Οδηγός επίλυσης προβλημάτων της Cisco

Αξιοποιήστε πλήρως την τεχνολογία της πληροφορικής – Δέκα βασικές συμβουλές για την ασφάλεια της επιχείρησής σας

Αν είστε επαγγελματίας, τότε σίγουρα σας αφορά το θέμα της ασφάλειας. Η ασφάλεια των πληροφοριών, των εγκαταστάσεων, των στοιχείων των πελατών σας θα πρέπει να διαδραματίζει κυρίαρχο ρόλο στην επιχείρησή σας, ακόμα και αν δεν αποτελεί μέρος της κύριας αποστολής της. Η δυσκολία έγκειται στο γεγονός ότι κυκλοφορεί τεράστιος όγκος πληροφοριών, όχι πάντα χρήσιμος. Ο μη ειδικός καλείται διαρκώς να λάβει αποφάσεις, όπως: Μου λένε ότι χρειάζομαι ένα firewall, αλλά πλέον υπάρχει firewall ενσωματωμένο στα Windows. Γιατί λοιπόν χρειάζομαι κι άλλο;

Με αυτόν τον οδηγό επιδιώκουμε να σας ενημερώσουμε για μια σειρά θεμάτων που πρέπει να εξετάσετε και ξεκινάμε εφοδιάζοντάς σας με τις πληροφορίες που κατά πάσα πιθανότητα θα χρειαστείτε. Θα επισημάνουμε επίσης ορισμένα διαχειριστικά και λιγότερο τεχνικά ζητήματα, τα οποία αντιμετωπίζουν όσοι ασχολούνται με την προστασία της επιχείρησής τους.

Δέκα βασικές συμβουλές

1. Πρόγραμμα προστασίας από ιούς (antivirus):

Ένα πακέτο προγράμματος προστασίας από ιούς (antivirus) είναι απολύτως απαραίτητο, δυστυχώς όμως δεν τα καταφέρνουν όλα εξίσου καλά. Πιθανόν να γνωρίζετε ότι ένα πακέτο antivirus λειτουργεί παίρνοντας στοιχεία από μια βάση δεδομένων σχετικά με οτιδήποτε μπορεί να αποτελεί απειλή για το σύστημά σας, ανά πάσα στιγμή (και για αυτόν το λόγο είναι ιδιαίτερα σημαντικό να ενημερώνετε εγκαίρως τη συνδρομή σας).

Εντούτοις, αυτό σημαίνει ότι, αν το πακέτο antivirus που διαθέτετε αγνοεί την ύπαρξη ενός συγκεκριμένου ιού, τότε δεν μπορεί να σας προστατέψει από αυτόν. Για αυτό η Cisco® συνιστά, εκτός από το σύστημα antivirus, και ένα Σύστημα Αποτροπής Εισβολών (Intrusion Prevention System). Η διαφορά είναι διπλή, αφενός το IPS ελέγχει ένα ολόκληρο πακέτο πληροφοριών για οτιδήποτε δείχνει παρείσακτο και αφετέρου παρακολουθεί το σύστημα για οποιαδήποτε ασυνήθιστη συμπεριφορά ενός προγράμματος λογισμικού στον υπολογιστή σας. Με άλλα λόγια δεν ψάχνει μόνο ιούς που ήδη γνωρίζει, αλλά σε περίπτωση που ένα πρόγραμμα αρχίσει να συμπεριφέρεται παράξενα, π.χ. διαγράφει άλλα αρχεία, ελέγχει τη βάση δεδομένων των πελατών σας κ.ο.κ., θα το σταματήσει. Οι ειδικοί σε θέματα ασφαλείας αποκαλούν αυτήν τη δραστηριότητα, την εκμετάλλευση δηλαδή ενός τρωτού σημείου ή μίας 'τρύπας' ενός προγράμματος ή ενός συστήματος προτού γίνει γνωστή στον κατασκευαστή, επίθεση "zero day". Μπορούμε να τη σταματήσουμε παρακολουθώντας περισσότερο τυχόν ασυνήθιστες συμπεριφορές.

Υπάρχουν διάφορα επίπεδα IPS, βασισμένα σε υπολογιστές και βασισμένα σε δίκτυα. Τα βασισμένα σε δίκτυο συστήματα IPS βρίσκονται στο σημείο εισόδου του δικτύου σας. Τα βασισμένα σε υπολογιστές συστήματα IPS βρίσκονται στο φορητό υπολογιστή σας και όχι στο δίκτυό σας με αποτέλεσμα να εξακολουθείτε να είστε προστατευμένοι όταν συνδέεστε σε άλλο δίκτυο.

2. Firewall:

Το firewall κάνει πολλά περισσότερα από μια απλή επισήμανση σε πλαίσιο ελέγχου που υποδηλώνει ότι διαθέτετε firewall. Ορισμένα είναι ενσωματωμένα στο λειτουργικό σύστημα, ενώ άλλα βρίσκονται σε ξεχωριστά μηχανήματα ενός δικτύου.

Το πιο σημαντικό από όλα είναι αυτό που ψάχνει να βρει το Firewall. Κάποια ψάχνουν να εντοπίσουν ό,τι θεωρούν απειλή για το δίκτυο, δηλαδή ουσιαστικά αυτό που χρειάζεστε. Στη Cisco προσφέρουμε επίσης προστασία σε επίπεδο εφαρμογών, έτσι ώστε, εάν ένα τμήμα κώδικα φαίνεται ότι μπορεί να προκαλέσει την ασυνήθιστη συμπεριφορά ενός επιμέρους προγράμματος, να εντοπίζεται. Είναι απαραίτητο να διαθέτετε firewall, το οποίο δεν βρίσκεται στον υπολογιστή σας, αλλά σε άλλο υπολογιστή, δρομολογητή (router) ή άλλη συσκευή που λειτουργεί ως πύλη για το δίκτυό σας. Εάν αυτή η συσκευή είναι η μοναδική πύλη, μέσω της οποίας διέρχεται η κυκλοφορία των δεδομένων για να φτάσει στο σύστημα του υπολογιστή σας, τότε η τοποθέτηση ενός τέτοιου προγράμματος προστασίας είναι συνετή επιλογή. Η Cisco διαθέτει πληθώρα επιπέδων ασφαλείας στις προσφορές της.

3. Εργαζόμενοι:

Προτού διεισδύσουμε περαιτέρω σε τεχνολογικά θέματα, αξίζει να αναλογιστούμε το μέγεθος του κινδύνου μη τεχνικής φύσης που διατρέχει μια επιχείρηση. Ας αναφερθούμε σε μερικούς τομείς στους οποίους έχουν χαθεί ή έχουν εκτεθεί δεδομένα:

- Όταν έχει καθιερωθεί αυστηρή πολιτική για το ποιος έχει πρόσβαση σε τι, με την προϋπόθεση ότι είναι ηλεκτρονικά αποθηκευμένο – αλλά η εφαρμογή της πολιτικής αυτής μπορεί να παραλείπεται σε έντυπο υλικό που πιθανόν να βρεθεί ξεχασμένο σε τρένα, διαδρόμους ξενοδοχείων κ.λπ.
- Όταν δεν θυμούνται όλοι ότι πρέπει να σβήνουν τις οθόνες τους φεύγοντας από το γραφείο – οι επισκέπτες μπορούν και σίγουρα θα διαβάσουν εμπιστευτικό υλικό από τις οθόνες (να σημειωθεί σε αυτό το σημείο ότι η προστασία οθόνης δαπανά ρεύμα χωρίς λόγο και οι ημέρες που προστάτευε την οθόνη από οτιδήποτε έχουν παρέλθει ανεπιστρεπτί).
- Συγχωρήστε μας για το στερεότυπο, αλλά εξακολουθεί να ισχύει: Σε καμία περίπτωση δεν αποτελεί ασφαλή κωδικό πρόσβασης το όνομα του σκύλου/του συντρόφου/της οδού κάποιου, πόσο μάλλον η λέξη p-a-s-s-w-o-r-d.
- Σε γενικές γραμμές, η μη ύπαρξη ξεκάθαρης πολιτικής σχετικά με το τι πρέπει να γίνει για να είναι ασφαλές ένα δίκτυο, ποιος πρέπει να το κάνει και ποιες θα είναι οι κυρώσεις για όποιον δεν συμμορφώνεται. Αντιμετωπίζετε τους γύρω σας ως ευφυείς ενηλίκους και θα εκπλαγείτε με το πόσο γρήγορα θα θελήσουν να συνεργαστούν.
- Συμπεριλάβετε σε αυτήν την πολιτική ότι κανείς δεν μπορεί να κατεβάζει λογισμικό κατά βούληση. Ένα μεγάλο μέρος του θα είναι ακίνδυνο, αλλά είναι αναγκαίο να έχετε τον έλεγχο των αδειών χρήσης λογισμικού και να απομονώνετε το δίκτυό σας από τον κίνδυνο κακόβουλου λογισμικού.

4. Συσκευές:

Οι συσκευές που εισέρχονται στο κτίριο και εξέρχονται από αυτό: Αν εργαζόσασταν στο Υπουργείο Άμυνας, θα έπρεπε, όπως λέγεται, να παραδώσετε το κινητό σας ή τη συσκευή αναπαραγωγής μουσικής σας στην είσοδο και να την παραλάβετε μόνο κατά την αναχώρησή σας. Αυτό δεν συμβαίνει επειδή δεν εμπιστεύονται τους εργαζομένους, αλλά επειδή τα τηλέφωνα, οι φωτογραφικές μηχανές και παρόμοιες συσκευές μπορεί να περιέχουν δεδομένα. Ένα iPhone 3G (επιλέγεται καθαρά λόγω των κορυφαίων του πωλήσεων) διαθέτει χωρητικότητα 16 gigabyte σε ορισμένες περιπτώσεις. Με σύνδεση σε μια θύρα USB ενός υπολογιστή οποιοσδήποτε μπορεί να φύγει από τη δουλειά έχοντας μεταφέρει τον κατάλογο των πελατών σας σε οποιοδήποτε μέσο έχει μαζί του. Εναλλακτικά κάποιος μπορεί να εισαγάγει κάποιον ιό στο σύστημά σας.

Ίσως να μην θέλετε να εφαρμόσετε τόσο δρακόντεια μέτρα απαγορεύοντας κάθε μορφή προσωπικής συσκευής μεταφοράς δεδομένων στο χώρο εργασίας σας, αλλά σίγουρα μπορείτε να λάβετε τα μέτρα σας:

- Μπορείτε να διαμορφώσετε τους υπολογιστές έτσι ώστε να μην δέχονται συσκευές USB.
- Έξυπνο λογισμικό παρακολούθησης, όπως εκείνο που είναι προεγκατεστημένο σε όλα τα προϊόντα της Cisco, θα ανιχνεύσει οποιαδήποτε ασυνήθιστη δραστηριότητα στο δίκτυό σας και θα την αναφέρει.
- Αν συνδέονται επισκέπτες (guests) στο δίκτυό σας, τότε είναι επιτακτική ανάγκη να ελέγχετε τον εξοπλισμό τους (π.χ. αν χρησιμοποιούν δικό τους φορητό υπολογιστή) και να τον εξισώνετε με το δικό σας επίπεδο ασφαλείας. Και πάλι, ο εξοπλισμός της Cisco θα ελέγξει αυτούς τους υπολογιστές και τις άλλες συσκευές μόλις συνδεθούν, αναζητώντας όχι μόνο γνωστούς ιούς, αλλά και οποιαδήποτε ασυνήθιστη δραστηριότητα.

5. Διασφάλιση δεδομένων οικιακών ή απομακρυσμένων χρηστών:

Φυσικά δεν έχει κανένα νόημα να διασφαλίζετε εσωτερικά το δίκτυό σας αν πρόκειται να γίνει διαρροή πληροφοριών ακριβώς έξω από το χώρο του γραφείου σας. Αυτό συνεπάγεται τα εξής: Αρχικά, διασφαλίστε ότι οποιοσδήποτε σύνδεσμος προς το δίκτυό σας από το Internet πραγματοποιείται μέσω του κατάλληλου Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network) με όλα τα χαρακτηριστικά ασφαλείας που το συνοδεύουν. Στη συνέχεια, βεβαιωθείτε ότι τα μη τεχνικά μέρη τις δραστηριότητας των εργαζομένων σας υπόκεινται στην ίδια ασφάλεια με εκείνη εντός του γραφείου. Δηλαδή, αν δεν έχουν δυνατότητα εκτύπωσης, μεταφοράς στοιχείων σε συσκευές USB κ.λπ., όταν βρίσκονται στο γραφείο, δεν πρέπει να νομίζουν ότι μπορούν να το πράξουν από το σπίτι.

Μπορείτε να επιτύχετε πολλά εγκαθιστώντας ένα δίκτυο έξυπνης μεταγωγής στο γραφείο και ασφαλίζοντας την πύλη του με το κατάλληλο σύνολο προϊόντων της Cisco.

6. Ασύρματα δίκτυα:

Μια υποενότητα του κεφαλαίου σχετικά με τη διασφάλιση των δεδομένων οικιακών και απομακρυσμένων χρηστών είναι η εξέταση των ρυθμίσεων ασύρματων δικτύων, τόσο σε εσωτερικό όσο και σε εξωτερικό επίπεδο και εφόσον είναι υπό τον έλεγχό σας. Μη βασίζεστε σε δίκτυο που εμφανίζεται ως 'ασφαλές' όταν το εντοπίσει κάποιος φορητός υπολογιστής ή κάποιο smartphone. Αυτό μπορεί να σημαίνει ότι διαθέτει μόνο ασφάλεια WEP, η οποία πλέον είναι ξεπερασμένη και θα μπορούσε να παραβιαστεί από οποιονδήποτε ενημερωμένο χάκερ.

Στο γραφείο, το σύνολο του εξοπλισμού δικτύωσης που παρέχει η Cisco θα περιλαμβάνει ενσωματωμένη ασφάλεια στο βασικό εξοπλισμό, την οποία θα μπορούν να διαμορφώσουν οι εξειδικευμένοι μας συνεργάτες. Εκτός γραφείου, οι εργαζόμενοι θα μπορούν να χρησιμοποιούν το δικό τους ασύρματο εξοπλισμό. Είναι απόλυτα λογικό να επιμένετε για την προστασία από τα εξής στοιχεία:

- Αν διαθέτει ρύθμιση WEP, θα πρέπει να αναβαθμιστεί σε κάτι με WPA.
- Οι προεπιλεγμένοι κωδικοί πρόσβασης που προέρχονται από τη συσκευασία με τον οικιακό εξοπλισμό πρέπει να αλλαχθούν.
- Ο υπολογιστής και ο δρομολογητής (router) δικτύου θα διαθέτουν ένα αναγνωριστικό με την ονομασία SSID, το οποίο θα μπορεί να εντοπιστεί στο μενού ρύθμισης του δρομολογητή. Αλλάξτε το και διακόψτε τη μετάδοση του SSID, έτσι κανείς δεν θα μπορεί να εντοπίσει τον υπολογιστή σας όταν προσπαθεί να εισέλθει παράνομα σε κάποιο δίκτυο.
- Απενεργοποιήστε την αυτόματη σύνδεση σε ασύρματα δίκτυα έτσι ώστε ο χρήστης να συνδέεται μόνο σε δίκτυα που εμπιστεύεστε.
- Αντιστοιχίστε μια στατική διεύθυνση IP στις συσκευές σας. Η εναλλακτική είναι η τυχαία αντιστοίχιση αυτών των διευθύνσεων από το δίκτυό σας, γεγονός ωστόσο που σας δημιουργεί προβλήματα όταν θέλετε να αποκλείσετε μια συγκεκριμένη συσκευή.
- Ο δρομολογητής σας κατά πάσα πιθανότητα θα έχει firewall – βεβαιωθείτε ότι είναι ενεργοποιημένο αφού πολλές φορές οι συσκευές αποστέλλονται με το firewall απενεργοποιημένο από προεπιλογή.
- Απενεργοποιήστε το δίκτυο αν πρόκειται να μη χρησιμοποιηθεί για μεγάλο χρονικό διάστημα.

7. Παράνομη πρόσβαση – Πόσο πιθανή είναι;

Μέχρι στιγμής μιλήσαμε για τον τρόπο αποφυγής της παράνομης πρόσβασης και την αποτροπή ανεπιθύμητων εισβολών στο δίκτυο των υπολογιστών σας. Πόσο πιθανό είναι όμως να δοκιμάσει κάποιος να παρεισφρύσει στο σύστημά σας; Πολλοί πελάτες της Cisco είναι μικρότερες επιχειρήσεις και, όπως πιστεύουν, σίγουρα κανείς δεν ενδιαφέρεται στην πραγματικότητα...

Παλαιότερα, όταν η παράνομη πρόσβαση σε δεδομένα γινόταν αποκλειστικά από ανθρώπους-χάκερ, αυτό ήταν πιθανότατα πιο αληθοφανές. Όχι όμως πια. Το πρόβλημα είναι ότι πλέον πολλές εισβολές γίνονται με αυτοματοποιημένο τρόπο. Θεωρήστε ότι ο χάκερ είναι ο συντονιστής πολλών κλεφτών οι οποίοι πρέπει να εισβάλουν σε αφύλακτα σπίτια για να δουν πού υπάρχει κάτι πολύτιμο για να κλέψουν. Σε αυτήν την περίπτωση, τα σπίτια είναι οι υπολογιστές και μοιάζουν όλοι ίδιοι, έτσι ο μόνος τρόπος να δει κανείς αν έχει κάτι να κερδίσει είναι πρώτα να εισβάλει και να ρίξει μια ματιά.

Αυτό γίνεται μέσω αυτοματοποιημένων διαδικτυακών ρομπότ τα οποία κάνουν αυτό που ονομάζεται διερεύνηση θυρών (port scanning) και που ουσιαστικά σημαίνει ότι έρχονται στην 'πόρτα' του δικτύου σας στο Internet και το πρώτο πράγμα που κάνουν είναι να βλέπουν αν είναι κλειδωμένη. Προφανώς καλό θα ήταν να είναι.

(Και μην ξεχνάτε και τις πραγματικές σας πόρτες. Η Cisco προσφέρει κάμερες που μπορούν να συνδεθούν στο Internet, ώστε να μπορείτε να δείτε τι συμβαίνει στο γραφείο σας, ανεξάρτητα από το πού βρίσκεστε. Ορισμένες ενεργοποιούνται όταν ανιχνεύουν κίνηση και έτσι μπορούν να σας ειδοποιούν ανά πάσα στιγμή όταν κάποιος εισέρχεται σε μη εξουσιοδοτημένο χώρο).

8. Online επιχειρήσεις:

Αν το μεγαλύτερο μέρος ή το σύνολο των επιχειρήσεών σας πραγματοποιείται online, τότε σίγουρα θα χρειαστεί να προβείτε σε ενέργειες ώστε να προστατέψετε τόσο τις πληροφορίες των μετοχών σας, εφόσον είναι εμπιστευτικές, όσο και τα δεδομένα των πελατών σας. Όλα τα μέτρα που έχουμε ήδη αναφέρει θα συμβάλλουν στην προστασία αυτή, αλλά υπάρχουν και κάποια ακόμα, διαχειριστικά αλλά και τεχνικά, στα οποία περιλαμβάνεται και η αποφυγή των πρακτικών της κυβέρνησης, να αφήνει εδώ κι εκεί μη κωδικοποιημένα CD, που μπορεί να βρεθούν ακόμα και μέσα σε λεωφορεία, για παράδειγμα! (Να θυμάστε ότι πρέπει να κωδικοποιείτε τα CD ώστε κανείς να μην μπορεί να διαβάσει τα δεδομένα, ακόμα και αν 'σπάσει' τον κωδικό πρόσβασης).

9. Πως λοιπόν γίνεται η απόσβεση;

Πολλές μικρότερες επιχειρήσεις, ιδιαίτερα σε καιρούς οικονομικής δυσχέρειας, προβληματίζονται κατά πόσο κάθε τεχνολογική επένδυση μπορεί να κάνει απόσβεση των δαπανών της. Κάτι τέτοιο είναι ελαφρώς περίπλοκο όσον αφορά τις δαπάνες για την ασφάλεια αφού πρόκειται για άυλο αγαθό. Πιθανότατα πληρώσατε για να βάλετε κλειδαριές στο σπίτι σας, κάποια στιγμή, αλλά ποτέ δεν υπολογίσατε πόσο χρειάστηκε για να κάνουν απόσβεση. Απλώς γνωρίζετε τι θα μπορούσατε να είχατε χάσει αν κάποιος τις παραβίαζε.

Υπάρχει ωστόσο κάποιο κέρδος από τις επενδύσεις σε δαπάνες για την ασφάλεια, το οποίο μπορούμε εύκολα να αναλύσουμε. Εάν για παράδειγμα λειτουργείτε ένα δικτυακό τόπο ηλεκτρονικού εμπορίου και δεν μπορείτε να διαβεβαιώσετε τους πελάτες σας ότι τα δεδομένα τους είναι ασφαλή, θα δείτε σε πολύ σύντομο χρονικό διάστημα την επιχείρησή σας να καταρρέει. Αν έχετε επισκέπτες στις εγκαταστάσεις σας, οι οποίοι συνδέονται στο δίκτυό σας και φεύγουν αγκαλιά με ένα νέο ιό στον υπολογιστή τους εξαιτίας της ρύθμισης ασφαλείας σας, πολύ σύντομα θα διακόψουν τις συναλλαγές μαζί σας. Και ούτω καθεξής.

Αξίζει να επισημάνουμε, ωστόσο, ότι ο βασικός εξοπλισμός δεν κοστίζει μια περιουσία. Για ένα μικρό γραφείο με μονοψήφιο αριθμό υπαλλήλων μπορείτε να βρείτε τον κατάλληλο ασύρματο δρομολογητή με firewall και πλήρη ασφάλεια με λιγότερα από €170.

10. Εξωτερική ανάθεση ασφαλείας:

Αν εξακολουθείτε να βρίσκετε το κόστος απαγορευτικό, αξίζει να εξετάσετε την περίπτωση εξωτερικής ανάθεσης ολόκληρης της υποδομής ασφαλείας σας. Υπάρχουν πολλοί συνεργάτες της Cisco που εξειδικεύονται στο να καθιστούν μικρές επιχειρήσεις ασφαλέστερες από πριν, και ακριβώς επειδή είναι ειδικοί, διαθέτουν ικανότητες και τιμές που δεν θα θέλετε να δαπανήσετε το χρόνο για να αποκτήσετε. Η μεταφορά όλων των δεδομένων σας εκτός των εγκαταστάσεών σας και η ανάθεση της φύλαξής τους σε μια εξειδικευμένη και αξιόπιστη εταιρεία είναι ένα επιπλέον επίπεδο προστασίας που εξυπηρετεί πολλές μικρότερες επιχειρήσεις.

Όπως είπαμε και στην αρχή, αν έχετε επιχείρηση οποιασδήποτε δυναμικότητας, τότε, θέλοντας και μη, εμπλέκεστε στον τομέα της ασφάλειας. Ευτυχώς τα πρώτα βήματα για τη διασφάλιση του δικτύου σας δεν κοστίζουν μια περιουσία και εμείς διαθέτουμε την πραγματογνωμοσύνη που χρειάζεται ώστε να σας βοηθήσουμε να την αποκτήσετε.

Καλή επιτυχία!