ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Η ΟΡΓΑΝΩΣΗ ΤΗΣ ΑΜΥΝΑΣ ΔΕΝ ΑΡΧΙΖΕΙ ΑΠΟ ΤΟΝ ΕΞΟΠΛΙΣΜΟ, ΑΛΛΑ ΑΠΟ ΤΟΝ ΚΑΝΟΝΙΣΜΟ ΠΕΙΘΑΡΧΙΑΣ, ΔΙΟΤΙ, ΠΟΛΥ ΑΠΛΑ, ΧΩΡΙΣ ΑΥΤΟΝ ΕΙΜΑΣΤΕ «ΑΤΑΚΤΟΙ»

Μπορεί να φταίνε οι συχνές επιθέσεις από τους διάφορους hacker, ίσως η πίεση του να είσαι πρώτος στην αγορά και η υιοθέτηση μη δοκιμασμένων μεθόδων ή το κλίμα τρομολαγνείας που καλλιεργείται πολλές φορές από τον Τύπο..... Το αποτέλεσμα είναι ότι οι εταιρείες ξοδεύουν όλο και περισσότερα για την ασφάλειά τους. Πόσα; Σύμφωνα με μια έρευνα της Datamonitor, εκτιμάται ότι, καθώς οι ζημιές που προξενούνται από προβλήματα ασφάλειας κοστίζουν στις επιχειρήσεις περισσότερα από 15 δισεκατομμύρια δολάρια ετησίως, οι δαπάνες για μέτρα ασφαλείας θα φτάσουν έως το 2005 το 30,3 δισεκατομμύρια δολάρια, παγκοσμίως. Άρα το θέμα τήρησης των μέτρων ασφάλειας κάθε άλλο παρά ασήμαντο είναι για τις επιχειρήσεις.

Τι είναι μια πολιτική ασφαλείας;
Η πολιτική ασφαλείας μια e-επιχείρισης είναι ο «Κώδικας Οδικής Κυκλοφορίας» στο εταιρικό δίκτυο. Είναι το κείμενο στο οποίο θα ανατρέξουν οι εργαζόμενοι, αν δεν ξέρουν πώς να πορευτούν στο εσωτερικό και εξωτερικό κυβερνοχώρο, αυτό που θα τους πει ποια είναι η «σωστή συμπεριφορά». Είναι το κείμενο στο οποίο θα καταφύγει και η διεύθυνση της επιχείρησης, όταν θα χρειαστεί να να αποφασίσει αν κάποιος εργαζόμενός τησυπέπεσε σε παράπτωμα και να αποφασίσει για την τιμωρία του. Η πολιτική ασφαλείας είναι ένα σύνολο κανόνων θεσπισμένων από την ανώτερη διοίκηση της κάθε επιχείρησης, που οριοθετούν με σαφή και αυστηρό τρόπο τις αρμοδιότητες και τις υποχρεώσεις των εργαζομένων της σε θέματα ασφαλείας, έτσι ώστε σε κάθε περίπτωση να διασφαλίζεται ότι η διαχείριση των δεδομένων και των πληροφοριών θα είναι ορθή. Η πολιτική αυτή καθορίζει ποιος είναι εξουσιο-δοτημένος να έχει πρόσβαση στα διάφορα είδη πληροφοριών, ποια και πόσο αυστηρά μέτρα ασφαλείας είναι αναγκαία.
Ως κείμενο η πολιτική ασφαλείας της όλης επιχείρησης χρειάζεται να είναι αρκετά μικρό, ιδιαίτερα περιεκτικό, περί τις τρεις με πέντε σελίδες. Προσοχή θα πρέπει να δοθεί στη γλώσσα και στην ορολογία που θα χρησιμοποιηθεί, αφού θα πρέπει να διαβαστεί από όλους του υπαλλήλους της επιχείρησης. Τέλος, όλο το κείμενο χρειάζεται να είναι γραμμένο με τέτοιο τρόπο, ώστε να επιδέχεται αλλαγές στη δομή της επιχείρησης και στην υιοθέτηση νέων τεχνολογιών, έχοντας τελικά διάρκεια ζωής τριών ή περισσότερων ετών.
Πώς όμως μπορεί να γράψει κανείς ένα κείμενο που θα απαιτεί ελάχιστες αλλαγές μετά την ολοκλήρωσή του; Το κλειδί είναι η πολιτική ασφαλείας να αναφέρεται ρητά σε σχετικά έγγραφα που περιλαμβάνουν τα όποια πρότυπα, κατευθύνσεις και διαδικασίες. Αυτά θα περιέχουν εκτενείς τεχνικές και διαδικαστικές λεπτομέρειες. Έτσι, αν, για παράδειγμα, αλλάξει κάποιο υπολογιστικό σύστημα, δεν θα είναι ανάγκη να επέμβουμε σε αυτή καθαυτή την πολιτική, αλλά στο έγγραφο που αναφερόταν στο συγκεκριμένο σύστημα. Η πολιτική είναι στην ουσία ένας καταστατικός χάρτης για την εφαρμογή της ασφάλειας και τα σχετικά έγγραφα παρέχουν τη μέθοδο εφαρμογής.
Πλέον, όλες σχεδόν οι σύγχρονες επιχειρήσεις έχουν μια πολιτική ασφαλείας. Συνήθως αυτή είναι καταγραμμένη, ενώ σε αρκετές επιχειρήσεις απαρτίζεται περισσότερο από μια σειρά άτυπων κανόνων. Βέβαια, κατ'αυτό τον τρόπο υπάρχει πάντα η πιθανότητα και να μη γίνεται σεβαστή από τους εργαζόμενους και να μην

μπορούν να επιβληθούν κυρώσεις. Το να έχει η επιχείρηση την πολιτική ασφαλείας καταγραμμένη της δίνει μια βάση για σωστή κατανόηση και εφαρμογή της, και προμηθεύει το προσωπικό ασφαλείας με ένα συγκεκριμένο σύνολο κανόνων για να εκτελούν τα καθήκοντά τους.
Ποιος όμως θα γράψει την πολιτική ασφαλείας μιας επιχείρησης ή ενός οργανισμού; Η καλύτερη λύση είναι μια μικρή ομάδα, που θα αποτελείται από ένα τουλάχιστον υψηλόβαθμο στέλεχος της επιχείρησης, τους διαχειριστές των συστημάτων ασφαλείας, τους διευθυντές του τμήματος MIS, νομικούς και, τέλος, εσωτερικούς και εξωτερικούς συμβούλους.
Όταν πλέον η πολτική γραφτεί, απομένει μόνο η έγκρισή της. Καθώς μια πολιτική ασφαλείας μοιάζει με καταστατικό χάρτη και ενσωματώνει θεμελιώδεις επιχειρηματικές πρακτικές, θα πρέπει να εγκριθεί να υπογραφεί από τον υψηλότερα ιστάμενο, κατά προτίμηση από το γενικό διευθυντή. Αν ένα χαμηλόβαθμο στέλεχος ή έστω και ο διευθυντής ασφάλειας υπογράψει την πολιτική, τότε τα υπόλοιπα τμήματα και οι εργαζόμενοί τους μπορεί να αντισταθούν ή να την αγνοήσουν. Αν συμβεί κάτι τέτοιο, τότε το συγκεκριμένο έγγραφο θα είναι περισσότερο μια πρόταση παρά μια πολιτική και, μολονότι θα παρέχει κάποιες αρχές για εθελοντική συμμόρφωση, δεν θα αποτελεί μια «διαταγή».
Σίγουρα δεν υπάρχει ούτε πρόκειται να υπάρξει κάτι ως γενική πολιτική ασφαλείας που να ταιριάζει στην κάθε επιχείρηση. Η πολιτική πρέπει να σχετίζεται άμεσα με τις επιχειρηματικές ανάγκες της εκάστοτε επιχείρησης και να είναι απόρροια των ειδικών συνθηκών του κάθε κλάδου. Άλλες, για παράδειγμα, είναι οι απαιτήσεις και οι ανάγκες μιας βιομηχανίας όπλων που πραγματοποιεί άκρως μυστική έρευνα και άλλες αυτές ενός βιντεοκλάμπ.
Έτσι, ενώ η βιομηχανία όπλων θα απασχολείται πιθανότατα περισσότερο με το πώς θα προστατέψει τα απόρρητα δεδομένα της, το βιντεοκλάμπ θα θέλει απλώς να είναι σίγουρο ότι τα στοιχεία που αφορούν στις κρατήσεις και στα λογιστικά θα είναι ακριβή και δεν θα έχουν υποστεί καμία «παρέμβαση».
Παρ'όλο όμως που η πολιτική ασφαλείας είναι κάτι υποκειμενικό και μπορεί να διαφέρει πολυ από επιχείρηση σε επιχείρηση, υπάρχουν κάποια κοινά θέματα που μπορούμε να τα προδιαγράψουμε:

- **Φυσική ασφάλεια**

Η ασφάλεια των δικτύων έχει άμεση σχέση με την ασφάλεια σε φυσικό επίπεδο. Επειδή το μέγεθος ή το σχήμα ενός δικτύου δεν είναι κάτι περιορισμένο, αλλά μπορεί να επεκτείνεται σε ένα ολόκληρο κτίριο, σε μια περιοχή, σε μια χώρα ή σε ολόκληρο τον κόσμο, καταλαβαίνουμε ότι η προστασία του είναι σημαντική και δύσκολη. Χωρίς τη φυσική ασφάλεια, τα άλλα προβλήματα της ασφάλειας των δικτύων –όπως η εμπιστοσύνη, η διαθεσιμότητα και η ακεραιότητα- απειλούνται σε μεγάλο βαθμό. Το κομμάτι που αφορά στη φυσική ασφάλεια καθορίζει πώς θα πρέπει να προστατεύονται οι διάφορες εγκαταστάσεις και το hardware που βρίσκεται μέσα σε αυτές, ή ποιοι εργαζόμενοι θα έχουν πρόσβαση σε περιορισμένες περιοχές, όπως δωμάτια διακομιστών ή περιοχές καλωδιώσεων.

- **Ασφάλεια δικτύου**

Στο τμήμα αυτό ορίζεται πώς θα προφυλάσσονται οι διάφοροι πόροι που είναι αποθηκευμένοι στο δίκτυο και αναφέρεται κυρίως στα δεδομένα. Σε αυτό μπορούν επίσης να περιληφθούν και τα μέτρα ασφαλείας για τα firewall, την πρόσβαση εκ του μακρόθεν, τις υπηρεσίες καταλόγου, τις υπηρεσίες Internet κ.λπ.

- **Έλεγχος πρόσβασης**

Ο έλεγχος πρόσβασης έχει σχέσημε τον καθορσμό του ποιος έχει πρόσβαση σε τι. Πρέπει να υάρχει μαι σωστή διαδικασία για να εξασφαλίζεται ότι μόνο οι κατάλληλοι

άνθρωποι θα έχουν πρόσβαση στις κατάλληλες πληροφορίες ή υπηρεσίες. Ο σωστός έλεγχος πρόσβασης παρέχει στους διαχειριστές τη δυνατότητα να είναι αποτελεσματικοί στην εργασία τους. Δεν χρειάζεται να είναι υπαρβολικά περίπλοκος, γιατί τότε κινδυνεύουμε να έχουμε τα αντίθετα αποτελέσματα.

- **Πιστοποίηση ταυτότητας**

Η πιστοποίηση αφορά στον τρόπο με τον οποίο οι χρήστες «λένε» στο δίκτυο ποιοι είναι. Ο τύπος και ο τρόπος της πιστοποίησης που χρησιμοποιείται κάθε φορά ποικίλλουν ανάλογα με το σημείο από όπου οι χρήστες θέλουν να πιστοποιηθούν: π.χ., από το γραφείο τους, μια απλή ταυτότητα χρήστη και ένας κωδικός ενδέχεται να αρκούν, λόγω και της επιπρόσθετης φυσικής ασφάλειας που υπάρχει (δεν μπορεί να εισέλθει ο οποιοσδήποτε σε ένα γραφείο μιας επιχείρησης). Όταν όμως επιχειρείται μια απομακρυσμένη σύνεση μέσω του Internet, ένας πιο ασφαλής και αυστηρός τρόπος είναι αναγκαίος.

- **Κρυπτογράφηση**

Η κρυπτογράφηση μπορεί να εξασφαλίσει την ακεραιότητα των δεδομένων και να προστατέψει ευαίσθητες πληροφορίες που στέλνονται μέσω μη ασφαλών συνδέσεων. Αυτού του είδους η προστασία είναι συνήθως απαραίτητη για την απομακρυσμένη πρόσβαση σε σημαντικούς πόρους, ή ως μια επιπρόσθετη προστασία, όταν χρησιμοποιείται το Intranet της επιχείρησης.

- **Διαχείριση «κλειδιών»**

Τα «κλειδιά» χρησιμοποιούνται για την κρυπτογράφηση ή την αποκρυπτογράφηση των δεδομένων. Ένα σοβαρό θέμα είναι η διαχείριση και η προστασία των κλειδιών. Μια σωστή πολιτική πρέπει να θεσπιστεί για τη διαχείριση των παρακάτω θεμάτων, καθώς αυτά επηρεάζουν τελικά σε μεγάλο βαθμό την αποτελεσματικότητα της κρυπτογράφησης. Συνήθη θέματα στον τομέα αυτό είναι τα εξής:

1. Μήκος κλειδιού-πόσο μακρύ;
2. Αλλαγή κλειδιού-πόσο συχνή;
3. Παραγωγή κλειδιών-ποιος, πώς;
4. Διανομή κλειδιών-ποιος, πως;

- **Συμμόρφωση**

Το τμήμα της συμμόρφωσης εξηγεί πώς θα πρέπει να γίνεται η επιβολή της πολιτικής ασφαλείας. Μπορεί επίσης να καθορίζει τους τρόπους και τις μεθόδους που θα χρησιμοποιούνται για να ερευνώνται οι όποιες παραβιάσεις της ασφάλειας. Οι όποιες κυρώσεις (οικονομικές, διοικητικές, νομικές) σε περιπτώσεις καταπάτησης της πολιτικής ασφαλείας μπορούν επίσης να αναφέρονται σε αυτό το κομμάτι.

- **Έλεγχος και αναθεώρηση**

Αφού δημιουργηθεί μια πολιτική ασφαλείας, πρέπει να ελεγθεί γτια να εξασφαλιστεί ότι όλα τα συστατικά της είναι σε συμφωνία. Ένας οργανισμός, για παράδειγμα, με ελλιπή έλεγχο ίσως να μην έχει καμία νομική διέξοδο, αν συμβεί μια παραβίαση ασφάλειας. Με τον έλεγχο είναι δυνατόν επίσης να αναγνωριστούν προβλήματα και παραλείψεις πριν αυτά μετατραπούν σε παραβιάσεις. Οι πολιτικές θα πρέπει ακόμη να αναθεωρούνται τακτικά για να εξασφαλίζεται ότι παραμένουν ενημερωμένες και σύμφωνες με τα δεδομένα και τις απατήσεις τόσο της επιχείρησης όσο και του περιβάλλοντός της.

- **Ενημέρωση ασφάλειας**

Οι «αδαείς χρήστες» θεωρούνται από όλους η πιο σοβαρή απειλή στην ασφάλεια μιας επιχείρησης. Αν οι ίδιοι οι εργαζόμενοι δεν κατανοούν πλήρως την ανάγκη σωστής χρήσης του δικτύου, μπορούν ακόμη και άθελά τους να θέσουν σε κίνδυνο την ασφάλειά του. Συγκεκριμένα, πρέπει να διαχειρίζονται σωστά τους κωδικούς ασφάλειας που τους έχουν δοθεί και να είναι προσεκτικοί στις λεγόμενες

«κοινωνικές» επιθέσεις (σε αυτές τις περιπτώσεις κάποιο άτομο, γνωστό με τον εργαζόμενο, προσπαθεί να πάρει πληροφορίες, όπως κωδικοί πρόσβασης, χρησιμοποιώντας ως μέσο τη σχέση του με αυτόν).

- **Σχέδιο αντιμετώπισης κρίσεων**

Ένας οργανισμός είναι περισσότερο ευπρόσβλητος μετά την ανακάλυψη μιας διείσδυσης στα συστήματά του ή όταν αντιμετωπίζει μια καταστροφή. Τα γεγονότα που θα συμβούν τα επόμενα λεπτά ή τις επόμενες ώρες από τη στιγμή της παραβίασης ίσως είναι αποφασιστικής σημασίας για το αν θα σωθούν η πνευματική ιδιοκτησία της επιχείρησης και η υπόληψή της, ή και κάποιες φορές η ίδια της η ύπαρξη. Το πλάνο εξηγεί πώς ένας οργανισμός θα αντιμετωπίσει οποιασδήποτε μορφής φυσική καταστροφή ή επίθεση, συμπεριλαμβανομένων των επιθέσεων από hacker αλλά και από παραλείψεις εργαζομένων. Μπορεί, για παράδειγμα, να περιλαμβάνει μέτρα ασφαλείας για το back up των διακομιστών, να περιγράφει με λεπτομέρειες πόσο συχνά θα πρέπει να πραγματοποιούνται τα back up, πώς και πού θα πρέπει να αποθηκεύονται τα εφεδρικά δεδομένα. Το πλάνο είναι δυνατόν επίσης να περιλαμβάνει μια λίστα με άτομα τα οποία θα αποτελούν την ομάδα έκτακτης ανάγκης που θα χειριστεί μια φυσική καταστροφή ή επίθεση. Επιπλέον, ενδέχεται να περιέχει μέτρα ασφαλείας για τη διεξαγωγή ασκήσεων, ώστε να διαπιστωθεί ότι όλοι οι χρήστες και η ομάδα έκτακτης ανάγκης γνωρίζουν τι να κάνουν εάν μια επίθεση ή καταστροφή λάβει χώρα.

- **Πολιτική ορθής χρήσης**

Το τμήμα αυτό καθορίζει πώς θα επιτρέπεται στους χρήστες να χρησιμοποιούν τους πόρους του δικτύου. Είναι πιθανόν, για παράδειγμα, να περιγράφει τους τύπους πληροφοριών που μπορούν να επισυνάπτονται στα μηνύματα μέσω e-mail (attachments) και να εξηγεί πότε και ποια e-mail πρέπει να κρυπτογραφούνται. Επίσης, είναι δυνατόν να καθορίζει θέματα, όπως οι χρήστες επιτρέπεται να παίζουν παιχνίδια στον υπολογιστή τους ή να χρησιμοποιούν τα e-mail και την πρόσβαση στο Internet για προσωπική τους χρήση.

- **Ασφάλεια λογισμικού**

Εδώ εξηγείται πώς η επιχείρηση θα αξιοποιεί το κάθε εμπορικό και μη λογισμικό στους διακομιστές της, στους σταθμούς εργασίας και στο δίκτυο γενικότερα. Αυτό το τμήμα μπορεί ακόμη να καθορίζει ποιος επιτρέπεται να αγοράσει λογισμικό, ποιος να το εγκαθιστά και τα μέτρα ασφαλείας για το «κατέβασμα» λογισμικού από το Internet.

ΟΙ «ΔΕΚΑ ΕΝΤΟΛΕΣ» ΓΙΑ ΤΟ ΧΤΙΣΙΜΟ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

1. **Προσδιόρισε και εντόπισε τους πόρους σου**

Υπολόγισε-ή τουλάχιστον εκτίμησε-τη σπουδαιότητα αλλά και την αξία του πληροφορικού εξοπλισμού.

Παράδειγμα: Ένας υπολογιστής ή κάποιο σύστημα μπορεί να κοστίζει 5.000.000 δραχμές για να αντικατασταθεί. Οι πληροφορίες όμως που υπάρχουν αποθηκευμένες σε αυτό μπορεί να αξίζουν 100 φορές περισσότερο.

2. **Εκτίμησε τον πιθανό κίνδυνο**

Κατηγοριοποίησε την πιθανότητα αυτά τα αγαθά να κλαπούν και προσδιόρισε την επικείμενη ζημιά στον οργανισμό-επιχείρηση, αν συμβεί κάτι τέτοιο.

Παράδειγμα: Αν μια εταιρεία έχει έναν Web server ο οποίος χρησιμοποιείται για να παρέχει πληροφορίες, το κόστος στην περίπτωση που θα «πέσει» από μια επίθεση μπορεί να είναι ο χρόνος που θα χρειαστεί να επανέλθει το σύστημα στην κανονική του λειτουργία (π.χ., δύο ώρες εργασίας από το τμήμα MIS). Αν με αυτό τον Web

server πραγματοποιούνται και οικονομικές συναλλαγές, τότε το κόστος μπορεί να περιλαμβάνει και τον αριθμό των συναλλαγών που δεν έγιναν όταν ο server ήταν εκτός λειτουργίας, ή και το κόστος από τη δυσφήμιση στην οποία υπόκειται η εταιρεία.

3. Έλεγξε τη φυσική πρόσβαση στους πόρους σου

Σε συμφωνία με τις περιγραφές των πόρων (βήμα πρώτο) μπορείς είτε να εγκαταστήσεις κάποια εξαιρετικά πολύτιμα αγαθά-πόρους σε κάποιο άλλο πιο ασφαλές σημείο ή να λάβεις πρόσθετα μέτρα στην παρούσα τοποθεσία (επιπλέον κλειδαριές, έξυπνες κάρτες, φύλαξη από φρουρούς κ.λπ.) για τη φύλαξη αυτών των αγαθών. Η συγκεκριμένη συμβουλή αναφέρεται σε φυσικούς περιορισμούς, καθώς δεν αρκεί μόνο η ψηφιακή τους προστασία αλλά απαιτείται και η φυσική.

Παράδειγμα: Συχνά είναι καλή ιδέα να τοποθετείς όλους τους σημαντικούς server σε ένα ξεχωριστό δωμάτιο με περιορισμούς σε ό,τι αφορά τη φυσική πρόσβαση. Αυτό μειώνει την πιθανότητα κάποιος να πραγματοποιήσει κάποια υποκλοπή ή παράνομη εξαγωγή πληροφοριών ή να προξενήσει υλικές ζημιές έστω και άθελά του.

4. Κατηγοριοποίησε τη σπουδαιότητα των πληροφοριών σου

Γνωστές κατηγοριοποιήσεις που χρησιμοποιούνται στις διάφορες επιχειρήσεις στις μέρες μας είναι: άκρως απόρρητο, απόρρητο, εμπιστευτικό, ιδιωτικό, κοινό κ.λπ. Ελέγχοντάς τες θα είναι ευκολότερο να καθορίσεις σε ποια είδη πληροφοριών, ποιοι υπάλληλοι ή ποια τμήματα της επιχείρησής του θα έχουν πρόσβαση, αφού όλες οι πληροφορίες σου θα φέρουν κάποιο χαρακτηρισμό.

Παράδειγμα: Ένα διαφημιστικό πλάνο μπορεί να είναι απόρρητο για συγκεκριμένους ανθρώπους στα τμήματα μάρκετινγκ και ανάπτυξης. Ένα έγγραφο του τμήματος παραγωγής με λεπτομέρειες σχετικά με διάφοροες διεργασίες της παραγωγής ίσως είναι προσβάσιμο μόνο σε καθορισμένους μηχανικούς και διευθυντές. Είναι ακόμη αναγκαίο να ελέγχονται κάθε έγγραφο που δημιουργείται, και όλη η πορεία του. Ποιος έχει, δηλαδή, τη δυνατότητα να το εκτυπώνει, πόσες φωτοτυπίες θα γίνουν και ποιος μπορεί θα τις έχει. Η πολιτική της εταιρείας θα πρέπει να είναι ιδιαίτερα αυστηρή σε παραβάσεις που αφορούν σε αυτά τα θέματα.

5. Διαπίστωσε ποιος χρειάζεται πρόσβαση σε πόρους

Καθόρισε κατ' αρχάς με ποιον τρόπο θα γίνεται η πρόσβαση (μέσω του Internet, modem, WAN κ.λπ.) και ποιοι πόροι θα πρέπει να διατίθενται. Εξακρίβωσε ποιος/οι από τους χρήστες (εργαζόμενοι, συνεργάτες, πελάτες, το κοινό) χρειάζεται να έχει πρόσβαση σε πόρους και πηγές εντός ή εκτός της εταιρείας και ποιες πηγές πρέπει να γίνουν διαθέσιμες. Μολονότι είναι δύσκολο, ίσως είναι ανάγκη να υιοθετήσεις αυστηρές πολιτικές σχετικά με το «κατέβασμα» και την εγκατάσταση προγραμμάτων από το Διαδίκτυο και ιδιαίτερα από άγνωστους κατασκευαστές. Εάν αυτό δεν είναι δυνατόν, τότε ένα αντι-ιικό λογισμικό θα πρέπει να ελέγχει όλους τους υπολογιστές του δικτύου, συνεχώς ή σε τακτά διαστήματα.

6. Δημιούργησε ένα πλάνο έκτακτης ανάγκης

Αυτό θα σε αναγκάσει να σκεφτείς πώς θα κάνεις back-up των πληροφοριών σου ή να αναθεωρήσεις τον ήδη υπάρχοντα τρόπο. Πολύ σημαντικός επίσης, εκτός από το back-up, είναι και ο χώρος αποθήκευσης αυτών των πληροφοριών. Τα εφεδρικά δεδομένα θα πρέπει να αποθηκεύονται σε σημεία εκτός δικτύου, και ακόμη καλύτερα σε τοποθεσίες εκτός του ίδιου κτιρίου με τις αρχικές πληροφορίες. Το πλάνο αυτό χρειάζεται να ασχολείται με την απώλεια των δεδομένων και του εξοπλισμού.

Παράδειγμα: Έστω ότι συνέβη το χειρότερο: οι εγκαταστάσεις καταστράφηκαν ολοσχερώς, μαζί με τα πρωτεύοντα δεδομένα. Με ποιον τρόπο θα συνεχίσεις να δουλεύεις και να εξυπηρετείς του πελάτες σου; Αυτή η άσκηση θα σε βοηθήσει να επισημάνεις τα δεδομένα και τον εξοπλισμό που είναι κρίσιμος για την απρόσκοπτη

λειτουργία της επιχείρησης. Επίσης, θα σε αναγκάσει να σκεφτείς ορισμένα θέματα, όπως για πόσο διάστημα μπορεί η επιχείρησή σου να παραμείνει εκτός λειτουργίας χωρίς να υποστείς ανεπανόρθωτη ζημιά.

7. Όρισε υπεύθυνο για την εφαρμογή της πολιτικής ασφαλείας

Μπορεί να είναι ένα άτομο ή μια ομάδα ατόμων. Οι αρμοδιότητες και οι λειτουργίες τους πρέπει να είναι αυστηρά καθορισμένες.

Παράδειγμα: Ο διαχειριστής των δικτύων μπορεί να είναι ο υπεύθυνος για την πρόσβαση στο Internet και για άλλες σχετικές λειτουγρίες του τμήματος πληροφορικής, ενώ ένα άτομο από το τμήμα ανθρώπινων πόρων θα είναι υπεύθυνο για την ασφάλεια των χώρων (συντήρηση συστημάτων πυρασφάλειας, διανομή καρτών πρόσβασης και κωδικών). Η επιλογή των ατόμων θα πρέπει να είναι τέτοια, ώστε να αποκλείονται αλληλοκαλύψεις και συγκρούσεις.

8. Εξέτασε την επίδραση των νέων διαδικασιών στους εργαζόμενους

Αξιολόγησε τις προϋποθέσεις υπό τις οποίες οι εργαζόμενοι θα κλειδώνουν τους υπολογιστές και τα δεδομένα τους, θα κλείνουν και θα εκκινούν συστήματα ασφαλείας, θα θέτουν και θα αλλάζουν κωδικούς πρόσβασης. Γενικότερα, με ποιον τρόπο θα εστερνιστούν μια κουλτούρα προσανατολισμένη στην ασφάλεια και στην προσοχή και θα εξοικειωθούν με νέες διαδικασίες και συνήθειες;

9. Ανάθεσε σε τρίτους την ασφάλειά σου, αν δεν νιώθεις σίγουρος

Μην επενδύεις σε κάτι, αν δεν έχεις αρκετή γνώση και εμπειρία γι'αυτό, το οποίο πιθανότατα δεν θα φέρεις εις πέρας. Καλύτερα να κάνεις outsourcing την ασφάλεια της επιχείρησής σου-και μάλιστα στον καλύτερο της αγοράς-παρά να ξοδέψεις υπερβολικά χρήματα για κάτι που αμφιβάλλεις πώς πρέπει να γίνει.

10. Κατανόησε ότι η εφαρμογή πολιτικής ασφαλείας απαιτεί τακτική επιβεβαίωση

Έλεγχοι ασφάλειας θα πρέπει να πραγματοποιούνται, και μάλιστα σε τακτά χρονικά διαστήματα, για να διαπιστώνεται αν η πολιτική ασφαλείας ικανοποιεί τους σκοπούς της. Εάν όχι, τότε τουλάχιστον τα προβλήματα που διαφαίνονται χρειάζεται να επιλύνονται άμεσα.

Παράδειγμα: Μια επανεξέταση της πολιτικής ασφαλείας έξι μήνες αφότου είχε γραφτεί θα αποκαλύψει τις όποιες ατέλειες υπάρχουν, έστω και ελάχιστες. Αν, για παράδειγμα, είχε υποτεθεί ότι μόνο ελάχιστοι άνθρωποι θα πρέπει να έχουν πρόσβαση σε μια προστατευμένη περιοχή και τελικά κάτι τέτοιο δεν ήταν αναγκαίο, τότε θα πρέπει να αλλάξει. Ίσως κάποια από τα υλικά που φυλάσσονται σε μια προστατευμένη περιοχή δεν είναι τελικά τόσο «ευαίσθητα» και μπορούν να μετακινηθούν σε άλλη τοποθεσία, ή και αντίστροφα.

FIREWALLS ΤΑ ΑΝΤΙΠΥΡΙΚΑ ΤΕΙΧΗ

Πολλοί οργανισμοί έχουν συνδέσει τα εσωτερικά τους δίκτυα με το Internet, πιστοί στο πνεύμα του e-επιχειρείν. Έτσι όμως τα εσωτερικά τους συστήματα γίνονται ευπρόσβλητα σε κακόβουλη χρήση και σκόπιμη επίθεση από εξωτερικούς χρήστες. Απαραίτητη φραγή για την εισερχόμενη επιβουλή συνιστά το firewall, μια διάταξη εξιδικευμένων μηχανισμών ασφαλείας που ελέγχει την πρόσβαση και τη μετακίνηση πληροφορίας μεταξύ ενός αξιόπιστου και ενός μη αξιόπιστου δικτύου.Δεν είναι απλώς ένα συστατικό λογισμικού ή υλικού αλλά μια ενιαία στρατηγική προφύλαξης πόρων.

Το firewall υλοποιεί και ενδυναμώνει μια πολιτική ασφαλείας. Χωρίς την ανάλογη πολιτική καθίσταται άσκοπο.Αφορά στο σύνολο του υλικού, του λογισμικού και των διαδικασιών που χρησιμοποιούνται για την υλοποίηση της πολιτικής ασφαλείας μέσω

της διαχείρισης της εισερχόμενης και εξερχόμενης κίνησης από το εσωτερικό δίκτυο.Αποτελεί την πρώτη γραμμή άμυνας, αλλά οπωσδήποτε ποτέ τη μόνη, έναντι οποιασδήποτε παράνομης κίνησης.
Η κύρια λειτουργία του είναι ο κεντρικός έλεγχος των σημείων πρόσβασης εσωτερικό μας δίκτυο. Το κρίσιμο θέμα είναι εάν μπορούν βέβαια να προσδιοριστούν όλα τα σημεία εισόδου καιι να προστατευθούν ανάλογα.Ακόμη και εάν έχει ληθφεί μέριμνα για τα παραπάνω, εφόσον εξωτερικοί χρήστες αποκτήσουν πρόσβαση στο εσωτερικό δίκτυο, χωρίς να περάσουν μέσω του firewall, η αποτελεσματικότητα του εκμηδενίζεται.Αυτό θα μπορούσε να συμβεί, για παράδειγμα, εάν ο υπάλληλος ενός οργανισμού επέλεγε να συνδεθεί με το internet μέσω ενός modem που βρίσκεται στο γραφείο του. Σε μια τέτοια περίπτωση δημιουργεί μια ανασφαλή σύνδεση, παρακάμποντας το firewall και εκθέτοντας το εσωτερικό δίκτυο στους επίδοξους εισβολείς.
Όπως και με κάθε μέτρο ασφαλείας, υπάρχουν συμβιβασμοί που πρέπει να γίνουν μεταξύ επιπέδων ασφαλείας και άνεσης. Το firewall θα πρέπει να είναι διαφανές πρός τους χρήστες, ενώ αντίθετα θα είναι ένα ορατό εμπόδιο για τους εξωτερικούς χρήστες.

ΠΟΙΑ ΤΑ ΟΦΕΛΗ ΚΑΙ ΟΙ ΠΕΡΙΟΡΙΣΜΟΙ ΤΟΥΣ

Τα firewall παρέχουν ορισμένους τύπους προστασίας:

- Μπορούν να μπλοκάρουν μη επιθυμητή κίνηση.
- Μπορούν να κατευθύνουν εσωτερική κίνηση σε πιο αξιόπιστα εσωτερικά συστήματα
- Μπορούν να αποκρύψουν ευαίσθητα ή ευπρόσβλητα συστήματα, τα οποία δεν είναι εύκολο να αποκοπούν και να προστατευτούν από το διαδίκτυο.
- Μπορούν να παρακολουθούν και να καταγράφουν την κίνηση από και προς το εσωτερικό δίκτυο.
- Μπορούν να αποκρύψουν ονόματα συστημάτων, τοπολογίες δικτύων, τύπους συσκευών δικτύων και ταυτότητες εσωτερικών χρηστών.
- Μπορούν να προσφέρουν καλύτερο και πιο αξιόπιστο έλεγχο ταυτότητας από ότι άλλες εφσρμογές.
- Δεν παρέχει επαρκή προστασία όσον αφορά τους ιούς.

Το firewall είναι μια προσέγγιση στην ασφάλεια του εσωτερικού δικτύου. Συνεισφέρει στην υλοποίηση μιας πολιτικής ασφάλειας που ορίζει υπηρεσίες και επιτρεπόμενη πρόσβαση. Γενικά υλοποιούνται δύο κύριες σχεδιαστικές πολιτικές: «Επιτρέπεται κάθε υπηρεσία, εκτός εάν έχει απαγορευτεί ρητά» ή «απαγορεύεται κάθε υπηρεσία εκτός εάν έχει επιτραπεί ρητά».
Η πρώτη πολιτική διευκολύνει περισσότερο τους επίδοξους εισβολείς. Ο οργανισμός μπορεί να τοποθετήσει τον κεντρικό υπολογιστή που θα τρέχει έναν web server έξω απο το firewall, ενώ, όταν ο web server θα πρέπει να επικοινώνησει με βάσεις δεδομένων εντός του εσωτερικού δικτύου, η σύνδεση θα προστατεύεται απο ένα firewall, υλοποιώντας έτσι μια αρχιτεκτονική ελεγχόμενων υποδικτύων (screened subnets).
Τα firewall που βασίζονται σε δρομολογητές δεν προσφέρουν έλεγχο ταυτότητας του χρήστη, ενώ αυτά πού βασίζονται σε κεντρικό υπολογιστή υποστηρίζουν τα συνήθη συνθηματικά μιας χρήσης τα οποία αλλάζουν σε κάθε σύνδεση, και ψηφιακά πιστοποιητικά. Η πολιτική θα πρέπει να ορίζει σαφώς εάν επιτρέπεται να κάνει και δρομολόγηση πακέτων ή απλώς θα τα προωθεί. Οι δρομολογητές που φιλτράρουν τα

πακέτα (ενεργώντας ως firewalls) κάνουν δρομολόγηση των πακέτων, γιατί υπάρχει ο κίνδυνος να παρακαμφούν οι έλεγχοι ασφάλειας. Επίσης, η δρομολόγηση πηγής (source routing) δεν πρέπει να επιτρέπεται και τα πακέτα να απορρίπονται από το δρομολογητή.
Εάν λειτουργεί και ως DNS server, τότε οι εξωτερικοί υπολογιστές δεν γνωρίζουν τίποτα για το εσωτερικό δίκτυο. Μπορεί να χρησιμοποιηθεί για την προστασία υποτμημάτων ενός εσωτερικού δικτύου αλλά και για τη σύνδεση με ένα άλλο firewall, δημιουργώντας ένα ιδεατό δίκτυο (VPN). Τα περισσότερα προιόντα πλέον υποστηρίζουν και αυτήν τη δυνατότητα.
Προκειμένου ο οργανισμός να υλοποιήσει ένα σύστημα firewalls, συνιστάται η ασφαλής οδός: άρνηση κάθε υπηρεσίας εκτός αυτών που σαφώς έχουν οριστεί. Ο σχεδιαστής θα πρέπει να προσδιορίσει τα εξής:

- Διαδικτυακές υπηρεσίες που χρειάζεται ο οργανισμός (TELNET, HTPP, SMTP, E-MAIL κλπ).
- Τρόπους χρήσης των υπηρεσιών (τοπικά, από το σπίτι, απο οποιοδήποτε σημείο του internet κλπ).
- Υποστήριξη πρόσθετων αναγκών όπως κρυπτογράφηση και dial-in.
- Κίνδυνοι που μπορούν να προέλθουν από την παροχή των συγκεκριμένων υπηρεσιών και επιπέδων πρόσβασης.
- Κόστος παροχής προστασίας σε επίπεδο ελέγχου και επίδρασης στους πόρους του δικτύου.
- Προτεραιότητα της ασφάλειας έναντι της χρήσης των πόρων και υπηρεσιών του δικτύου.

ΕΙΔΗ FIREWALLS

Το φιλτράρισμα πακέτων (packet filtering) είναι ένας μηχανισμός firewall, ο οποίος ελέγχει τις επικεφαλίδες πακέτων δεδομένων και, με βάση συγκεκριμένους κανόνες, αποφασίζει αν τα πακέτα αυτά θα συνεχίσουν την πορεία τους ή όχι. Ο μηχανισμός εκτελείται σε μία συσκευή η οποία είναι συνδεδεμένη με δύο ή περισσότερα δίκτυα. Συνδυάζεται δε με το μηχανισμό δρομολόγησης, ο οποίος επιλέγει ανάμεσα στις εναλλακτικές γραμμές προώθησης του κάθε πακέτου. Ο μηχανισμός φιλτραρίσματος βασίζεται στις διευθύνσεις και ασχολείται με μεμονωμένα πακέτα και οι αποφάσεις για δρομολόγηση ή όχι κάθε πακέτου βασίζονται αποκλειστικά και μόνο στα πεδία διευθύνσεων του πακέτου. Αναγκαστικά λοιπόν ο μηχανισμός εμπιστεύεται την αυθεντικότητα της διεύθυνσης από την οποία το πακέτο «ισχυρίζεται» ότι προέρχεται, γεγονός που ελλοχεύει σημαντικούς κινδύνους.
Στην προσπάθειά μας να καθορίσουμε την πολιτική ασφαλείας, συναντάμε την ανάγκη για παροχή συγκεκριμένων υπηρεσιών στους εσωτερικούς αλλά και εξωτερικούς χρήστες. Πολλές από αυτές τις υπηρεσίες, σε περίπτωση ελεύθερης παροχής τους αποτελούν εύκολο και ελκυστικό στόχο επίδοξων εισβολέων. Παρουσίαζεται λοιπόν η ανάγκη για την υποβολή των υπηρεσιών σε αυτόματο έλεγχο, έτσι ώστε τυχόν «παράνομες» και επικίνδυνες εντολές να ανιχνεύονται και να αποτρέπεται η εκτέλεσή τους. Αυτή ακριβώς η ανάγκη οδήγησε στην ιδέα των proxy server ή application gateway. Πρόκειται για ειδικές μονάδες λογισμικού, οι οποίες παρεμβαίνουν στην επικοινωνία μεταξύ του εσωτερικού και του εξωτερικού δικτύου στο πλαίσιο της παροχής κάποιας συγκεκριμένης υπηρεσίας. Με αυτό τον τρόπο παρέχεται και πολύ καλός έλεγχος ταυτότητας των χρηστών.
Μια νεότερη τεχνική που εφαρμόζεται είναι το packet inspection (επίβλεψη πακέτων) ή dynamic packet filtering (δυναμικό φιλτράρισμα πακέτων), όπου το φιλτράρισμα

των πακέτων διεξάγεται με πιο έξυπνους κανόνες, εξετάζοντας λεπτομερώς και τα δεδομένα των πακέτων.

ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ΔΙΑΡΘΡΩΣΗΣ

Τα firewall μπορούν να διαρθρωθούν ποικιλοτρόπως, σχηματίζοντας διαφορετικές αρχιτεκτονικές και παρέχοντας διαφορετικά επίπεδα ασφάλειας, με διαφορετικό κόστος εγκατάστασης και λειτουργίας. Ο οργανισμός θα πρέπει να επιλέξει την αρχιτεκτονική ανάλογα με τους κινδύνους που θέλιε να αντιμετωπίσει.
Μια αρχιτεκτονική multi-homed είναι ένας υπολογιστής (το firewall στην περίπτωσή μας) με περισσότερες από μία διεπαφές δικτύου, όπου κάθε διεπαφή αντιστοιχεί λογικά και φυσικά σε διαφορετικά τμήματα ενός δικτύου. Η αρχιτεκτονική dual-homed είναι ένας κεντρικός υπολογιστής με δύο διεπαφές: μία προς το εσωτερικό δίκτυο και μία προς το Διαδίκτυο, που δεν επικοινωνούν μεταξύ τους παρά μόνο μέσω αυτού του υπολογιστή.
Στην αρχιτεκτονική screened-host προσφέρονται υπηρεσίες μέσω ενός κεντρικού υπολογιστή, ο οποίος συνδέεται μόνο με το εσωτερικό δίκτυο. Χρησιμοποιείται ένας ξεχωριστός δρομολογητής και η ασφάλεια πρώτου επιπέδου παρέχεται με φιλτράρισμα πακέτων. Το φιλτράρισμα πακέτων στον εξωτερικό δρομολογητή (screening router) είναι ρυθμισμένο έτσι, ώστε να επιτρέπονται συνδέσεις αφενός από το εξωτερικό δίκτυο μόνο προς τον κεντρικό υπολογιστή-ο οποίος πρέπει να έχει και υψηλό επίπεδο ασφάλειας-αφετέρου συνδέσεις από τον κεντρικό υπολογιστή με το Internet, οι οποίες και καθορίζονται από την πολιτική ασφαλείας. Μπορούμε να ρυθμίσουμε το φιλτράρισμα πακέτων έτσι, ώστε να επιτρέπεται σε ορισμένους εσωτερικούς υπολογιστές να συνδέονται απευθείας με το Internet για ορισμένες υπηρεσίες, ή να τους εξαναγκάζει να χρησιμοποιούν τις υπηρεσίες proxy που παρέχει ο κεντρικός υπολογιστής. Επιπλέον, είναι ευκολότερο να προστατέψουμε ένα δρομολογητή που παρέχει περιορισμένες υπηρεσίες, παρά τον κεντρικό υπολογιστή. Η αρχιτεκτονική screened host παρέχει περισσότερη ασφάλεια και ευχρηστία.
Συγκρινόμενη με άλλες αρχιτεκτονικές, όπως με τη screened-subnet, παρουσιάζει ορισμένα μειονεκτήματα, διότι εάν κάποιος «καταλάβει» το δρομολογητή, τότε όλο το εσωτερικό δίκτυο είναι εκτεθειμένο. Αν μάλιστα «καταλάβει» και τον κεντρικό υπολογιστή, τότε δεν υπάρχει τίποτα να τον σταματήσει, καθώς δεν υπάρχουν περαιτέρω επίπεδα ασφάλειας.
Η αρχιτεκτονική screened-subnet προσθέτει ένα επιπλέον επίπεδο ασφάλειας στη screened-host, δημιουργώντας ένα περιμετρικό δίκτυο που απομονώνει το εσωτερικό δίκτυο. Όταν απομονώσουμε τον κεντρικό υπολογιστή σε ένα περιμεντρικό δίκτυο, ακόμη και αν κάποιος πετύχει πρόσβαση σε αυτόν, δεν θα έχει ολική πρόσβαση.
Υπάρχουν δύο δρομολογητές στο περιμετρικό δίκτυο: ένας συνδεδεμένος με το εσωτερικό δίκτυο και ένας με το Internet. Μπορούμε να δημιουργήσουμε πολλά επίπεδα ασφάλειας, όσα και τα περιμετρικά δίκτυα, όπου οι περισσότερο ευπαθείς και λιγότερο ασφαλείς υπηρεσίες τοποθετούνται στα εξωτερικά επίπεδα.
Έτσι, αν «σπάσει» κάποιο επίπεδο, δεν θα μένει το υπόλοιπο δίκτυο απροστάτευτο. Αυτό προϋποθέτει διαφορετικό φιλτράρισμα σε κάθε επίπεδο. Η αρχιτεκτονική αυτή είναι ευρύτερα γνωστή ως «αποστρατικοποιημένη» ζώνη (demilitarized zone) και υποστηρίζεται από πολλά προϊόντα της αγοράς.
Συνήθως σε αυτό το ενδιάμεσο δίκτυο τοποθετούμε server δημόσια προσβάσιμους, ώστε να απομονώσουμε τον πιθανό εισβολέα έξω από το εσωτερικό μας δίκτυο. Με αυτό τον τρόπο παρεμβάλλονται τρεις συσκευές ασφάλειας στο δρόμο προς το εσωτερικό δίκτυο: ο εξωτερικός δρομολογητής που προστατεύει το δίκτυο από το

Internet, ο εσωτερικός δρομολογητής που προστατεύει το εσωτερικό δίκτυο από τον κεντρικό υπολογιστή και ο κεντρικός υπολογιστής (bastion host) που κατευθύνει όλη την κίνηση του εσωτερικού δικτύου.

ΠΩΣ ΤΑ ΕΓΚΑΘΙΣΤΟΥΜΕ

Η υλοποίηση ενός firewall περιλαμβάνει τις εξής φάσεις, που εκτελούνται το ένα μετά το άλλο:

1. Σχεδιασμός πολιτικής: ο σχεδιασμός ενός firewall προϋποθέτει την κατανόηση και τον προσδιορισμό των ορίων των διακριτών περιοχών ασφαλείας το δικτύου, όπου κάθε περιοχή ασφάλειας του δικτύου λειτουργεί βάσει μιας συγκεκριμένης πολιτικής ασφαλείας. Στα σημεία επικάλυψης των περιοχών αυτών απαιτείται ένας μηχανισμός επίλυσης της σύγκρουσης των διαφορετικών πολιτικών και αυτό ακριβώς κάνει το firewall. Αφού αποφανθούμε για τη βασική αρχιτεκτονική (αριθμός υπολογιστών, μέθοδοι συνδέσεων, λειτουργίες που εκτελούν), επιλέγουμε τις λειτουργίες που θα υλοποιηθούν (packet filtering, application gateway, stateful inspection) και στη συνέχεια επιλέγουμε το αρχιτεκτονικό σχέδιο του firewall (multi-homed, screened-host, screened-subnet).
2. Απόκτηση υλικού και λογισμικού: σε αυτήν τη φάση εξασφαλίζεται η ύπαρξη των απαιτούμενων συστατικών λογισμικού και υλικού και εσωτερικών πόρων για την εγκατάσταση, το δοκιμαστικό έλεγχο, τη λειτουργία, την επίβλεψη και τον έλεγχο του firewall. Ενδείκνυται μια πρώτη δοκιμαστική εγκατάσταση όλων των συστατικών, για να διαπιστωθούν έγκαιρα τυχόν ελλείψεις ή ανάγκη προσφυγής σε εξωτερικό σύμβουλο.
3. Απόκτηση τεκμηρίωσης, εκπαίδευσης κα υποστήριξης: ανάλογα με τον επιλεγμένο αρχιτεκτονικό σχεδιασμό πιθανότατα απαιτούν επιπρόσθετη εκπαίδευση και υποστήριξη από τον πωλητή. Εάν ο οργανισμός δεν έχει εμπειρία στις τεχνολογίες που πρόκειται να υλοποιήσει, υπάρχει σοβαρό ενδεχόμενο να δριαπράξει λάθη που θα του κοστίσουν, όπως καθυστέρηση στην εγκατάσταση, στη ρύθμιση και στη λειτουργία συστήματος firewall. Τα πιο σοβαρά λάθη προέρχονται από λάθος ρυθμίσεις ασφάλειας αλλά ακόμη και η συντήρηση του λογισμικού και του υλικού μπορεί να είναι τόσο πολύπλοκη, ώστε να χρειάζονται εκπαίδευση και συνεχή υποστήριξη. Σε αυτήν την φάση πρέπει να μελετηθεί και η μορφή της υποστήριξης.
4. Εγκατάσταση υλικού και λογισμικού: σε αυτήν την φάση εγκαθίσταται και ρυθμίζεται το λειτουργικό σύστημα που θα υποστηρίξει το λογισμικό του firewall και στην συνέχεια το λογισμικό του firewall στο επιλεγμένο υλικό αλλά στο περιβάλλον όπου γίνονται οι δοκιμαστικοί έλεγχοι. Το λειτουργικό σύστημα πρέπει να περιλαμβάνει μόνο τις υπηρεσίες που απαιτούνται για την λειτουργία του firewall, όλες οι άλλες πρέπει να είναι απενεργοποιημένες. Τυχόν ασυμβατότητες πρέπει να διορθωθούν εκείνη τη στιγμή με την προμήθεια των ανάλογων διορθωτικών προγραμμάτων.
5. Ρύθμιση της δρομολόγησης: η δρομολόγηση είναι η διαδικασία απόφασης για τη διάθεση ενός πακέτου που φτάνει στο δρομολογητή. Στόχοι του μηχανισμού δρομολόγησης είναι η απόδοση και η αξιοπιστία, όχι η υλοποίηση πολιτικής ασφαλείας.
6. Ρύθμιση των κανόνων φιλτραρίσματος πακέτων: ο μηχανισμός φιλτραρίσματος παρέχει τη βασική προστασία, ελέγχει το περιεχόμενο του πακέτου και βάσει ορισμένων κριτηρίων και κανόνων υλοποιεί την πολιτική ασφαλείας, αποφασίζοντας για τη διάθεση ή την απόρριψη του πακέτου. Εάν ο

αρχιτεκτονικός σχεδιασμός περιλαμβάνει και proxy servers, τότε πρέπει να εγκατασταθεί το λογισμικό για κάθε υποστηριζόμενη υπηρεσία, καθώς και οι μηχανισμοί ελέγχου ταυτοτήτων.

7. Ρύθμιση μηχανισμών καταγραφής και έγκυρης προειδοποίησης: το firewall πρέπει να καταγράφει όλες τις δραστηριότητές του και τα συμβάντα. Επιπλέον πρέπει να ορίσουμε εκείνα τα γεγονότα για τα οποία θα πρέπει να ειδοποιηθούμε άμεσα για να επέμβουμε. Η καταγεγραμμένη πληροφορία θα χρησιμοποιηθεί από ένα intrusion detection system για την ανίχνευση ακανόνιστης και μη προβλεπόμενης συμπεριφοράς.
8. Δοκιμαστικός έλεγχος του συστήματος: το σύστημα ελέγχεται στο περιβάλλον δοκιμών για τυχόν λάθη και ελλείψεις με τη χρήση συστημάτων intrusion detection, port scanners, εργαλείων ανίχνευσης αδυναμιών (vulnerability analysis), εργαλείων παραγωγής κίνησης στο δίκτυο (traffic generation tools) και εργαλείων παρακολούθησης δικτύων (network monitoring). Επιπλέον, εκτελούνται συγκεκριμένα πιθανά σενάρια, όπως προβλέπονται στο σχέδιο ελέγχου.
9. Εγκατάσταση: το firewall εγκαθίστανται σταδιακά, εάν πρόκειται να συνδέσει ασύνδετα και απροστάτευτα δίκτυα, ή παράλληλα με τη λειτουργία ενός υπάρχοντος συστήματος, εάν πρόκειται να το αντικαταστήσει, προσέχοντας πάντα να μην επηρεάσουμε το παραγωγικό περιβάλλον λειτουργίας.

ΠΩΣ ΕΠΙΛΕΓΟΥΜΕ

Κατά τη διαδικασία της αξιολόγησης και της επιλογής ενός firewall πρέπει να έχουμε ήδη αποφασίσει για:

- Τους κινδύνους που θέλουμε να αντιμετωπίσουμε (πληροφορίες και πόρους που θέλουμε να προστατέψουμε, απειλές από τις οποίες τα προστατεύουμε).
- Τις υπηρεσίες που θα παρέχουμε στο Internet από το δίκτυό μας.
- Τις υπηρεσίες του Internet που θέλουμε να χρησιμοποιήσουμε.
- Τους χρήστες αυτών των υπηρεσιών.
- Την απαιτούμενη διαθεσιμότητα και τις απαιτούμενες επιδόσεις του firewall.
- Το ποιος θα διαχειρίζεται το firewall και πώς.
- Την αναμενόμενη ανάπτυξη του συστήματός μας και του δικτύου μας, την οποία και θα πρέπει το firewall να υποστηρίξει στο μέλλον. Η αξιολόγηση και η επιλογή μιας συγκεκριμένης λύσης βασίζεται στα κριτήρια που έχουμε θέσει και στην εκπλήρωση αυτών από τις υπό μελέτη λύσεις. Έτσι λοιπόν πρέπει να απαντήσουμε σε ορισμένα ερωτήματα, τα οποία αντικατοπτρίζουν τις απαιτήσεις μας και την ικανοποίησή τους από το προϊόν.

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

- Υποστήριξη «αποστρατιωτικοποιημένης» ζώνης DMZ
- Υποστήριξη NAT (Network Address Translation)
- Υποστήριξη LDAP directory (Lightweight Directory Access Protocol) για υποστήριξη e-mail
- Είδος firewalling που παρέχει (απλό ή δυναμικό φιλτράρισμα πακέτων, application gateway).
- Υποστήριξη Virtual Private Networks (VPN), πρωτόκολλο κρυπτογράφησης IPSsec και ασφαλής σύνδεση από μακρινό υπολογιστή για διαχείριση

- Υποστήριξη υπηρεσιών (FTP, HTTP, HTTPS, SMTP, TELNET, FTP) και υπηρεσιών σε επίπεδο εφαρμογών (ActiveX, Java JavaScript).

ΑΣΦΑΛΕΙΑ, ΑΞΙΟΠΙΣΤΙΑ, ΕΠΙΔΟΣΕΙΣ

- Τεχνογνωσία του πωλητή, το ιστορικό του, υποστήριξη που παρέχει.
- Ασφάλεια κρυπτοσυστημάτων και αλγόριθμων-ορισμένοι πωλητές τα υλοποιούν λάθος και υπάρχει σοβαρός κίνδυνος.
- Επεκτασιμότητα-το προϊόν δέχεται plug-ins της ίδιας εταιρείας ή τρίτων, με ποιο τρόπο τα ενσωματώνει, τι προσθέτουν στη συνολική ασφάλεια του συστήματος.
- Παροχή αυτόματης ενημέρωσης του προϊόντος με νέες εκδόσεις και διορθώσεις.
- Αποδοτικότητα του προϊόντος στη διαχείριση της κίνησης του δικτύου, συνολικές συνδέσεις που υποστηρίζει, δυνατότητα προσδιορισμού προτεραιοτήτων για τα είδη κίνησης που πρέπει να διαχειρίζεται.

ΣΥΝΤΗΡΗΣΗ, ΔΙΑΧΕΙΡΙΣΗ

- Ευκολία και ταχύτητα εγκατάστασης του προϊόντος
- Γραφική διεπαφή διαχείρισης
- Δυνατότητα διαχείρισης από μακριά
- Καταγραφή συμβάντων και δραστηριοτήτων
- Μηχανισμοί ειδοποίησης

Σημαντική είναι επίσης η μελέτη του αρχιτεκτονικού σχεδιασμού του προϊόντος και της φιλοσοφίας που το διέπει. Ένας σωστός αρχιτεκτονικός σχεδιασμός, εξασφαλίζει στον οργανιμσό ότι το προϊόν έχει την ικανότητα να εκτλέσει τις προβλεπόμενες λειτουργίες με ασφάλεια, προστατεύοντας το δίκτυο και τους υπολογιστές αλλά και το ίδιο. Οι μηχανισμοί με τους οποίους ανταποκρίνεται σε αυτά πρέπει να μελετηθούν διεξοδικά από τον επίδοξο αγοραστή. Ενδιαφέρουν επίσης οι υποθέσεις που έχει να κάνει ο κατασκευαστής και τις οποίες πρέπει εμείς να αποδεχθούμε (προρρυθμίσεις, απαιτήσεις λογισμικού, υλικού ή άλλων προϊόντων, τοπολογία δικτύου). Οι υποθέσεις αυτές περιλαμβάνουν και τις προκαθορισμένες και προεπιλεγμένες λειτουργίες του προϊόντος, οι οποίες συνθέτουν την πολιτική που υλοποιεί, εάν εγκατασταθεί άμεσα.

Πρόσθετες υπηρεσίες που δύναται να παρέχει το firewall, όπως προστασία από ιούς, μας ενδιαφέρουν πάντοτε. Επειδή όμως ο συγκεκριμένος στόχος εξυπηρετείται καλύτερα από άλλα αντιβιοτικά προϊόντα, μας ενδιαφέρει πρωτίστως με ποια προϊόντα μπορεί και συνεργάζεται το firewall. Η συνεργασία του με άλλα προϊόντα δεν περιορίζεται στα αντιβιοτικά, αλλά περιλαμβάνει και τα intrusion detection system.

Η διασυνδεδιμότητά του με άλλα συστήματα firewall και πλατφόρμες υλικού και λογισμικού αποτελεί βασικό μας στόχο. Πιθανόν να απαιτεί οι υπολογιστές που προστατεύει να είναι συγκεκριμένης πλατφόρμας ή να χρειάζονται επιπλέον λογισμικό. Το προϊόν θα πρέπει να υποστηρίζει γνωστά πρότυπα, κυρίως αυτά που αφορούν στη χρήση κρυπτογραφίας.

Μια επιπλέον αξιολόγηση του προϊόντος από τρίτο οργανισμό είναι πάντα θεμιτή. Έτσι λοιπόν πέρα από τη δικής αξιολόγηση και τους δοκιμαστικούς ελέγχους που θα

διενεργήσουμε εμείς ή ο ίδιος ο πωλητής για λογαριασμό μας, καλό είναι το προϊόν να είναι πιστοποιημένο από κάποιον τρίτο οργανισμό.
Ένας οργανισμός θα πρέπει να επιλέξει ανάμεσα σε ένα καθαρό προϊόν λογισμικού που φιλοξενείται σε ένα συνηθισμένο υπολογιστή και σε μια αφοσιωμένη συσκευή υλικού, στην οποία είναι ενσωματωμένο το λογισμικό. Στην πρώτη περίπτωση το firewall είναι ένα προϊόν λογισμικού, ενώ στη δεύτερη είναι μια συσκευή υλικού με προεγκατεστημένο και προρρυθμισμένο λογισμικό, η οποία εκτελεί συγκεκριμένες λειτουργίες. Η πρώτη λύση παρέχει ευελιξία, σταθερότητα και δυνατότητα πλουσιότερων και καλύτερων ρυθμίσεων, αλλά μεγαλύτερο χρόνο και προσπάθει υλοποίησης, ενώ το επιλεγμένο προϊόν μπορεί να βασίζεται σε μια πλατφόρμα για την οποία υπάρχη αρκετή εμπειρία. (Windows, NT, Unix).
Η δεύτερη λύση απαιτεί ελάχιστο χρόνο για την υλοποίησή της, γι' αυτό και παρουσιάζεται πολλές φορές ως λύση άμεσης αντίδρασης ενός οργανισμού έπειτα από ένα περιστατικό. Έχει μικρότερο κόστος και παρουσιάζει υψηλή διαθεσιμότητα, καθώς σε περίπτωση αποτυχίας η ενεργοποίηση και η εύρυθμη λειτουργία ενός εφεδρικού firewall είναι σαφώς ευκολότερη υπόθεση από ό,τι στην πρώτη περίπτωση. Επίσης, διαχειρίζεται αποδοτικά την κίνηση του δικτύου-άλλωστε η λειτουργία αυτή είναι από τις σημαντικότερες του firewall, αν και παρελκόμενη.

IP SECURITY: BUILDING BLOCK FOR THE TRUSTED VIRTUAL NETWORK

Η ΑΝΑΓΚΗ ΓΙΑ ΕΝΑ ΝΕΟ ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ

Ένα μέρος της λύσης (για την εξασφάλιση ασφάλειας) υπάρχει ήδη, το firewall. Βρίσκεται συνήθως τοποθετημένο περιμετρικά της επιχείρησης και ελέγχει την πρόσβαση στις ηλεκτρονικές πηγές της επιχείρησης, *φιλτράροντας* τα πακέτα IP βάση μίας σειράς κανόνων, τους οποίους ορίζει ο χρήστης. Μέχρι τώρα, αυτός ο τύπος εξασφάλισης ασφάλειας πρόσφερε ικανοποιητικού βαθμού προστασία, καθώς η κύρια απειλή για την ασφάλεια προερχόταν από έξω(από παράγοντες έξω από την επιχείρηση).

Μία απλή αναλογία/ παράδειγμα μας βοηθά να καταλάβουμε γιατί πλέον αυτή η μέθοδος προστασίας είναι ελλιπής. Μία τράπεζα π.χ. δεν λαμβάνει μέτρα μόνο για την περιμετρική προστασία του κτιρίου της και κλειδώνει τις πόρτες της τη νύχτα, αλλά διαθέτει επιπλέον και *κρύπτη*. Η τράπεζα 'γνωρίζει' ότι ανεξάρτητα με το πόσο ασφαλές είναι το κτίριο, εξακολουθεί να υπάρχει η ανάγκη να προστατευτούν τα χρήματα από τους ανθρώπους που βρίσκονται μέσα στην τράπεζα καθώς και από κλέφτες, οι οποίοι μπορούν να μπουν μέσα στο κτίριο προσποιούμενοι τους πελάτες.

Η ίδια αρχή ισχύει και για το δίκτυο. Πολλαπλά στρώματα ασφάλειας/προστασίας απαιτούνται, το καθένα από τα οποία θα συμπληρώνει το

άλλο. Προκειμένου μια επιχείρηση να προσφέρει πλήρη ασφάλεια/προστασία μέσα και έξω από το δίκτυο πρέπει να διασφαλίσει τις πληροφορίες καθώς αυτές ταξιδεύουν στο LAN.

ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΗ ΔΗΜΙΟΥΡΓΙΑ ΕΝΟΣ ΑΣΦΑΛΟΥΣ ΕΙΚΟΝΙΚΟΥ ΔΙΚΤΥΟΥ

Απαιτείται μία νέα προσέγγιση για να καλύψουμε τις σημερινές ανάγκες προστασίας (Figure B). Τα προαπαιτούμενα στοιχεία περιλαμβάνουν:

*** ασφάλεια LANσε επίπεδο desktop και server.**

Η μεγαλύτερη ανταλλαγή πληροφοριών (μεγαλύτερη επικοινωνία) πραγματοποιείται ανάμεσα σε έναν server και τα desktop των πελατών, καθώς και μεταξύ των desktop μέσα σε (μία ομάδα εργασίας) workgroup. Εκεί βρίσκεται και ο μεγαλύτερος κίνδυνος για την εσωτερική ασφάλεια, η οποία μπορεί να εξασφαλιστεί με authentication, integrity encryption.

*** έλεγχος πρόσβασης στο rooter/firewall και το φορητό PC.**

Για παράδειγμα, ένας εργαζόμενος έξω από την περίμετρο/όρια του οργανισμού μπορεί να χρειαστεί να μπει μέσα στο δίκτυο προκειμένου να συμμετάσχει σε δραστηριότητες, ως μέλος μιας ομάδας εργασίας. Έτσι, σε συνδυασμό με την προστασία που παρέχει το firewall στην περίμετρο, πρέπει να χρησιμοποιηθεί ένα ασφαλές πέρασμα ανάμεσα στο αποκομμένο/απομακρυσμένο PC και το firewall, για να έχουμε ασφαλή επικοινωνία μέσω του ίντερνετ.

*** WAN/ίντερνετ ασφάλεια.**

Ένας οργανισμός μπορεί να διαθέτει ένα παράρτημα, με το οποίο πρέπει να επικοινωνούν καθημερινά πολλά άτομα από το κεντρικό κτίριο του οργανισμού και το αντίστροφο. Αυτή η επικοινωνία μπορεί να πραγματοποιείται μέσω ίντερνετ, VPN, με μία γραμμή αφιερωμένη αποκλειστικά για τη λειτουργία αυτή ή ακόμη και με τις τρεις. Όπως και να γίνεται όμως αυτή η επικοινωνία τα κανάλια της/ οι δίοδοι της θα πρέπει να προφυλάσσονται από παραβιάσεις, που μπορούν να προέλθουν μέσα ή και έξω από τον οργανισμό.

*** διαχείριση ασφάλειας σε όλο το δίκτυο.**

Σήμερα, οι οργανισμοί μπορούν να χρησιμοποιούν πολλά διαφορετικά μέτρα ασφάλειας/προστασίας. Συχνά προτείνονται λύσεις, οι οποίες είναι δύσκολο να συνδυαστούν μεταξύ τους. Στο μέλλον, όλες οι λύσεις/ τα μέτρα ασφαλείας σε μία επιχείρηση θα πρέπει να λειτουργούν σε συνεργασία μεταξύ τους και ιδανικό θα

ήταν, εάν αυτά είχαν εξελιχθεί τόσο, ώστε, να αποτελούν κοινά building blocks κι έτσι να συνεργάζονται μεταξύ τους (interoperable).

Προκειμένου να είναι επιτυχείς οι λύσεις αυτές θα πρέπει να είναι βασισμένες σε στάνταρντς εύρους επιχείρησης (industry-wide) και συμβατά με τα παγκόσμια δεδομένα. Πρέπει ακόμη να διαθέτουν «λογικές» τιμές, να διαθέτουν διακυμάνσεις(scalable) και να μπορούν να συνεργαστούν με τη εγκατεστημένη βάση της infrastructure του δικτύου (!). Τέλος, απαιτείται και common management interface για την επιχείρηση καθώς και κανόνες και πολιτικές χειρισμού προκειμένου να υπάρχει πλήρη ασφάλεια από άκρο εις άκρον.

Τι είναι η πολιτική(policy) διαχείρισης ασφάλειας; για παράδειγμα θα μπορούσε να υπάρχει μια *πολιτική* τύπου «πότε και πως να encrypt»,η οποία και να απαιτεί encryption 168-bit για την ανταλλαγή υλικού ιδιαίτερα ευαίσθητου και μόλις 56-bit για την ανταλλαγή μετρίως ευαίσθητου υλικού. Η ευαισθησία του *υλικού* καθορίζεται ανάλογα με το είδος της εφαρμογής, τη διεύθυνση του αποστολέα, ή τον αριθμό port, κριτήρια, τα οποία είναι εύκολο να 'διαβαστούν' από τις κάρτες interface του δικτύου ή άλλους μηχανισμούς.

Ένα ουσιώδες building block

Μία απάντηση για πολλές από αυτές τις προκλήσεις είναι η τεχνολογία IPSec (Internet Protocol Security). Ανοιχτή και βασισμένη σε στάνταρντσ, η IPSec υιοθετείται ευρύτερα και προβάλλεται ως η de facto βασική building block του ασφαλούς δικτύου.

Η IPSec τρέχει στο Layer 3 in the protocol stack, με αποτέλεσμα να είναι transparent (αλάνθαστη) στις εφαρμογές, σε αντίθεση με τεχνολογίες ασφάλειας/προστασίας, οι οποίες τρέχουν σε άλλα στρώματα. Αυτό σημαίνει ότι η IPSec είναι σχετικώς εύκολη και φθηνή στην εγκατάστασή της, καθώς οι εφαρμογές μπορούν να τη χρησιμοποιούν χωρίς να χρειάζεται να μεταβληθούν/ γίνουν μετατροπές και οι χρήστες δεν χρειάζεται να εκπαιδευτούν για να τη χειριστούν.

Τί είναι η IPSec;

Όπως ορίζεται από την IETF, η IPSec αποτελεί ένα στάνταρντ το οποίο παρέχει πιστοποίηση (authentication), ακεραιότητα(integrity) και encryption. Προσφέρει δύο τρόπους λειτουργίας- διόδου και μεταφοράς. Η IPSec έχει ήδη χρησιμοποιηθεί ευρέως για τα VPSs (Virtual Private Networks) δίνοντας τη δυνατότητα σε οργανισμούς να χρησιμοποιήσουν το ίντερνετ ως μία μορφή

ασφαλούς WAN. Συνήθως οι VPNs εφαρμόζουν τον τρόπο λειτουργίας ‘διόδου’ IPSec, αλλά μπορεί να εφαρμοστεί και ο τρόπος λειτουργίας ‘μεταφοράς’ προκειμένου να διασφαλίσει την κίνηση LAN.

Ένα από τα κύρια οφέλη της IPSec, σε εφαρμογή κίνησης, είναι ότι τα encrypted πακέτα μπορούν να δρομολογηθούν και να κατευθυνθούν σε δίκτυα, τα οποία υποστηρίζουν την κίνηση IP, χωρίς να απαιτείται αναβάθμιση στην εσωτερική δομή του δικτύου. Τα πακέτα μπορούν να ‘γυρνούν’ / μετακινούνται από το ιντρανετ, στο εξτρανετ και στο ίντερνετ με ευκολία και transparently, χωρίς διαλείμματα και χωρίς να το *καταλαβαίνει* ο χρήστης. Επιπρόσθετα οι λύσεις που χρησιμοποιούν το IPSec ως βάση για ένα πρωτόκολλο μπορούν να συνεργαστούν μεταξύ τους, ανοίγοντας νέες ελπίδες και δυνατότητες για τη ασφαλή διανομή δεδομένων.

Τα οφέλη της IPSec στον τελικό πελάτη περιλαμβάνουν:

* Λιγότερο δαπανηρή σύνδεση branch office

* ταχύτερη και αρτιότερη σύνδεση πελάτη-προμηθευτή

* περισσότερο ασφαλή LAN, συμπεριλαμβανομένης καλύτερης προστασίας έναντι ‘εσωτερικών’ απειλών

Πώς εφαρμόζει στο εικονικό δίκτυο

Ως βασικό building block στο στρώμα του δικτύου, η IPSec εφαρμόζει καλά στο αυριανό μοντέλο του ασφαλούς εικονικού δικτύου, παίζοντας ένας ουσιώδη ρόλο στην ασφάλεια LAN, στον έλεγχο πρόσβασης και στην ασφάλεια WAN. Οι χρήσεις της μπορεί να περιλαμβάνουν τους παρακάτω τύπους επικοινωνιών και σχηματισμών δικτύου

*** Peer-to-Peer**

***Client-Server**

***Protected Workgroup**

***Protected Enterprise**

*** VPNs and Remote Access**

Η ασφάλεια *από άκρου εις άκρου* είναι βασική για την προστασία των επικοινωνιών. Αυτό είναι ήδη εμφανές στην περίπτωση του ηλεκτρονικού ταχυδρομείου, όπου θέλουμε να διασφαλίσουμε τα δεδομένα καθ’όλη την πορεία τους από το desktop του αποστολέα ώς το desktop το παραλήπτη. Αρχεία/ φάκελοι, οι οποίοι αποστέλλονται μαζί με το ηλεκτρονικό μήνυμα μπορούν εύκολα να «κλαπούν» και συχνά περιέχουν ευαίσθητες πληροφορίες.

Για πλήρη προστασία, η Network Interface Card (NIC) είναι η καλύτερη τοποθεσία για την εφαρμογή της τεχνολογίας IPSec. Εκεί, τα δεδομένα μπορούν να αξιολογηθούν, πριν τη μεταφορά τους, και το hardware offload μπορεί να χρησιμοποιηθεί με τον καλύτερο τρόπο για να επιταχύνει την encryption.

Οι χρήστες θα έχουν προηγμένη επικοινωνία client /server- όπως ταχύτερο ηλεκτρονικό ταχυδρομείο ή ταχύτερη πρόσβαση στο διαδίκτυο- εάν τα πακέτα έχουν encrypted και decrypted σε ένα NIC με IPSec. Ξεφορτώνοντας(offloading) τη διαδικασία encryption στο NIC επιταχύνει τους μαθηματικούς κύκλους που απαιτούνται από την encryption, ενώ παράλληλα ελευθερώνει τον κεντρικό επεξεργαστή (host processor) (figure C).

Πώς δουλεύει

Όπως ορίζεται από την IETF, η IPSec περιλαμβάνει δύο επεκτάσεις internet protocol που έχουν σχεδιαστεί για να υποστηρίζουν την κατασκευή ασφαλών πακέτων IP.

Τα στοιχεία αυτά είναι :

* **Authentication Header (AH)** , το οποίο παρέχει πιστοποίηση πηγής και ακεραιότητα δεδομένων, προκειμένου να εξασφαλίσει ότι τα δεδομένα δεν θα είναι διαθέσιμα σε σταθμό, που δεν θα διαθέτει άδεια αλλά και δεν θα μετατραπούν καθοδόν.

* **Encapsulated Security Payload(ESP)** παρέχει *εχεμύθεια* καθώς και διασφάλιση πιστοποίησης και ακεραιότητας, έτσι ώστε τα στοιχεία/δεδομένα να μην μπορούν να αναγνωστούν ή αντιγραφούν από τρίτους.

Ποιοι είναι οι ειδικοί αυτοί μηχανισμοί που χρειάζονται για την εφαρμογή αυτών των στοιχείων; Η IPSec λειτουργεί σε IP πακέτα όπως περιγράφεται παρακάτω:

Transport Mode Uses-

Η transport mode χρησιμοποιείται συνήθως σε επικοινωνίες peer-to-peer, όπου προσφέρει ασφάλεια intranet or LAN. Το IP header παραμένει αναλλοίωτο, έτσι ώστε να μπορεί να 'διαβαστεί' και να χρησιμοποιηθεί από οποιοδήποτε 'μηχάνημα' standards -based infrastructure. Το πακέτο δεδομένο είναι encrypted και πιστοποιημένο (authenticated) κι έτσι προστατεύεται όλο το περιεχόμενο του IP πακέτου.

Tunnel mode access

Χρησιμοποιείται για μακρινή πρόσβαση και ασφάλεια από site σε site, συμπεριλαμβανομένων των VPNs. Τοποθετώντας το πακέτο σε ένα καινούργιο wrapper με μία νέα διεύθυνση IP, αποκρύπτεται η τοπολογία/τοποθεσία των προστατευόμενων sites.

Αυξημένη ασφάλεια και μειωμένο κόστος

Όταν εφαρμόζεται η encryption IPSec, η κίνηση του LAN δεν μπορεί να διαβαστεί από κάποιον 'υποκλοπέα-εισβολέα' και τα δεδομένα εμφανίζονται ως ακατανόητα σύμβολα. Το IPSec επίσης 'κλειδώνει' τα δεδομένα,με τρόπο αντίστοιχο ενός φακέλου, ο οποίος δεν μπορεί να ανοιχθεί (tamper proof). Όσο το 'κάλυμα- η κλειδαριά' του αποστολέα παραμένει ανέπαφη, εξασφαλίζεται η ακεραιότητα-προστασία των δεδομένων.

Το IPSec χρησιμοποιείται όλο και περισσότερο για τη δημιουργία trusted virtual workgroups, τα οποία συμβάλουν στην προστασία ευαίσθητων δεδομένων. Για παράδειγμα, το Τμήμα Έρευνας και Ανάπτυξης μπορεί να προστατευτεί από άλλα τμήματα, τα οποία δεν χρειάζεται να 'γνωρίζουν' τις εμπιστευτικές πληροφορίες/δεδομένα του τμήματος αυτού. Ή ακόμη, τα αρχεία υπαλλήλων που βρίσκονται στο τμήμα Ανθρώπινου Δυναμικού μιας επιχείρησης μπορούν με τον τρόπο αυτό να προστατευτούν από μη εξουσιοδοτημένη πρόσβαση.

Για τις ηλεκτρονικές επιχειρήσεις η IPSec προσφέρει τη δυνατότητα σχηματισμού προστατευμένων εικονικών συνδέσεων με τους πελάτες/καταναλωτές, προμηθευτές και συνεργάτες μέσω ίντερνετ. Έτσι επιτυγχάνεται ταχύτερη και ορθότερη ταξινόμηση παραγγελειών, μειώνεται ο όγκος προς αποθήκευση αλλά και το κόστος των πωλήσεων, ενώ θα πρέπει να σημειωθεί ότι το κόστος των πωλήσεων μειώνεται ακόμη περισσότερο με την εμπόδιση της κλοπής πληροφοριών.

IPSec-related work by Intel

Η εταιρεία Intel έχει αναπτύξει την πρώτη της 'οικογένεια' προσαρμογών προστασίας- την Intel PRO/100 S Desktop, Server and Mobile Adapters. Αυτοί έχουν βελτιωθεί και μπορούν να ξεφορτώνουν IPSec από τα Windows 2000, με δυνατότητα λειτουργίας στα Windows NT 4.0 και στα Windows 98 με τη χρήση Intel Packet Protect software.

Με την λύση της Intel, η encryption/decryption *ξεφορτώνεται* στον adapter's 82550 Controller, which has an integrated encryption co-processor.

Παρόλο που η IPSec αποτελεί μηχανισμό προστασίας επικοινωνιών το «πότε και πώς» εφαρμόζεται είναι κάτι, το οποίο πρέπει να καθορίσει ο χρήστης. Προκειμένου, δηλαδή, να είναι αποτελεσματική η IPSec πρέπει να διαχειρίζεται/χειρίζεται σωστά. Για τον λόγο αυτό η Intel υποστηρίζει κίνητρα/προσπάθειες προκειμένου ...

Συμπέρασμα

Οι προσδοκίες για τη δημιουργία ενός νέου μοντέλου ηλεκτρονικής επιχείρησης, της Trusted Virtual Network, συνεπάγεται εντυπωσιακές νέες δυνατότητες για έναν πολύ μεγάλο αριθμό επιχειρήσεων.

Η IPSec πιθανώς να αποτελέσει, από πολλές απόψεις, τη νέα «βάση»/το νέο πλαίσιο για την ασφάλεια στο LAN. IT-επαγγελματίες έχουν ήδη ξεκινήσει να εφαρμόζουν την IPSec από το 1999 και, καθώς η ηλεκτρονική-επιχείρηση(E-business) συνεχίζει να εξαπλώνεται, αναμένεται η IPSec να διαδοθεί ακόμη περισσότερο αποτελώντας βασικό κομμάτι του δικτύου.

Προκειμένου να είναι πλήρως αποτελεσματική η IPSec πρέπει είναι integrated στη συγκεκριμένη *πολιτική* διαχείρισης ασφάλειας και διαχειρισης δικτύου της επιχείρησης. Αυτό δεν μπορεί να επιτευχθεί μόνο του, αντιθετα, πρέπει να αποτελέσει μέρος μίας ευρύτερης «στρατηγικής' διαχείρισης. Καθένας που ασχολείται με την τεχνολογία θα πρέπει να ανιχνεύσει πως η IPSec μπορεί να επιρρεάσει την επιχείρησή του/δουλειά του τόσο στο τακτικό,όσο και στο στρατηγικό επίπεδο.

Για περισσότερες πληροφορίες...

CISCO SYSTEMS

CiscoAssure: End-to-End Security Policy Management

Ο σχεδιασμός, η εφαρμογή και η ενίσχυση συστημάτων/πολιτικών ασφαλείας , όπως έχει αποδειχθεί ιστορικά, απαιτούν μεγάλο χρονικό διάστημα προκειμένου να ολοκληρωθούν και για τον λόγο αυτό είναι δαπανηρά. Είναι επίσης αλήθεια ότι η εφαρμογή μίας πολιτικής ασφαλείας *end-to-end* στα δίκτυα μίας επιχείρησης προϋποθέτει τις ανάλογες γνώσεις από το προσωπικό της επιχείρησης αυτής, οι οποίες κατά κανόνα δεν υπάρχουν.

Τα συστήματα Cisco έρχονται να καλύψουν τις επιχειρηματικές και τεχνικές ανάγκες των επιχειρήσεων για απλουστευμένο, αυτοματοποιημένο έλεγχο δικτύου, με

την CiscoAssure. Η CiscoAssure αποτελεί μία «οικογένεια» στοιχείων πολιτικης, που βασίζεται σε τέσσερα βασικά building blocks (Figure1). Αυτά είναι:

* Intelligent network devices - εφυή μηχανήματα δικτύου

Στα στοιχεία/μηχανήματα του δικτύου πρέπει να διαθέτουν «επίγνωση εφαρμογής» (application -aware) , δηλαδή, να μπορούν να λαμβάνουν και να «μεταφράζουν» τις εντολές πολιτικής και να διενεργούν ελέγχους ασφαλείας για κάθε χρήστη ή για κάθε εφαρμογή.

* Quality of service (QoS) and security policy services- ποιότητα υπηρεσιών και υπηρεσίες ασφαλείας

Server-based συστήματα ελέγχου, τα οποία παρέχουν interface ανάμεσα στον διευθυντή/διαχειριστή και στο δίκτυο. Οι δυνατότητες «μετάφρασης» καθιστούν εφικτό τον αυτόματο σχηματισμό όλων των μηχανισμό του δικτύου μέσω μίας κεντρικής κονσόλας. Security is communicated to network elements using Comon Open Policy Service (COPS) protocol

*Registration and directory services - υπηρεσίες εγγραφής/καταγραφής και καταλόγου

Παρέχουν ισχυρή «σύνδεση» ανάμεσα στις υπηρεσίες και στις διευθύνσεις του δικτύου, user profiles, application profiles και άλλων πληροφοριών που είναι βασικές για την ομαλή εφαρμογή πολιτικής. Αυτές οι υπηρεσίες βασίζονται σε ένα Domain Name Server/Dynamic Host Configuration Protocol (DNS/DHCP) server system and Lightweight Directory Access Protocol (LDAP)v3-based directories.

*Centralized policy administration - κεντρική διαχείριση

Ο «διευθυντής/διαχειριστής» αλληλοεπιδρά με το σύστημα CiscoAssure μέσω ενός graphical user interface (GUI) , το οποίο απλοποιεί τον ορισμό *πολιτικής* και παρέχει τη δυνατότητα σχηματισμού των κανόνων της επιχείρησης κεντρικά and map these rules onto the intelligent network. Το GUI δίνει στους διαχειριστές πολλαπλά επίπεδα ελέγχου προκειμένου να δεχθούν/ή να απορρίψουν την κίνηση στο δίκτυο και να επιβάλουν «πολιτική» βασισμένη στην IP διεύθυνση, την εφαρμογή, τον χρήστη, την ώρα της ημέρας ή την τοποθεσία. Αυτό το GUI δίνει τη δυνατότητα στους «διαχειριστές» να δημιουργήσουν ή να ενισχύσουν «πολιτικές» , χρησιμοποιώντας τα πολλαπλά στοιχεία ασφάλειας της Cisco, όπως routers, firewalls, and intrusion-detection devices.

Επίκεντρο αυτής της σελίδας είναι η διαχείριση πολιτικών ασφαλείας ...

οι προσφερόμενες λύσεις ασφαλείας μπορούν να κατηγοριοποιηθούν στις παρακάτω τεχνολογικές «οικογένειες»:

***Identity (Ταυτότητα)**

Σε ποιόν επιτρέπεται να κάνει τί και από πού; Η Cisco προσφέρει την CiscoSecure authentication (πιστοποίηση), authorization(εξουσιοδότηση) and accountin (AAA) server, και λύσεις ψηφιακής πιστοποίησης με συνεργάτες τις Veisisign, Entrust, Microsoft Corporation, και Netscape Communications.

*** Ingegrity (Ακεραιότητα)**

Προστατεύει πληροφορίες και πηγές από μη εξουσιοδοτημένες προσβάσεις. Τα Cisco firewalls περιλαμβάνουν τον PIX Firewall και το Cisco IOS Firewall. Άλλα στοιχεία «ακεραιότητας» της Cisco περιλαμβάνουν καταλόγους ελέγχου προσβάσεων (ACLs) και IPSec-based encryption.

*** Active audit (ενεργός έλεγχος)**

Παρακολουθεί την κίνηση του δικτύου, εντοπίζει τους κινδύνους ασφαλείας, ενισχύει την «πολιτική» ασφαλείας και εμποδίζει την μη εξουσιοδοτημένη δραστηριότητα. Τα προϊόντα της Cisco στον τομέα αυτό περιλαμβάνουν το σύστημα NetRanger, ένα σύστημα εντοπισμού-εισβολής σε πραγματικό χρόνο, και το NetSonar scanner, a proactive vulnerability scanner.

Μία ισχυρή λύση ασφαλείας περιλαμβάνει στοιχεία από όλες τις παραπάνω τεχνολογικές οικογένειες προκειμένου να διαθέτει ένα «έφυές», αυτοαμυνόμενο περιβάλλον δικτύου. Ωστόσο, το πιο βασικό στοιχείο είναι η δυνατότητα να διαχειριστεί κανείς αυτό το ουσιαστικό κομμάτι του «παζλ ασφαλείας», μέσω ενός κεντρικά χειριζόμενου, ολοκληρωμένου συστήματος.

Γιατί Cisco?

Προκειμένου να είναι πραγματικά αποδοτική μία λύση «πολιτικής» δικτύου πρέπει να πληρεί τρεις προϋποθέσεις και η Cisco Systems είναι η μοναδική εταιρεία που το έχει κατορθώσει αυτό.

- Πρώτον, η λύση θα πρέπει να εφαρμόσιμη από άκρη σε άκρη σε πολύ μεγάλα δίκτυα, καλύπτοντας πολλαπλά μέσα και περιβάλλοντα πρωτοκόλλων. Πρέπει να εφαρμόζει «πολιτικές» σε ίντρανετ, έξτρανετ, και ιδιωτικά εικονικά δίκτυα, ανεξάρτητα από την ιδιαίτερη δομή μεταξύ τους. Η Cisco έχει μία παράδοση στη δυνατότητα συνεργασία ετερογενών δικτύων με τη χρήση του λογισμικού Cisco IOS και συμβατών συσκευών.

- Δεύτερον, μία σταθερή «λύση» απαιτεί μία ‘έξυπνη’ infrastructure δικτύου για την εφαρμογή και ενίσχυση της «πολιτικής». Τα δίκτυα Cisco περιλαμβάνουν (ένθετες) τεχνολογίες οι οποίες διαθέτουν αυτή την «εξυπνάδα»- μέσω του λογισμικού Cisco IOS και τεχνολογίες σε switches and routers- και optimized features in internet appliances, όπως το Cisco PIX Firewall.
- Τρίτον, η λύση θα πρέπει να διαθέτει κεντρικό χειρισμό, με δυνατότητα για υψηλή διαβάθμιση. Η CiscoAssure έχει σχεδιαστεί έτσι ώστε να «μεταφέρει» εντολές ‘πολιτική’ από ένα κεντρικό σημείο στα δίκτυα ολόκληρης της επιχείρησης.

How CiscoAssure Works

Ας υποθέσουμε ότι ένας οργανισμός θέτει μία απλή «πολιτική» ασφαλείας, όπως « να μην επιτρέπεται καμία πρόσβαση Telnet, μέσα στο router, το οποίο προστατεύει the Engineering R &D server κάθε στιγμή». Πώς θα μπορούσε οι διαχειριστές του δικτύου αυτού να χρησιμοποιήσουν την CiscoAssure προκειμένου να εφαρμόσουν και να ενισχύσουν αυτή την πολιτική;

Αρχικά η «πολιτική» εισάγεται στην κεντρική διαχείριση GUI με κρυπτογραφημένες οδηγίες, οι οποίες μεταφέρονται στα μηχανήματα του δικτύου μέσω COPS, ως πολιτική σύνδεσης πληροφοριών. Τα μηχανήματα ασφάλειας της Cisco μεταφράζουν την πολιτική σύνδεσης πληροφοριών και προσαρμόζουν τους τοπικούς μηχανισμούς ασφάλειας (router ACLs, Firewall policy filters, NetRanger, alarm settings, κτλ) όπως απαιτείται.

Με ποιόν τρόπο η CiscoAssure εφαρμόζει και προσαρμόζει αυτή την πολιτική;

Φανταστείτε ότι ένας «μη έντιμος» μηχανικός εισέρχεται στο δίκτυο της επιχείρησης από μία απομακρυσμένη τοποθεσία. Ας υποθέσουμε ότι η σύνδεση/επικοινωνία του μηχανικού αυτού είναι κρυφή/κρυπτογραφημένη encrypted στο επίσης απομακρυσμένο «υποκατάστημα» Cisco 2500router, με τη χρήση του IPSec, και decrypted με ένα PIX Firewall, το οποίο είναι τοποθετημένο πίσω από έναCisco 7500 router. Ο εισβολέας αναγνωρίζεται/authenticated μέσω του server ελέγχου πρόσβασης CiscoSecure με τη χρήση του πρωτοκόλλου TACACS. Στη συνέχεια το PIX Firewall παραχωρεί πρόσβαση στο δίκτυο.

Ας υποθέσουμε τώρα ότι ο μηχανικός επιχειρεί στη συνέχεια να telnet μέσα στο Engineering R&D, το οποιο αναφέραμε νωρίτερα. Τότε το σύστημα Cisco NetRanger εντοπίζει αυτή τη μη εξουσιοδοτημένη δραστηριότητα σε πραγματικό

χρόνο και στέλνει σήμα συναγερμού στην κεντρική κονσόλα χειρισμού. Στο σημείο αυτό, η CiscoAssure θα προσαρμόσει είτε το Cisco 7500 router ACLs, είτε τα φίλτρα PIX Firewall έτσι ώστε να απαγορεύσει/καταστείλει αυτόματα τη μη εξουσιοδοτημένη δραστηριότητα και να «διώξει» τον εισβολέα από το δίκτυο.

Λεπτομερείς συναγερμοί, κλειδώματα και αναφορές από τη CiscoAssure για το γεγονός αυτό, δηλαδή την εισβολή, δίνουν τη δυνατότητα στους διαχειριστές να το εξετάσουν αναλυτικά και να κατανοήσουν την κατάσταση ασφαλείας του οργανισμού. Ως αποτέλεσμα μπορούμε να έχουμε δηλαδή ένα «εφυές», αυτοαμυνόμενο δίκτυο, διαχειριζόμενο από τη CiscoAssure και οδηγούμενο από την «πολιτική» ασφαλείας.

Το πλεονέκτημα της Cisco για ασφάλεια από άκρη-σε-άκρη
The Cisco Advantage for End-to-End Security

Η ασφάλεια εξακολουθεί να είναι κύριο μέλημα των οργανισμών που χρησιμοποιούν την τεχνολογία δικτύων προκειμένου να ανταγωνιστούν και αυτές στην παγκόσμια οικονομία του σήμερα. Μέχρι στιγμής, ο χειρισμός συστημάτων ασφαλείας αποτελεί μία τρομακτική δουλειά καθώς δεν διαθέτει κάποιον κεντρικό μηχανισμό για την εφαρμογή μιας «πολιτικής», την επαλήθευσή της ή την ενίσχυσή της στα διανεμημένα δίκτυα μίας επιχείρησης.

Η Cisco παρέχει στους διαχειριστές/χειριστές των δικτύων μιας επιχείρησης μία λύση η οποία τους δίνει τη δυνατότητα να ελαχιστοποιήσουν τον κίνδυνο χειρισμού. Η CiscoAssure διαθέτει ένα απλό, ολοκληρωμένο σύστημα έτσι ώστε οι λύσεις ασφαλείας της Cisco να μπορούν να «συμβιβαστούν' με τις «πολιτικές» ενός οργανισμού.

Η CiscoAssure δίνει τη δυνατότητα αποτελεσματικής διαχείρισης/χειρισμού μίας intelligent network infrastructure, η οποία καλύπτει τα βασικά σημεία στα οποία επιθυμεί ασφάλεια μία επιχείρηση. Με αυτόν τον τρόπο η ciscoassure «απελευθερώνει» τους διευθυντές/διαχειριστές των επιχειρήσεων από το άγχος της προστασίας δίνοντάς τους τη δυνατότητα να επικεντρωθούν σε άλλους τομείς.

ΠΕΡΙΕΧΟΜΕΝΑ

ΒΙΒΛΙΟΓΡΑΦΙΑ

SITES : WWW.INTELL.COM Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με τις λύσεις που προσφέρει η επιχείρηση στον τομέα της ασφάλειας των δικτύων επιχειρήσεων.

www.cert.org

Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με τους τρόπουσαντιμετώπισης επιθέσεων από διάφορους ιούς.

www.cisco.com.

Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με τις λύσεις που προσφέρει η επιχείριση σχετικά με την ασφαλή διακίνηση πληροφοριών μέσω ανοιχτών δικτύων.

www.novell.com

Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με τις λύσεις που προσφέρει η επιχείριση σχετικά με την ασφάλεια δικτύων.

www.security .com

Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με λύσεις ασφάλειας.

www.rsa.com.

Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με τον αλγόριθμο κρυπτογράφησης RSA καθώς και ειδικότερες πληροφορίες για θέματα τα οποία

αφορούν λύσεις προστασίας των ευαίσθητων δεδομένων που διακινούνται καθημερινά μέσω των δικτύων των επιχειρήσεων και μέσω του internet.
www.pgp.com.
Στο site αυτό μπορούμε να βρούμε πληροφορίες σχετικά με το πολύ δημοφιλές πρόγραμμα PGP το οποίο μας επιτρέπει την κρυπτογράφηση των e-mail μας με τα διακινούμε σε καθημερινή βάση πολλά προσωπικά δεδομένα τα οποία χωρίς τη βοήθεια που μας προσφέρει η χρήση μεθόδων κρυπτογράφησης είναι εκτεθειμένα στον οποιονδήποτε κακόβουλο χρήστη και θα μπορούσε πολλύ εύκολα να μας τα υποκλέψει.