αντικατάσταση / αποκατάσταση εξοπλισμού και βεβαίως το κόστος του προσωπικού με ευθύνη για την ασφάλεια και την καλή λειτουργία της υποδομής ασφάλειας.

Η PhoenixPro **www.phoenixpro.com** παρέχει πρωτοποριακές και άκρως καινοτόμες λύσεις ασφάλειας μέσα από το Cloud, κάτω από την οικογένεια λύσεων του **φ-Cloud** (το PhoenixPro Security-as-a-Service Cloud). Το **φ-Cloud** είναι βέλτιστα σχεδιασμένο για τις ανάγκες προστασίας της ηλεκτρονικής περιμέτρου μίας ή περισσοτέρων υποδομών των πελατών μας, με συγκεκριμένα, απτά και μετρήσιμα οφέλη: Υψηλή ηλεκτρονική ασφάλεια υποδομών και δεδομένων. Ασφάλεια για κινητές συσκευές και για απομακρυσμένη επικοινωνία σε υποδομές και συστήματα. Σημαντική μείωση του κόστους (μέχρι και 60% σε ορίζοντα 3ετίας). Υλοποίηση εντός I ημέρας. Υποστήριξη κινητών πλατφόρμων (iPhones, iPads, Android κ.λπ.). Υψηλή διαθεσιμότητα υπηρεσιών. Δεν απαιτείται αγορά υλισμικού ή λογισμικού. Δεν χρειάζονται αλλαγές στην υποδομή του Οργανισμού. Δεν απαιτείται εξειδικευμένο προσωπικό ασφάλειας. Παρέχεται (προαιρετικά) κονσόλα διαχείρισης. Αναβαθμίζεται γρήγορα (χρήστες, επιπλέον υπηρεσίες). Ασφαλή επιχειρηματικά δεδομένα. Οι λύσεις είναι ανεξάρτητες της τοποθεσίας των σημείων και των χρηστών του Οργανισμού. Δυνατότητα τυποποίησης και ταυτόσημης εφαρμογής των πολιτικών ασφάλειας παντού και πάντα. iTSecurity