

κτρονικού ταχυδρομείου στο IM (Instant Message) και στον Ιατό. Προχωρήσαμε σε αυτό το βήμα γιατί η σύγκλιση των εφαρμογών θολώνει τα όρια ανάμεσα στις διάφορες μεθόδους επικοινωνίας. Το προϊόν μας για την ασφάλεια του VoIP είναι η φυσική εξέλιξη της τεχνολογίας ασφαλείας, από το επίπεδο εφαρμογών μέχρι την ανταλλαγή μηνυμάτων σε πραγματικό χρόνο, και επιτρέπει στη Borderware να διασφαλίζει όλες τις συγκλινόμενες εφαρμογές μηνυμάτων. Το SIPassure Firewall παρέχει λύσεις για την ασφάλεια των SIP εφαρμογών VoIP και τηλεδιάσκεψης, καθώς και των instant messaging εφαρμογών που βασίζονται σε SIP. Το SIPassure αποτελεί μέρος μιας ευρύτερης σειράς προϊόντων για την ασφάλεια των δικτύων, τα οποία μαζί παρέχουν ασφάλεια για την πλήρη σειρά των εφαρμογών μηνυμάτων.

nw: Ποια είναι τα χαρακτηριστικά της λύσης που προσφέρει η Borderware;

P. Cox: Το SIPassure Firewall της Borderware παρέχει εφαρμογές ασφαλείας και NAT traversal υπηρεσίες για SIP και τα σχετικά πρωτόκολλα που είναι απαραίτητα για την υποστήριξη VoIP, τηλεδιάσκεψης και SIP based IM. Το SIPassure ελέγχει και πιστοποιεί την ταυτότητα των χρηστών VoIP πριν επιτρέψει απόρρητες ή επισφαλείς διαδικασίες, ελέγχει την εγκυρότητα όλων των εντολών και αιτημάτων, διακρίνει ανεπιθύμητες κλήσεις ρυθμίζοντας VoIP spam και διασφαλίζει το περιεχόμενο των πληροφοριών με υπηρεσίες κρυπτογράφησης.

Το SIPassure κατασκευάζεται στο αποδεδειγμένα ασφαλές λειτουργικό σύστημα της Borderware, το οποίο χρησιμοποιείται από την εταιρεία σε όλα τα περιμετρικά προϊόντα ασφαλείας τα τελευταία 13 χρόνια και έχει κερδίσει τρία Common Criteria EAL4 πιστοποιητικά. Το EAL4 πιστοποιητικό αντιπροσωπεύει ένα υψηλό επίπεδο πιστοποίησης ασφαλείας, το επίπεδο που απαιτείται από πολλές κυβερνήσεις και στρατιωτικούς οργανισμούς για την επιλογή περιμετρικών προϊόντων ασφαλείας, τα οποία θα διαχειριστούν ευαίσθητα δεδομένα.

nw: Πόσο εύκολη είναι η εγκατάσταση της συγκεκριμένης λύσης;

P. Cox: Το SIPassure διατίθεται σαν μία συσκευή που μπορεί να συνδεθεί ανάμεσα σε ένα εταιρικό δίκτυο ή ένα δίκτυο παροχής υπηρεσιών και ένα λιγότερο ασφαλές δίκτυο (π.χ. το Internet) και εναρμονίζεται λειτουργικά σε λίγα λεπτά μέσω ενός απλού wizard εγκατάστασης.

nw: Τα δεδομένα μπορούν να κρυπτογραφηθούν. Πώς μπορεί κάποιος να κρυπτογρα-

φήσει τη φωνή χωρίς εκπτώσεις στην ποιότητα; Η ταχύτητα επηρεάζεται από την αυξημένη ασφάλεια;

P. Cox: Υπάρχουν δύο πτυχές στην εξασφάλιση των VoIP κλήσεων ή άλλων εφαρμογών επικοινωνίας σε πραγματικό χρόνο με υπηρεσίες κρυπτογράφησης. Η πρώτη αφορά στη δημιουργία των πρωτοκόλλων της κρυπτογράφησης των κλήσεων, η οποία είναι κρίσιμης σημασίας. Αν δεν προστατευτεί, τότε υπάρχει ο κίνδυνος τηλεφωνικής εξαπάτησης, να κρυφακούσει κάποιος ή να πραγματοποιηθούν άλλες επιθέσεις, όπως απάτη κόστους κλήσεων, ενώ ακόμα και το spam είναι πιθανό. Η δεύτερη αφορά φυσικά στην κρυπτογράφηση του media stream (φωνή, βίντεο κ.λπ.). Η κρυπτογράφηση της σηματοδότησης είναι σχετικά απλή. Οι εφαρμογές που βασίζονται στο SIP μπορούν να χρησιμοποιήσουν μία σύνδεση TLS για να προστατεύσουν την κίνηση των σημάτων (TLS είναι η επίσημη ονομασία για το SSL, τη γνωστή τεχνολογία κρυπτογράφησης που χρησιμοποιούν όλοι οι browsers).

Η κρυπτογράφηση του media stream είναι δυσκολότερη, καθώς, όπως η ερώτηση υπονοεί, οι υπηρεσίες κρυπτογράφησης θα επιβραδύνουν τις υπηρεσίες ασφαλείας. Η απάντηση σε αυτό το πρόβλημα είναι η υιοθέτηση μιας τεχνολογίας ασφαλείας, η οποία είναι κλιμακώσιμη και μπορεί να υποστηρίξει υπηρεσίες κρυπτογράφησης του media stream. Το SIPassure της Borderware στηρίζεται σε μια τμηματική αρχιτεκτονική. Με το SIPassure η σηματοδότηση και το media stream μπορούν να "τρέξουν" σε διαφορετικές συσκευές, επιτρέποντας την εγκατάσταση κλιμακώσιμων συστοιχιών με μερικούς κόμβους για τη διαχείριση της σηματοδότησης ασφαλείας του SIP και με άλλους για τη διαχείριση της ασφαλείας του media stream, συμπεριλαμβανομένης της κρυπτογράφησης. Με το σωστά σχεδιασμένο προϊόν, η ασφάλεια δεν οδηγεί σε υποβάθμιση υπηρεσιών.

nw: Η αυξημένη ασφάλεια θα επηρεάσει το κόστος του VoIP; Θα αυξήσει το συνολικό κόστος κτήσης (TCO);

P. Cox: Το αντίθετο. Η παρεχόμενη ασφάλεια θα μειώσει το TCO των VoIP υπηρεσιών. Η επαρκής και κατάλληλη ασφάλεια επιτρέπει τη διάδοση της υπηρεσίας. Πολλές VoIP εγκαταστάσεις περιορίζονται στα εταιρικά δίκτυα ή στα δίκτυα των πανεπιστημιούπολων.

Οι διαχειριστές των δικτύων είναι διστακτικοί να "ανοίξουν" τα VoIP δίκτυά τους για να πραγματοποιούν και να δέχονται κλήσεις μέσω Internet. Παρόλο που αυτή η διστακτικότητα είναι κατανοητή, περιορίζει τις δυνατότητες του

VoIP. Η ανάθεση των ζητημάτων ασφαλείας σε ένα σωστά σχεδιασμένο προϊόν μιας εταιρείας με αποδεδειγμένη εμπειρία στην κατανόηση και το φράξιμο των απειλών μέσω Internet, επιτρέπει την εκμετάλλευση όλων των δυνατοτήτων των υπηρεσιών VoIP.

Έπειτα, πολλές μελέτες έχουν εξετάσει και έχουν προσπαθήσει να υπολογίσουν το κόστος από τις παραβιάσεις της ασφαλείας των δικτύων. Παρόλο που είναι πάντα δύσκολο να προκύψουν ακριβή στοιχεία, όλες οι έρευνες και μελέτες συμφωνούν ότι το κόστος είναι πάντα σημαντικό. Το κόστος αυτό συνίσταται τόσο από το άμεσο κόστος που προκύπτει από τις παραβιάσεις στο δίκτυο, όσο και από έμμεσα κόστη που προκύπτουν από ζημιές στις δραστηριότητες και τη φήμη του οργανισμού ή της επιχείρησης. Σωστά σχεδιασμένα και εφαρμοσμένα συστήματα ασφαλείας μειώνουν πάντα το πραγματικό TCO τέτοιων εφαρμογών, καθώς προλαμβάνουν το κρυφό κόστος από παραβιάσεις της ασφαλείας. Η εικόνα για τους παρόχους υπηρεσιών είναι ακόμα πιο ξεκάθαρη. Εξ' ορισμού, δεν μπορούν να περιορίσουν τις VoIP εφαρμογές στο δικό τους δίκτυο. Τα VoIP δίκτυα των παρόχων υπηρεσιών είναι "αναγκασμένα" να πραγματοποιούν και να δέχονται εξωτερικές κλήσεις από την πρώτη μέρα. Επιπλέον, καμία εταιρεία παροχής υπηρεσιών δεν μπορεί να ρισκάρει ζημιά στη φήμη της ή τις δραστηριότητές της από τις αναπόφευκτες παραβιάσεις της ασφαλείας.

nw: Πού βλέπετε το μέλλον της ασφαλείας VoIP;

P. Cox: Το μέλλον της ασφαλείας VoIP βρίσκεται σαφώς στις απαιτήσεις της ασφαλείας που βασίζονται στα πρότυπα των VoIP εφαρμογών. Τα πρότυπα των εφαρμογών είναι απαραίτητα να προωθούν τη διαλειτουργικότητα, η οποία είναι κρίσιμης σημασίας για τη μακροπρόθεσμη επιτυχία του VoIP.

Επιπλέον, θα δούμε την εξάπλωση των VoIP υπηρεσιών και εφαρμογών και σε άλλους τομείς - όπως το ζήτημα της σύγκλισης στο οποίο αναφερθήκαμε παραπάνω. Επιτυχημένες λύσεις ασφαλείας θα ακολουθήσουν αυτό το μονοπάτι της σύγκλισης.

|nw

www.btc06.gr

Περισσότερες πληροφορίες, πρόγραμμα και δηλώσεις συμμετοχής για το Business Telecommunications θα βρείτε στο www.btc06.gr, ενώ μπορείτε να επικοινωνήσετε και με το Βασίλη Κουτσαβλή στο τηλ. 210 661 77 77 (εσωτ. 123), vkoutsavlis@boussias.com.