Microsoft Business Solutions

Navision Security Hardening Guide

Έκδοση: Οκτώβριος 2004

Microsoft

Περιεχόμενα

Εισαγωγή

Τα Microsoft® Windows® παρέχουν εξελιγμένη ασφάλεια δικτύου βάσει προτύπων. Η ασφάλεια, υπό την ευρεία έννοια, αφορά διαδικασίες σχεδιασμού και σημαντικές αντισταθμίσεις. Για παράδειγμα, μπορείτε να κλειδώσετε έναν υπολογιστή σε ένα χώρο φύλαξης και η πρόσβαση σε αυτόν να είναι δυνατή μόνο από το διαχειριστή συστήματος. Ο υπολογιστής αυτός ενδεχομένως να είναι ασφαλής, αλλά δεν είναι ιδιαίτερα χρήσιμος γιατί δεν συνδέεται με κανέναν άλλο υπολογιστή. Αυτό που χρειάζεστε είναι να διασφαλίσετε όσο το δυνατόν περισσότερο την ασφάλεια του δικτύου χωρίς να χρειαστεί να θυσιάσετε τις δυνατότητες χρήσης του.

Οι περισσότεροι οργανισμοί σχεδιάζουν λύσεις για επιθέσεις από εξωτερικούς παράγοντες και κατασκευάζουν τείχη προστασίας, αλλά πολλές εταιρείες δεν ξέρουν πώς να αντιμετωπίσουν μια παραβίαση της ασφάλειας που πραγματοποιεί κάποιος κακόβουλος χρήστης εισβάλλοντας στο τείχος προστασίας. Τα μέτρα ασφαλείας που θα εφαρμοστούν από τον πελάτη σας θα είναι επαρκή μόνο στην περίπτωση που οι χρήστες δεν θα χρειάζονται να εκτελούν πολλές διεργασίες και βήματα για να διασφαλίσουν την ασφάλεια των ενεργειών τους. Η εφαρμογή των πολιτικών ασφαλείας πρέπει να είναι όσο το δυνατόν πιο εύκολη για τους χρήστες. Σε αντίθετη περίπτωση, οι τελευταίοι θα αναζητήσουν λιγότερο ασφαλείς τρόπους για να κάνουν ό,τι χρειάζονται.

Επειδή το μέγεθος των εγκαταστάσεων του Navision ποικίλλει, είναι σημαντικό να λάβετε υπόψη τις ανάγκες του κάθε πελάτη και να υπολογίσετε την αποτελεσματικότητα της ασφάλειας σε σχέση με το κόστος που απαιτείται. Ως έμπιστος σύμβουλος του πελάτη σας, εξετάστε προσεκτικά τις απαιτήσεις και προτείνετε μια πολιτική που να ικανοποιεί τις ανάγκες σε ασφάλεια χωρίς να δημιουργεί οποιοδήποτε εμπόδιο που θα αναγκάσει τον πελάτη να σταματήσει την εφαρμογή της.

Οι καλύτερες πρακτικές ασφάλειας του Navision

Οι ακόλουθοι γενικοί κανόνες μπορούν να σας βοηθήσουν να αυξήσετε την ασφάλεια του περιβάλλοντος εργασίας του Navision:

- Αν θέλετε να εκτελέσετε το Navision Database Server ως υπηρεσία ή να χρησιμοποιήσετε την παράμετρο γραμμής εντολής *installasservice* όταν ξεκινάτε το διακομιστή, θα πρέπει να βεβαιωθείτε ότι η υπηρεσία εκτελείται ως λογαριασμός NT Authority\Network Service. Ο λογαριασμός NT Authority\Network Service είναι διαθέσιμος μόνο στα Windows™ XP και στο Windows Server™ 2003. Αν εκτελείτε Windows 2000 Server, θα πρέπει να δημιουργήσετε ένα λογαριασμό με τα λιγότερα δικαιώματα για την υπηρεσία, διαφορετικά θα αντιστοιχιστεί στην υπηρεσία ένα λογαριασμός τοπικού συστήματος Local System. Αυτός ο λογαριασμός θα πρέπει να έχει το πολύ όσα δικαιώματα έχει ο κανονικός λογαριασμός Users ή να είναι λογαριασμός τομέα που δεν είναι administrator ούτε στον τομέα ούτε σε κάποιον τοπικό υπολογιστή.

  Θυμηθείτε να δώσετε στο λογαριασμό NT Authority\Network Service ή στο λογαριασμό χρήστη, με τον οποίο εκτελείται ο διακομιστής, δικαιώματα πρόσβασης στα αρχεία της βάσης δεδομένων για ανάγνωση και εγγραφή, ώστε να είναι δυνατή η σύνδεση των χρηστών με τη βάση δεδομένων.

  Για να δώσετε δικαιώματα πρόσβασης σε ένα αρχείο της βάσης δεδομένων για ανάγνωση και εγγραφή στο λογαριασμό NT Authority\Network Service στα Windows XP:

  1. Στην Εξερεύνηση των Windows, μεταβείτε στο φάκελο που περιέχει το αρχείο της βάσης δεδομένων.
  2. Επιλέξτε το αρχείο της βάσης δεδομένων, κάντε δεξί κλικ και επιλέξτε Ιδιότητες.
  3. Στο παράθυρο ***Ιδιότητες***, κάντε κλικ στην καρτέλα ***Ασφάλεια*** και σο πεδίο **Ονόματα χρηστών και ομάδων**, πατήστε Προσθήκη.
  4. Στο παράθυρο ***Επιλογή χρηστών, υπολογιστών ή ομάδων*** καταχωρήστε *Network Service (Υπηρεσία δικτύου)* και πατήστε OK.
  5. Το NETWORK SERVICE προστίθεται στο πεδίο **Ονόματα χρηστών και ομάδων** στο παράθυρο ***Ιδιότητες***.
  6. Επιλέξτε NETWORK SERVICE και στο πεδίο **Δικαιώματα** καταχωρήστε δικαίωμα *ανάγνωσης* και *εγγραφής*.
- Η υπηρεσία Navision Application Server εκτελείται ως λογαριασμός NT Authority\ Network Service από προεπιλογή και με αυτόν τον τρόπο επιτρέπεται η πρόσβαση της τοπικά στο Navision Database Server. Ωστόσο, θα πρέπει να βεβαιωθείτε ότι σε ένα δίκτυο η υπηρεσία Navision Application Server εκτελείται ως λογαριασμός τομέα Windows που αναγνωρίζεται από το Navision Database Server, για να μπορείτε να έχετε πρόσβαση στο διακομιστή βάσης δεδομένων. Αυτός ο λογαριασμός δεν πρέπει να είναι Administrator ούτε στον τομέα ούτε σε οποιονδήποτε τοπικό υπολογιστή.
- Αν εκτελείται το SQL Server Option for Navision, το Microsoft SQL Server™ εκτελείται ως υπηρεσία. Το SQL Server Option for Navision προϋποθέτει ότι το SQL Server έχει τη δυνατότητα να πραγματοποιεί αναζήτηση και να κάνει λήψεις των ομάδων χρηστών Windows από τον κατάλογο Active Directory ώστε να ικανοποιούνται οι ανάγκες για έλεγχο ταυτοτήτων. Πρέπει συνεπώς να διασφαλίσετε ότι η υπηρεσία SQL Server εκτελείται ως λογαριασμός NT Authority\Network Service.

Για να διασφαλίσετε ότι η υπηρεσία εκτελείται ως NT Authority\Network Service:

1. Στον υπολογιστή SQL Server εντοπίστε την υπηρεσία MSSQLSERVER, κάντε δεξί κλικ και επιλέξτε Ιδιότητες.
2. Στο παράθυρο ***Ιδιότητες***, επιλέξτε την καρτέλα ***Σύνδεση***.
3. Στην καρτέλα ***Σύνδεση***, στο πεδίο «Σύνδεση ως» επιλέξτε «Αυτός ο λογαριασμός», καταχωρήστε *NT Authority\NetworkService* και πατήστε OK.

Για περισσότερες πληροφορίες σχετικά με την ασφάλεια του SQL Server μεταβείτε στις διευθύνσεις:

http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

και

http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- Αν εκτελείτε ένα προϊόν ηλεκτρονικού εμπορίου του Navision όπως το Commerce Gateway, βεβαιωθείτε ότι ο διακομιστής Commerce Gateway Request Server έχει εγκατασταθεί σωστά με την προεπιλεγμένη ρύθμιση λογαριασμού για τις υπηρεσίες. Η προεπιλεγμένη ρύθμιση λογαριασμού ονομάζεται *CGRSUser* και εκχωρεί στο Commerce Gateway Server δικαίωμα πρόσβασης στην ελάχιστη ομάδα των άλλων υπηρεσιών που απαιτεί, συμπεριλαμβανομένων των υπηρεσιών *MSSQLSERVER* και *BizTalk Service BizTalk Group: BizTalkServerApplication* και δεν περιλαμβάνει συνολικές ρυθμίσεις λογαριασμού, όπως συμβαίνει με το λογαριασμό *τοπικού συστήματος*.
- Χρησιμοποιείτε πάντα δύσκολους κωδικούς πρόσβασης. Για περισσότερες πληροφορίες σχετικά με τους δύσκολους κωδικούς πρόσβασης, ανατρέξτε στην ενότητα Δύσκολοι κωδικοί πρόσβασης.
- Χρησιμοποιείτε συνδέσεις Windows. Το Navision σας επιτρέπει να δημιουργείτε δύο τύπους σύνδεσης: συνδέσεις βάσης δεδομένων και συνδέσεις Windows. Σας συνιστούμε να χρησιμοποιείτε συνδέσεις Windows οι οποίες χρησιμοποιούν έλεγχο ταυτότητας Windows και σας δίνουν τη δυνατότητα να εφαρμόσετε καλύτερη πολιτική κωδικού πρόσβασης.
- Οι κωδικοί πρόσβασης δεν πρέπει να ξαναχρησιμοποιούνται. Το φαινόμενο της εκ νέου χρήσης των κωδικών πρόσβασης μεταξύ συστημάτων και τομέων είναι σύνηθες. Για παράδειγμα, κάποιος διαχειριστής, υπεύθυνος για δύο τομείς, μπορεί να δημιουργήσει λογαριασμούς Domain Administrator στον καθένα που να χρησιμοποιούν τον ίδιο κωδικό πρόσβασης, και ακόμα να ορίσει ίδιους κωδικούς πρόσβασης τοπικού διαχειριστή σε υπολογιστές του ίδιου τομέα. Σε αυτήν την περίπτωση, αν ένας υπολογιστής ή λογαριασμός εκτεθεί σε κίνδυνο τότε ενδέχεται να εκτεθεί σε κίνδυνο και ολόκληρος ο τομέας.
- Μετά την εγκατάσταση του Navision και τη δημιουργία ή την ενημέρωση των βάσεων, πρέπει να δημιουργήσετε μια σύνδεση Windows και να αντιστοιχίσετε σε αυτήν το ρόλο SUPER στο Navision. Αυτός ο χρήστης SUPER θα διαχειρίζεται τη βάση δεδομένων, την ασφάλεια, κ.α. Δώστε σε αυτήν τη σύνδεση έναν δύσκολο κωδικό πρόσβασης. Αυτός ο κωδικός δεν θα πρέπει να γνωστοποιηθεί. Θα πρέπει να εγγυάται την ίδια προστασία που προσφέρει ο κωδικός πρόσβασης διαχειριστή συστήματος στο SQL Server. Ο ρόλος SUPER διαχειρίζεται όλα τα δικαιώματα πρόσβασης στη βάση δεδομένων για την οποία απαιτείται το μέγιστο επίπεδο προστασίας. Ο κωδικός πρόσβασης του χρήστη SUPER θα πρέπει να γνωστοποιείται μόνο στους διαχειριστές του συστήματός σας (System Administrators).
- Οι υπόλοιποι χρήστες που έχουν πρόσβαση στη βάση δεδομένων του Navision θα πρέπει να έχουν τα λιγότερα δικαιώματα. Αυτό σημαίνει ότι σε αυτούς αντιστοιχίζονται ρόλοι στο Navision που τους επιτρέπουν πρόσβαση μόνο στις δυνατότητες και τις λειτουργίες που χρειάζονται για να εκτελούν τις εργασίες τους στην εταιρεία.
- Βεβαιωθείτε ότι μόνο οι χρήστες με τις απαραίτητες αρμοδιότητες μέσα στην εταιρεία μπορούν να εισάγουν αρχεία FOB, να σχεδιάζουν εκ νέου αντικείμενα καθώς και να δημιουργούν και να επαναφέρουν αντίγραφα ασφαλείας της βάσης δεδομένων.

- Δημιουργείτε συχνά αντίγραφα ασφαλείας της βάσης δεδομένων του Navision και να ελέγχετε τα αντίγραφα για να είστε σίγουροι ότι μπορείτε να τα επαναφέρετε επιτυχώς.
- Αποθηκεύετε τα αντίγραφα σε ασφαλές μέρος για να περιορίσετε την πιθανότητα καταστροφής από πυρκαγιά, καπνό, υψηλή θερμοκρασία, φωτισμό και περιβαλλοντικές καταστροφές (π.χ. κάποιο σεισμό).
- Παρόλο που η εκτέλεση του Navision είναι δυνατή σε διάφορες εκδόσεις των Windows, σας συνιστούμε να χρησιμοποιήσετε το νεότερο λειτουργικό σύστημα με τις πιο ενημερωμένες δυνατότητες ασφάλειας. Αυτή τη στιγμή αυτά είναι τα Windows XP, Service Pack 2 και Windows Server 2003.
- Χρησιμοποιήστε την υπηρεσία Windows Update που παρέχεται με τα Windows 2000, Windows XP και Windows Server 2003 για να εφαρμόσετε τις πιο πρόσφατες ενημερώσεις ασφαλείας. Χρησιμοποιείτε τη δυνατότητα αυτόματης ενημέρωσης των Windows για να διατηρείτε τους υπολογιστές-πελάτες ενημερωμένους με τις τελευταίες συμπληρώσεις κώδικα, τα τελευταία service pack και τις τελευταίες ενημερώσεις ασφαλείας.
- Σας συνιστούμε να χρησιμοποιείτε το πρωτόκολλο ασφαλείας TCPS για την επικοινωνία μεταξύ των υπολογιστών-πελατών με Navision και του Navision Database Server. Το TCPS είναι μια ασφαλής έκδοση του TCP/IP και χρησιμοποιεί τη διασύνδεση Security Support Provider Interface (SSPI) με ενεργοποίηση κρυπτογράφησης και έλεγχο ταυτότητας του Kerberos. Το TCPS είναι το προεπιλεγμένο πρωτόκολλο για το Navision Database Server.
- Ο πελάτης θα πρέπει να διαθέτει ένα σχέδιο επαναφοράς που να διασφαλίζει τη γρήγορη συνέχιση των υπηρεσιών σε περίπτωση καταστροφής. Ένα σχέδιο επαναφοράς θα πρέπει να περιλαμβάνει θέματα όπως:
  - την απόκτηση νέου/σύγχρονου εξοπλισμού.
  - την επαναφορά αντιγράφων ασφαλείας σε νέα συστήματα.
  - τον έλεγχο της σωστής λειτουργίας του σχεδίου επαναφοράς.

Ασφάλεια σε φυσικό επίπεδο

Η ασφάλεια σε φυσικό επίπεδο είναι επιτακτική καθώς η ασφάλεια σε λογισμικό επίπεδο δεν είναι δυνατόν να την αντικαταστήσει. Για παράδειγμα, αν κλαπεί κάποιος σκληρός δίσκος, ενδεχομένως να κλαπούν και τα δεδομένα που περιέχει. Συζητήστε τα ακόλουθα ζητήματα ασφαλείας σε φυσικό επίπεδο με τον πελάτη σας κατά την ανάπτυξη μιας πολιτικής:

- Σε περιπτώσεις μεγάλων εγκαταστάσεων με ανεξάρτητα τμήματα IT, βεβαιωθείτε ότι τα δωμάτια που βρίσκονται οι διακομιστές και οι χώροι αποθήκευσης του λογισμικού είναι κλειδωμένα.
- Τα μηχανήματα αυτής της κατηγορίας περιλαμβάνουν:
  - Το διακομιστή Microsoft SQL Server 2000
  - Το διακομιστή αρχείων όπου βρίσκονται εγκατεστημένα τα εκτελέσιμα αρχεία του Navision.
- Κρατάτε τους μη εξουσιοδοτημένους χρήστες μακριά από τους υπολογιστές.
- Εγκαταστήστε αντικλεπτικά συστήματα, ανεξάρτητα από την ευαισθησία των δεδομένων.
- Αποθηκεύετε τα αντίγραφα ασφαλείας μέσα σε ειδικά αλεξίπυρα κουτιά σε χωριστούς χώρους από όπου βρίσκονται τα συστήματα.

Οι εργαζόμενοι

Θα ήταν καλό να περιορίσετε τα δικαιώματα διαχείρισης που αφορούν όλα τα προϊόντα και τις δυνατότητες. Από προεπιλογή, οι πελάτες θα πρέπει να εκχωρούν στους υπαλλήλους τους μόνο δικαιώματα πρόσβασης για ανάγνωση σε λειτουργίες του συστήματος, εκτός και αν οι αρμοδιότητές τους απαιτούν περισσότερα δικαιώματα πρόσβασης. Η Microsoft σας συνιστά να ακολουθείτε την πολιτική του ελάχιστου δικαιώματος: εκχωρήστε στους χρήστες μόνο τα δικαιώματα που χρειάζονται για την πρόσβασή τους στα δεδομένα και τις λειτουργίες.

Οι δυσαρεστημένοι εργαζόμενοι καθώς και αυτοί που έχουν απολυθεί συνιστούν απειλή για την ασφάλεια του δικτύου. Στις συζητήσεις με του πελάτες σας για την ασφάλεια, προτείνετε την παρακάτω πολιτική σχετικά με τους εργαζόμενους:

- Διεξάγετε έρευνα για το παρελθόν των εργαζομένων προ της προσλήψεώς τους.
- Να είσαστε προετοιμασμένοι για ενδεχόμενη «εκδίκηση» από δυσαρεστημένους εργαζόμενους και από αυτούς που έχουν απολυθεί.
- Βεβαιωθείτε ότι ο εργαζόμενος μετά την απομάκρυνσή του απενεργοποιεί όλους τους σχετικούς λογαριασμούς Windows και κωδικούς πρόσβασης. Για λόγους αναφοράς, μην διαγράφετε τους χρήστες. Μην ξαναχρησιμοποιήσετε τους λογαριασμούς.
- Εκπαιδεύετε τους χρήστες ώστε να αντιλαμβάνονται και να αναφέρουν περιπτώσεις ύποπτης δραστηριότητας.
- Μην εκχωρείται δικαιώματα αυτόματα. Αν οι χρήστες δεν χρειάζονται πρόσβαση σε συγκεκριμένους υπολογιστές, δωμάτια υπολογιστών ή συνόλων αρχείων, βεβαιωθείτε ότι δεν έχουν πρόσβαση.
- Εκπαιδεύετε τους εποπτεύοντες ώστε να αναγνωρίζουν και να αντιμετωπίζουν πιθανά προβλήματα με εργαζόμενους.
- Βεβαιωθείτε ότι οι εργαζόμενοι κατανοούν το ρόλο τους στη διαδικασία διατήρησης της ασφάλειας δικτύου.
- Μοιράστε αντίγραφο των πολιτικών της εταιρείας σε κάθε εργαζόμενο.
- Μην επιτρέπεται στους χρήστες να εγκαθιστούν λογισμικό που δεν έχει εγκριθεί από τους εργοδότες τους.

Ο διαχειριστής

Συνιστούμε οι διαχειριστές συστημάτων των πελατών σας να μένουν ενημερωμένοι με τις τελευταίες ενημερώσεις κώδικα ασφαλείας που διατίθενται από την Microsoft. Οι εισβολείς είναι πολύ ικανοί να μετατρέπουν μικρά σφάλματα σε σοβαρές παραβιάσεις του δικτύου. Οl διαχειριστές θα πρέπει πρώτα να διασφαλίσουν τη μεγαλύτερη δυνατή ασφάλεια για κάθε υπολογιστή ξεχωριστά και στη συνέχεια να προσθέσουν ενημερώσεις ασφαλείας και να χρησιμοποιήσουν λογισμικό προστασίας από ιούς. Στον παρόντα οδηγό θα βρείτε πολλές συνδέσεις και πόρους που θα σας βοηθήσουν στην εύρεση σημαντικών πληροφοριών και των καλύτερων πρακτικών.

Η πολυπλοκότητα εμπεριέχει ακόμα μια αντιστάθμιση για την ασφάλεια του δικτύου σας. Όσο πιο πολύπλοκο είναι το σύστημα, τόσο πιο δύσκολο είναι να εξασφαλιστεί η ασφάλειά του ή η επιδιόρθωσή του σε περίπτωση που κάποιος εισβολέας επιτύχει πρόσβαση σε αυτό. Ο διαχειριστής πρέπει να μελετήσει διεξοδικά τη φυσική τοπολογία του δικτύου, με σκοπό να το καταστήσει όσο το δυνατόν πιο απλό.

Βασικό μέλημα της ασφάλειας είναι η διαχείριση του κινδύνου. Επειδή η τεχνολογία δεν είναι πανάκεια, για την ασφάλεια απαιτείται ένας συνδυασμός τεχνολογιών και πολιτικών. Με άλλα λόγια, δεν θα υπάρξει ποτέ ένα μόνο προϊόν που θα μπορείτε να εγκαταστήσετε στον υπολογιστή σας και το οποίο θα σας προσφέρει άμεσα την τέλεια ασφάλεια. Η ασφάλεια είναι αποτέλεσμα τεχνολογίας και πολιτικής: πώς δηλαδή χρησιμοποιείται η τεχνολογία ώστε τελικά να καθορίζεται το επίπεδο ασφάλειας ενός δικτύου. Η Microsoft παρέχει τεχνολογίες και δυνατότητες με κύριο μέλημα την ασφάλεια, αλλά μόνο ο διαχειριστής, με την δική σας καθοδήγηση, μπορεί να καθορίσει τις κατάλληλες πολιτικές για κάθε οργανισμό. Ο σχεδιασμός της ασφάλειας πρέπει να αποτελεί ένα από τα αρχικά βήματα στη διαδικασία της εφαρμογής και της ανάπτυξης του δικτύου σας. Μάθετε τι είναι αυτό που θέλει να προστατέψει ο πελάτης σας και τι μπορεί να κάνει για να το προστατέψει.

Τέλος, αναπτύξτε προληπτικά σχέδια για περιπτώσεις εκτάκτου ανάγκης. Συνδυάστε διεξοδικό σχεδιασμό και αξιόπιστη τεχνολογία για να προσφέρετε στον πελάτη σας την καλύτερη ασφάλεια.

Για περισσότερες πληροφορίες σχετικά με την ασφάλεια γενικά, ανατρέξτε στο άρθρο «The Ten Immutable Laws of Security Administration» (Οι δέκα αμετάτρεπτοι κανόνες για τη διαχείριση ασφάλειας), στη διεύθυνση:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

και τα άρθρα σχετικά με τη διαχείριση ασφάλειας στη διεύθυνση:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Ασφάλεια του λειτουργικού συστήματος διακομιστή

Παρόλο που θα διαπιστώσετε ότι πολλοί μικρότεροι πελάτες δεν διαθέτουν λειτουργικό σύστημα διακομιστή, είναι σημαντικό να μπορείτε να κατανοείτε και να χρησιμοποιείτε τις καλύτερες πρακτικές ασφάλειας σε μεγαλύτερους πελάτες που διαθέτουν πολυπλοκότερα περιβάλλοντα δικτύου. Θα πρέπει επίσης να γνωρίζετε ότι πολλές από τις πολιτικές και τις πρακτικές που περιγράφονται στο παρόν έγγραφο μπορούν εύκολα να εφαρμοστούν σε πελάτες που διαθέτουν μόνο λειτουργικά συστήματα υπολογιστή-πελάτη.

Οι έννοιες σε αυτήν την ενότητα εφαρμόζονται και στο Microsoft Windows 2000 Server και στο Microsoft Windows Server 2003, παρόλο που οι πληροφορίες έχουν εξαχθεί κυρίως από την ηλεκτρονική βοήθεια του Windows Server 2003. Το Windows Server 2003 προσφέρει ένα σύνολο αποτελεσματικών δυνατοτήτων ασφάλειας. Η ηλεκτρονική βοήθεια του Windows Server 2003 περιλαμβάνει πλήρεις πληροφορίες για όλες τις δυνατότητες και τις διαδικασίες ασφάλειας.

Για πρόσθετες πληροφορίες σχετικά με το Windows 2000 Server, μεταβείτε στο κέντρο ασφάλειας Windows 2000 Server Security Center, στη διεύθυνση:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

και διαβάστε τον οδηγό Windows 2000 Security Hardening Guide στη διεύθυνση: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Για πρόσθετες πληροφορίες σχετικά με το Windows 2003 Server, ανατρέξτε στον οδηγό ασφαλείας *Windows Server 2003 Security Guide*, στη διεύθυνση: http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

Οι βασικές δυνατότητες του μοντέλου ασφαλείας του διακομιστή Windows είναι ο έλεγχος ταυτότητας, ο έλεγχος πρόσβασης και η τεχνολογία μοναδικής εισόδου (Single Sign-On):

- Ο έλεγχος ταυτότητας είναι μια διαδικασία κατά την οποία το σύστημα πιστοποιεί την ταυτότητα ενός χρήστη μέσω των στοιχείων σύνδεσής τους. Το όνομα και ο κωδικός πρόσβασης ενός χρήστη συγκρίνονται βάσει μιας εγκεκριμένης λίστας. Όταν το σύστημα εντοπίζει συμφωνία στοιχείων, εκχωρεί στο χρήστη όσα δικαιώματα πρόσβασης καθορίζονται στη λίστα δικαιωμάτων για αυτόν το χρήστη.
- Ο έλεγχος πρόσβασης περιορίζει την πρόσβαση σε πληροφορίες ή σε υπολογιστικούς πόρους ανάλογα με την ταυτότητα του χρήστη και τη συμμετοχή του σε διάφορες προκαθορισμένες ομάδες. Η δυνατότητα αυτή χρησιμοποιείται συνήθως από τους διαχειριστές για τον έλεγχο της πρόσβασης των χρηστών σε πόρους του δικτύου, όπως τους διακομιστές, τους καταλόγους και τα αρχεία. Ο έλεγχος αυτός επιτυγχάνεται με την εκχώρηση δικαιωμάτων σε χρήστες και ομάδες για πρόσβαση σε συγκεκριμένα αντικείμενα.
- Η μοναδική είσοδος επιτρέπει σε έναν χρήστη να συνδεθεί σε έναν τομέα Windows μία φορά, χρησιμοποιώντας έναν μόνο κωδικό πρόσβασης, και ο έλεγχος ταυτότητας να είναι δυνατός σε κάθε υπολογιστή του τομέα Windows. Η μοναδική είσοδος επιτρέπει στους διαχειριστές να εφαρμόζουν την πιστοποίηση του κωδικού πρόσβασης σε όλο το δίκτυο Windows, διευκολύνοντας παράλληλα την πρόσβαση των χρηστών.

Οι ακόλουθες ενότητες περιγράφουν λεπτομερέστερα τις τρεις αυτές βασικές δυνατότητες.

Έλεγχος ταυτότητας

Ο έλεγχος ταυτότητας συνιστά θεμελιώδη πτυχή της ασφάλειας συστήματος και χρησιμοποιείται για την επιβεβαίωση της ταυτότητας οποιουδήποτε χρήστη προσπαθεί να συνδεθεί σε έναν τομέα ή επιχειρεί πρόσβαση σε πόρους δικτύου. Ο αδύναμος κρίκος στα περισσότερα συστήματα ελέγχου ταυτότητας είναι ο κωδικός πρόσβασης του χρήστη.

Οι κωδικοί πρόσβασης αποτελούν το πρώτο επίπεδο άμυνας κατά μη εξουσιοδοτημένης πρόσβασης σε τομέα και τοπικούς υπολογιστές. Προτείνετε τις ακόλουθες κορυφαίες πρακτικές σχετικά με τους κωδικούς πρόσβασης:

- Χρησιμοποιείτε πάντα δύσκολους κωδικούς πρόσβασης.
- Αν χρειαστεί να καταγράψετε τους κωδικούς σε κάποιο χαρτί, αποθηκεύστε το χαρτί σε ασφαλές μέρος και καταστρέψτε το όταν πλέον δεν το χρειάζεστε.
- Μην κάνετε κοινή χρήση των κωδικών με κανέναν.
- Χρησιμοποιείτε διαφορετικούς κωδικούς πρόσβασης για τους λογαριασμούς όλων των χρηστών.
- Αλλάζετε τους κωδικούς πρόσβασης σε τακτά χρονικά διαστήματα.
- Προσέχετε πού αποθηκεύετε τους κωδικούς πρόσβασης στον υπολογιστή.

Δύσκολοι κωδικοί πρόσβασης

Ο ρόλος των κωδικών πρόσβασης στην ασφάλεια του δικτύου ενός οργανισμού συχνά υποτιμάται και παραβλέπεται. Όπως ήδη προαναφέρθηκε, οι κωδικοί πρόσβασης αποτελούν το πρώτο επίπεδο άμυνας κατά μη εξουσιοδοτημένης πρόσβασης στο δίκτυο. Γι' αυτό το λόγο θα πρέπει να είστε βέβαιοι ότι οι πελάτες σας θα καθοδηγήσουν τους εργαζομένους τους, ώστε να χρησιμοποιούν δύσκολους κωδικούς.

Ωστόσο, τα εργαλεία διάσπασης των κωδικών πρόσβασης εξελίσσονται και οι υπολογιστές που χρησιμοποιούνται για τη διάσπαση των κωδικών είναι πιο ισχυροί από ποτέ. Το εργαλείο αυτόματης διάσπασης κωδικού μπορεί να διασπάσει οποιοδήποτε κωδικό πρόσβασης, έστω κι αν χρειαστεί αρκετός χρόνος. Ωστόσο, η διάσπαση δύσκολων κωδικών είναι πιο επίπονη από ό,τι η διάσπαση εύκολων κωδικών.

Για οδηγίες σχετικά με τη δημιουργία δύσκολων κωδικών που ο χρήστης μπορεί να θυμάται, μεταβείτε στις διευθύνσεις

http://www.microsoft.com/athome/security/privacy/password.mspx

και

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

Καθορισμός της πολιτικής κωδικών πρόσβασης

Κατά τον καθορισμό της πολιτικής κωδικών πρόσβασης με τον πελάτη σας, βεβαιωθείτε ότι η πολιτική που δημιουργείτε απαιτεί τη χρήση δύσκολων κωδικών από όλους τους χρήστες. Για τα περισσότερα συστήματα, αρκεί να ακολουθήσετε τις συστάσεις του οδηγού ασφάλειας Windows Server 2003 Security Guide:

- Ορίστε τη ρύθμιση πολιτικής **Επιβολή ιστορικού κωδικών πρόσβασης** ώστε να αποθηκεύονται στη μνήμη προηγούμενοι κωδικοί πρόσβασης. Με αυτή τη ρύθμιση πολιτικής, οι χρήστες δεν μπορούν να χρησιμοποιούν τον ίδιο κωδικό όταν αυτός λήξει.

  Συνιστώμενη ρύθμιση: 24

- Ορίστε τη ρύθμιση πολιτικής **Μέγιστη διάρκεια κωδικού πρόσβασης** ώστε οι κωδικοί να λήγουν όσο συχνά κρίνεται απαραίτητο για το περιβάλλον του χρήστη.

  Συνιστώμενη ρύθμιση: μεταξύ 42 (προεπιλογή) και 90.

- Ορίστε τη ρύθμιση πολιτικής **Ελάχιστη διάρκεια του κωδικού πρόσβασης** ώστε να μην είναι δυνατή η αλλαγή των κωδικών πριν παρέλθει συγκεκριμένος αριθμός ημερών. Αυτή η ρύθμιση πολιτικής δουλεύει σε συνδυασμό με τη ρύθμιση πολιτικής **Επιβολή ιστορικού κωδικών πρόσβασης**. Αν οριστεί ελάχιστη διάρκεια κωδικού πρόσβασης, οι χρήστες δεν μπορούν να αλλάζουν συνεχώς τους κωδικούς τους για να «παραπλανήσουν» τη ρύθμιση πολιτικής **Επιβολή ιστορικού** κωδικών πρόσβασης και στη συνέχεια να χρησιμοποιήσουν τους αρχικούς τους κωδικούς. Οι χρήστες θα πρέπει να περιμένουν τον καθορισμένο αριθμό ημερών για να αλλάξουν τους κωδικούς πρόσβασής τους.

  Συνιστώμενη ρύθμιση: 2.

- Ορίστε τη ρύθμιση πολιτικής **Ελάχιστο μήκος του κωδικού πρόσβασης** ώστε οι κωδικοί να αποτελούνται τουλάχιστον από τον καθορισμένο αριθμό χαρακτήρων. Οι μακροσκελείς κωδικοί, επτά ή περισσότεροι χαρακτήρες, είναι συνήθως πιο δύσκολοι από ό,τι οι μικρότεροι. Με αυτή τη ρύθμιση πολιτικής, οι χρήστες δεν μπορούν να χρησιμοποιήσουν κενούς κωδικούς αλλά πρέπει να δημιουργήσουν κωδικούς που να περιέχουν τουλάχιστον έναν χαρακτήρα.

  Συνιστώμενη ρύθμιση: 8.

- Ενεργοποιήστε τη ρύθμιση πολιτικής **Οι κωδικοί πρόσβασης πρέπει να πληρούν τις προϋποθέσεις πολυπλοκότητας**. Αυτή η ρύθμιση πολιτικής ελέγχει αν όλοι οι κωδικοί πρόσβασης πληρούν τις βασικές προϋποθέσεις ενός δύσκολου κωδικού. Αυτή ρύθμιση διασφαλίζει ότι οι κωδικοί έχουν τουλάχιστον τρία σύμβολα από τις τέσσερις κατηγορίες (κεφαλαία, πεζά, αριθμοί, μη αλφαριθμητικά σύμβολα) και δεν περιέχουν κανένα τμήμα από το όνομα χρήστη (για τη σύνδεση) και το ονοματεπώνυμο του χρήστη.

  Σημείωση
  Οι κωδικοί που πληρούν αυτές τις προϋποθέσεις δεν είναι απαραιτήτως και δύσκολοι. Για παράδειγμα, ο κωδικός «Κωδικός1» πληροί τις παραπάνω προϋποθέσεις.

  Συνιστώμενη ρύθμιση: Ναι

- Για πλήρη λίστα αυτών των προϋποθέσεων, ανατρέξτε στην ενότητα «Password Must Meet Complexity Requirements» (Οι κωδικοί πρόσβασης πρέπει να πληρούν τις προϋποθέσεις πολυπλοκότητας) στην ηλεκτρονική βοήθεια του Windows Server.

- Αποθηκεύετε τους κωδικούς πρόσβασης χρησιμοποιώντας την αμετάκλητη κρυπτογράφηση. Η αμετάκλητη κρυπτογράφηση χρησιμοποιείται σε συστήματα όπου μια εφαρμογή πρέπει να έχει πρόσβαση σε κωδικούς απλού κειμένου. Στις περισσότερες εγκαταστάσεις δεν είναι απαραίτητο.

  Συνιστώμενη ρύθμιση: Όχι.

Για περισσότερες πληροφορίες, ανατρέξτε στον οδηγό ασφάλειας Windows Server 2003 Security Guide:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

Καθορισμός μιας πολιτικής κλειδώματος λογαριασμού

Να είστε προσεκτικοί κατά τον καθορισμό της πολιτικής κλειδώματος λογαριασμού. Η πολιτική κλειδώματος λογαριασμού δεν πρέπει να εφαρμόζεται σε μικρές επιχειρήσεις γιατί υπάρχει ο κίνδυνος αποκλεισμού εξουσιοδοτημένων χρηστών, γεγονός που μπορεί να αποβεί δαπανηρό για τον πελάτη σας.

Αν ο πελάτης αποφασίσει να εφαρμόσει την πολιτική κλειδώματος λογαριασμού, ορίστε τη ρύθμιση **Account lockout threshold policy** σε ένα αρκετά υψηλό νούμερο ώστε να μην κλειδώνονται οι λογαριασμοί των εξουσιοδοτημένων χρηστών επειδή απλώς πληκτρολόγησαν λάθος τον κωδικό τους αρκετές φορές.

Για περισσότερες πληροφορίες σχετικά με την πολιτική κλειδώματος λογαριασμού, ανατρέξτε στην ενότητα «Account Lockout Policy Overview» (Προεπισκόπηση της πολιτικής κλειδώματος λογαριασμού) στην ηλεκτρονική βοήθεια του Windows Server.

Για πληροφορίες σχετικά με τον τρόπο εφαρμογής ή τροποποίησης της πολιτικής κλειδώματος πληκτρολογίου, ανατρέξτε στην ενότητα «To Apply or

Modify Account Lockout Policy» (Εφαρμογή ή τροποποίηση πολιτικής κλειδώματος πληκτρολογίου) στην ηλεκτρονική βοήθεια του Windows Server.

Έλεγχος πρόσβασης

Η ασφάλεια ενός δικτύου Windows και των πόρων του (συμπεριλαμβανομένου του Navision) διασφαλίζονται με τον καθορισμό των δικαιωμάτων που μπορούν να έχουν οι χρήστες, οι ομάδες χρηστών και οι άλλοι υπολογιστές στο δίκτυο. Μπορείτε να ασφαλίσετε έναν υπολογιστή ή πολλούς υπολογιστές εκχωρώντας στους χρήστες ή στις ομάδες συγκεκριμένα δικαιώματα. Μπορείτε να ασφαλίσετε ένα αντικείμενο, όπως ένα αρχείο ή ένα φάκελο, εκχωρώντας δικαιώματα που επιτρέπουν στους χρήστες ή στις ομάδες να εκτελούν συγκεκριμένες ενέργειες με αυτό το αντικείμενο. Στις βασικές έννοιες που συνιστούν τον έλεγχο πρόσβασης περιλαμβάνονται οι εξής:

- Δικαιώματα
- Κατοχή αντικειμένων
- Μεταβίβαση δικαιωμάτων
- Δικαιώματα χρήστη
- Έλεγχος αντικειμένων

Δικαιώματα

Τα δικαιώματα καθορίζουν τον τύπο της πρόσβασης που εκχωρείται σε έναν χρήστη ή μια ομάδα για ένα αντικείμενο ή την κατοχή ενός αντικειμένου, όπως τα αρχεία, οι φάκελοι και τα αντικείμενα μητρώου. Τα δικαιώματα εφαρμόζονται σε κάθε αντικείμενο που ασφαλίζεται, όπως τα αρχεία και τα αντικείμενα μητρώου. Τα δικαιώματα μπορούν να εκχωρηθούν σε οποιονδήποτε χρήστη, ομάδα ή υπολογιστή. Η εκχώρηση δικαιωμάτων σε ομάδες είναι προτιμότερη.

Κατοχή αντικειμένων

Αντιστοιχίζεται κάτοχος σε κάποιο αντικείμενο κατά τη δημιουργία αυτού του αντικειμένου. Από προεπιλογή στο 2000 Server, ο κάτοχος είναι και ο δημιουργός του αντικειμένου. Αυτό έχει αλλάξει στο Windows Server 2003 για τα αντικείμενα που δημιουργούνται από μέλη της ομάδας διαχειριστών.

Όταν ένα μέλος της ομάδας διαχειριστών δημιουργεί ένα αντικείμενο στο Windows Server 2003, η ομάδα διαχειριστών γίνεται ο κάτοχος και όχι ο προσωπικός λογαριασμός που δημιούργησε το αντικείμενο. Αυτή η συμπεριφορά μπορεί να αλλάξει μέσα από το συμπληρωματικό πρόγραμμα της κονσόλας διαχείρισης (MMC) των τοπικών ρυθμίσεων ασφάλειας της Microsoft, χρησιμοποιώντας τη ρύθμιση **Αντικείμενα συστήματος: Προεπιλεγμένος κάτοχος για αντικείμενα δημιουργούμενα από μέλη της ομάδας Administrators**. Ασχέτως με τα δικαιώματα που έχουν οριστεί για ένα αντικείμενο, ο κάτοχος του αντικειμένου μπορεί πάντα να αλλάζει τα δικαιώματα για αυτό.

Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα «Ownership» (Κατοχή) στην ηλεκτρονική βοήθεια του Windows Server.

Μεταβίβαση δικαιωμάτων

Η μεταβίβαση δίνει τη δυνατότητα στους διαχειριστές να εκχωρούν και να διαχειρίζονται εύκολα τα δικαιώματα. Αυτή η δυνατότητα μεταβιβάζει αυτόματα σε αντικείμενα μιας συλλογής όλα τα μεταβιβαζόμενα δικαιώματα αυτής της συλλογής. Για παράδειγμα, όταν δημιουργείτε αρχεία μέσα σε ένα φάκελο τότε μεταβιβάζονται σε αυτά τα δικαιώματα του φακέλου. Η μεταβίβαση είναι δυνατή μόνο για τα δικαιώματα με επισήμανση μεταβίβασης.

Δικαιώματα χρήστη

Τα δικαιώματα χρήστη αφορούν συγκεκριμένα δικαιώματα και δικαιώματα σύνδεσης με το υπολογιστικό σας περιβάλλον, που εκχωρούνται σε χρήστες και ομάδες.

Για πληροφορίες σχετικά με τα δικαιώματα χρήστη, ανατρέξτε στην ενότητα «User Rights» (Δικαιώματα χρήστη) στην ηλεκτρονική βοήθεια του Windows Server.

Έλεγχος αντικειμένων

Μπορείτε να ελέγχετε την πρόσβαση χρηστών σε αντικείμενα. Μπορείτε να προβάλλετε τα συμβάντα που σχετίζονται με την ασφάλεια από το αρχείο καταγραφής ασφαλείας, χρησιμοποιώντας την Προβολή συμβάντων.

Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα «Auditing» (Έλεγχος) στην ηλεκτρονική βοήθεια του Windows Server.

Κορυφαίες πρακτικές ελέγχου πρόσβασης

- Εκχωρείτε δικαιώματα κατά προτίμηση σε ομάδες και όχι σε χρήστες. Επειδή η διατήρηση λογαριασμών χρηστών απευθείας δεν είναι αποτελεσματική, η εκχώρηση δικαιωμάτων σε χρήστη θα πρέπει να γίνεται σε εξαιρετικές περιπτώσεις.
- Χρησιμοποιείτε δικαιώματα «Άρνηση» σε συγκεκριμένες ειδικές περιπτώσεις. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε δικαιώματα «Άρνηση» για να αποκλείσετε ένα υποσύνολο ομάδας που έχει δικαιώματα «Αποδοχή».
- Μην αρνείστε ποτέ το δικαίωμα πρόσβασης της ομάδας «Everyone» σε ένα αντικείμενο. Αν ορίσετε δικαίωμα «Άρνηση» στην ομάδα «Everyone» για ένα αντικείμενο, ο περιορισμός περιλαμβάνει επίσης και τους διαχειριστές (administrators). Προτιμότερο θα ήταν μα καταργήσετε την ομάδα «Everyone», εφόσον εκχωρείτε σε άλλους χρήστες, ομάδες ή υπολογιστές δικαιώματα σε αυτό το αντικείμενο. Έχετε υπόψη σας ότι αν δεν καθορίσετε δικαιώματα τότε δεν επιτρέπεται καμία πρόσβαση.
- Εκχωρήστε δικαιώματα σε ένα αντικείμενο που βρίσκεται σε όσο το δυνατόν υψηλότερο επίπεδο στη δομή δέντρου και στη συνέχεια εφαρμόστε μεταβίβαση για τη μετάδοση των ρυθμίσεων ασφαλείας σε όλη τη δομή δέντρου. Μπορείτε γρήγορα και αποτελεσματικά να εφαρμόσετε ρυθμίσεις ελέγχου πρόσβασης σε όλα τα εξαρτημένα στοιχεία ή σε μια δευτερεύουσα δομή δέντρου ενός γονικού στοιχείου. Με αυτήν την ενέργεια καλύπτετε ένα μεγάλο φάσμα εφαρμογής των ρυθμίσεων χωρίς να καταβάλλετε κόπο. Οι ρυθμίσεις δικαιωμάτων που ορίζετε πρέπει να είναι επαρκείς για την πλειοψηφία των χρηστών, των ομάδων και των υπολογιστών.
- Τα ρητά δικαιώματα πολλές φορές παρακάμπτουν τα μεταβιβαζόμενα δικαιώματα. Τα μεταβιβαζόμενα δικαιώματα «Άρνηση» δεν αποτρέπουν την πρόσβαση σε ένα αντικείμενο, αν για το αντικείμενο έχει καταχωριστεί ρητό δικαίωμα «Αποδοχή». Η εφαρμογή των ρητών δικαιωμάτων προηγείται της αντίστοιχης των μεταβιβαζόμενων δικαιωμάτων, ακόμα και των μεταβιβαζόμενων δικαιωμάτων «Άρνηση».

- Για δικαιώματα σε αντικείμενα Active Directory®, βεβαιωθείτε ότι έχετε κατανοήσει ποιες είναι οι καλύτερες πρακτικές ειδικά για τα αντικείμενα του καταλόγου Active Directory.

Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα «Best Practices for Assigning Permissions on Active Directory Objects» (Κορυφαίες πρακτικές για εκχώρηση δικαιωμάτων σε αντικείμενα Active Directory) στην ηλεκτρονική βοήθεια του Windows Server 2003.

Εξωτερικό τείχος προστασίας

Το τείχος προστασίας είναι ένα υλικό ή λογισμικό που εμποδίζει την είσοδο σε ή την έξοδο από συγκεκριμένο δίκτυο πακέτων δεδομένων. Για τον έλεγχο της ροής κυκλοφορίας, οι θύρες του τείχους ανοίγουν ή κλείνουν σε πακέτα πληροφοριών. Το τείχος προστασίας διερευνά διάφορα κομμάτια πληροφοριών μέσα σε κάθε πακέτο δεδομένων: το πρωτόκολλο παράδοσης του πακέτου, τον προορισμό ή τον αποστολέα του πακέτου, τον τύπο του περιεχομένου που περιλαμβάνει το πακέτο και τον αριθμό θύρας στην οποία αποστέλλεται. Αν το τείχος προστασίας έχει ρυθμιστεί ώστε να αποδέχεται το καθορισμένο πρωτόκολλο μέσω της θύρας προορισμού, τότε επιτρέπεται και η είσοδος του πακέτου. Η έκδοση Microsoft Windows Small Business Server 2003 Premium Edition παρέχεται με το Microsoft Internet Security and Acceleration (ISA) Server 2000 ως λύση τείχους προστασίας. Η έκδοση Small Business Server Standard Edition περιλαμβάνει επίσης ένα τείχος προστασίας.

ISA Server 2004

Ο διακομιστής Internet Security and Acceleration (ISA) Server 2000 δρομολογεί με ασφάλεια αιτήσεις και αποκρίσεις μεταξύ του Internet και των υπολογιστών-πελατών στο εσωτερικό δίκτυο.

Ο ISA Server λειτουργεί ως ασφαλή πύλη για το Internet για υπολογιστές-πελάτες στο τοπικό δίκτυο. Ο υπολογιστής ISA Server είναι ορατός στα άλλα μέρη της επικοινωνιακής αλυσίδας. Ο χρήστης Internet δεν πρέπει να αντιλαμβάνεται την παρουσία ενός διακομιστή τείχους προστασίας, εκτός κι αν επιχειρήσει πρόσβαση σε μια υπηρεσία ή μεταβεί σε μια τοποθεσία στην οποία ο υπολογιστής ISA Server αρνείται την πρόσβαση. Ο διακομιστής Internet στον οποίο πραγματοποιείται πρόσβαση προσλαμβάνει τις αιτήσεις του υπολογιστή ISA Server ως αιτήσεις που προέρχονται από μια εφαρμογή-πελάτη.

Όταν επιλέγετε φιλτράρισμα τμημάτων πρωτοκόλλου Internet Protocol (IP), ενεργοποιούνται οι υπηρεσίες Web Proxy και Firewall για το φιλτράρισμα κατακερματισμένων πακέτων. Φιλτράροντας κατακερματισμένα πακέτα, όλα τα κατακερματισμένα πακέτα IP απορρίπτονται. Μια συνηθισμένη «επίθεση» συνίσταται στην αποστολή κατακερματισμένων πακέτων και στη συνέχεια στην ανασυγκρότησή τους με τέτοιο τρόπο ώστε να βλάπτουν το σύστημα.

Ο ISA Server προσφέρει ένα μηχανισμό εντοπισμού παραβίασης, ο οποίος αναγνωρίζει την παραβίαση του δικτύου κατά τη στιγμή της απόπειρας και εκτελεί μια σειρά από ρυθμισμένες ενέργειες (ή προειδοποιήσεις) σε περίπτωση επίθεσης.

Αν έχουν εγκατασταθεί υπηρεσίες Internet Information Services (IIS) στον υπολογιστή ISA Server, πρέπει να τις ρυθμίσετε ώστε να μην χρησιμοποιούν τις θύρες που χρησιμοποιεί ο ISA Server για εξερχόμενες αιτήσεις Web (προεπιλογή, 8080) και για εισερχόμενες αιτήσεις Web (προεπιλογή, 80). Για παράδειγμα, μπορείτε να αλλάξετε τις υπηρεσίες IIS ώστε να εποπτεύουν τη θύρα 81 και στη συνέχεια να ρυθμίσετε τον υπολογιστή ISA Server ώστε να δρομολογεί τις εισερχόμενες αιτήσεις Web στη θύρα 81 του τοπικού υπολογιστή στον οποίο εκτελούνται οι υπηρεσίες IIS.

Αν υπάρχει κάποια διένεξη μεταξύ των θυρών που χρησιμοποιούν ο ISA Server και οι υπηρεσίες IIS, το πρόγραμμα εγκατάστασης διακόπτει την υπηρεσία δημοσίευσης IIS. Μπορείτε τότε να αλλάξετε τις υπηρεσίες IIS ώστε να εποπτεύουν μια διαφορετική θύρα και να επανεκκινήσετε την υπηρεσία δημοσίευσης IIS.

Πολιτικές διακομιστή ISA Server

Μπορείτε να ορίσετε μια πολιτική διακομιστή ISA Server η οποία να επιβάλλει κανόνες πρόσβασης σε εισερχόμενα και εξερχόμενα στοιχεία. Οι κανόνες τοποθεσιών και περιεχομένου θα καθορίζουν ποιες τοποθεσίες και ποιο είδος περιεχόμενου είναι προσπελάσιμα. Οι κανόνες πρωτοκόλλου υποδεικνύουν αν ένα συγκεκριμένο πρωτόκολλο είναι προσπελάσιμο για εισερχόμενη ή εξερχόμενη επικοινωνία.

Μπορείτε να δημιουργήσετε κανόνες τοποθεσιών και περιεχομένου, κανόνες πρωτοκόλλου, κανόνες δημοσίευσης στο Web και φίλτρα πακέτων IP. Αυτές οι πολιτικές καθορίζουν πώς οι πελάτες που διαθέτουν ISA Server θα διαδρούν με το Internet και ποιες επικοινωνίες θα επιτρέπονται.

Προστασία από ιούς

Ένας ιός υπολογιστή είναι ένα εκτελέσιμο αρχείο που σχεδιάζεται με στόχο την αυτόματη αναπαραγωγή του, τη διαγραφή ή την καταστροφή αρχείων και προγραμμάτων και την αποφυγή εντοπισμού του. Στην πραγματικότητα, οι ιοί συχνά δημιουργούνται εκ νέου και προσαρμόζονται ώστε να μην είναι δυνατός ο εντοπισμός τους. Οι ιοί συχνά αποστέλλονται ως συνημμένα ηλεκτρονικού ταχυδρομείου. Τα προγράμματα προστασίας από ιούς πρέπει να ενημερώνονται συνεχώς για να μπορούν να εντοπίζουν νέους και τροποποιημένους ιούς. Οι ιοί είναι ο κυριότερος αντιπρόσωπος του φαινομένου του υπολογιστικού βανδαλισμού.

Το λογισμικό προστασίας από ιούς σχεδιάζεται ειδικά για τον εντοπισμό και την αντιμετώπιση προγραμμάτων ιών. Επειδή δημιουργούνται συνεχώς νέα προγράμματα ιών, πολλοί κατασκευαστές προϊόντων προστασίας από ιούς προσφέρουν στους πελάτες τους, κατά τακτά χρονικά διαστήματα, ενημερώσεις για το λογισμικό τους. Η Microsoft εφιστά την προσοχή σας στην απαραίτητη εφαρμογή λογισμικού προστασίας από ιούς στο υπολογιστικό περιβάλλον του πελάτη σας.

Το λογισμικό ιών εγκαθιστάτε συνήθως σε κάθε ένα από τα ακόλουθα τρία σημεία: σταθμοί εργασίας χρήστη, διακομιστές και δίκτυο, όπου η ηλεκτρονική αλληλογραφία εισέρχεται (και σε μερικές περιπτώσεις εξέρχεται) στον οργανισμό.

Τύποι ιών

Υπάρχουν τρεις κύριοι τύποι ιών που προσβάλλουν συστήματα υπολογιστών: ιοί που προσβάλουν τομείς εκκίνησης, ιοί που μολύνουν αρχεία και προγράμματα Trojan horse.

Ιοί που προσβάλουν τομείς εκκίνησης

Ο υπολογιστής, κατά την έναρξη, σαρώνει τον τομέα εκκίνησης του σκληρού δίσκου πριν τη φόρτωση του λειτουργικού συστήματος ή άλλων αρχείων εκκίνησης. Ένας ιός που προσβάλει τον τομέα εκκίνησης στοχεύει στην αντικατάσταση των πληροφοριών των τομέων εκκίνησης του σκληρού δίσκου με το δικό του κώδικα. Όταν προσβάλλεται κάποιος υπολογιστής από έναν ιό τέτοιου τύπου, εκτελείται ανάγνωση του κώδικα του ιού πριν από ο,τιδήποτε άλλο. Αφού αποθηκευτεί ο ιός στη μνήμη, αναπαράγεται αυτόματα και στους άλλους δίσκους που χρησιμοποιούνται από τον μολυσμένο υπολογιστή.

Ιοί που μολύνουν αρχεία

Ο πιο συνηθισμένος τύπος ιού, ο ιός που μολύνει αρχεία, επισυνάπτεται αυτόματα σε ένα αρχείο εκτελέσιμου προγράμματος προσθέτοντας τον κώδικά του στον εκτελέσιμο κώδικα. Ο κώδικας ιού συνήθως προστίθεται με τέτοιο τρόπο ώστε να αποφεύγεται ο εντοπισμός του. Όταν εκτελείται το μολυσμένο αρχείο, ο ιός επισυνάπτεται αυτόματα σε άλλα εκτελέσιμα αρχεία. Η προέκταση των ονομάτων αρχείων που προσβάλλονται συνήθως από αυτόν τον τύπο ιού είναι .com, .exe ή .sys.

Μερικοί ιοί που μολύνουν αρχεία σχεδιάζονται για συγκεκριμένα προγράμματα. Οι τύποι προγραμμάτων που αποτελούν συνηθισμένο στόχο είναι τα αρχεία επικάλυψης (.ovl) και αρχεία βιβλιοθηκών δυναμικής σύνδεσης (.dll). Παρόλο που τα αρχεία αυτά δεν εκτελούνται, τα εκτελέσιμα αρχεία τα καλούν. Ο ιός μεταδίδεται κατά την πραγματοποίηση της κλήσης.

Τα δεδομένα καταστρέφονται όταν ο ιός ενεργοποιείται. Ένας ιός ενεργοποιείται όταν εκτελείται κάποιο μολυσμένο αρχείο ή όταν ικανοποιείται κάποια συγκεκριμένη ρύθμιση περιβάλλοντος (όπως με την έλευση μιας συγκεκριμένης ημερομηνίας συστήματος).

Προγράμματα Trojan horse

Ένα πρόγραμμα Trojan horse δεν είναι στην πραγματικότητα ιός. Η βασική διαφορά μεταξύ ενός ιού και ενός προγράμματος Trojan horse είναι ότι το τελευταίο δεν αναπαράγεται αυτόματα, αλλά καταστρέφει μόνο πληροφορίες στο σκληρό δίσκο. Το πρόγραμμα Trojan horse ξεγελά το σύστημα εμφανίζοντας τον εαυτό του ως αξιόπιστο πρόγραμμα, όπως ένα παιχνίδι ή ένα βοηθητικό πρόγραμμα. Όταν εκτελείται, όμως, καταστρέφει ή διαστρεβλώνει δεδομένα.

Κορυφαίες πρακτικές προστασίας από ιούς

Η εξάπλωση ενός ιού μακροεντολών είναι δυνατόν να αποφευχθεί. Ακολουθούν μερικές συμβουλές για την αποτροπή προσβολών που μπορείτε να προτείνετε στους πελάτες σας:

- Εγκαταστήστε μια λύση προστασίας από ιούς που ελέγχει τα εισερχόμενα μηνύματα από το Internet για ιούς πριν περάσουν από το δρομολογητή. Με αυτόν τον τρόπο διασφαλίζετε ο έλεγχος της ηλεκτρονικής αλληλογραφίας για γνωστούς ιούς.
- Αποδέχεστε έγγραφα μόνο όταν γνωρίζετε την πηγή προέλευσής τους. Μην ανοίγετε έγγραφα εκτός και αν προέρχονται από κάποιον που ο πελάτης θεωρεί αξιόπιστο.
- Μιλήστε με το άτομο που δημιούργησε το έγγραφο. Αν οι χρήστες δεν είναι απολύτως βέβαιοι για την ασφάλεια του εγγράφου, θα πρέπει να επικοινωνήσουν με το άτομο που δημιούργησε το έγγραφο.
- Χρησιμοποιείτε την προστασία από ιούς μακροεντολών του Microsoft Office. Στο Office, οι εφαρμογές προειδοποιούν το χρήστη στην περίπτωση που το έγγραφο περιέχει μακροεντολές. Αυτή η δυνατότητα επιτρέπει στο χρήστη να ενεργοποιήσει ή να απενεργοποιήσει τις μακροεντολές για το άνοιγμα του εγγράφου.
- Χρησιμοποιείτε λογισμικό ελέγχου για ιούς για τον εντοπισμό και τη διαγραφή ιών μακροεντολών. Το λογισμικό ελέγχου μακροεντολών μπορεί να εντοπίσει και συχνά να διαγράψει ιούς μακροεντολών από έγγραφα. Η Microsoft συνιστά τη χρήση λογισμικού προστασίας από ιούς που έχει πιστοποιηθεί από το διεθνή οργανισμό για την ασφάλεια των υπολογιστών International Computer Security Association (ICSA).

Για περισσότερες πληροφορίες σχετικά με τους ιούς και την ασφάλεια των υπολογιστών γενικότερα, μεταβείτε στις ακόλουθες τοποθεσίες για την ασφάλεια της Microsoft Security:

- Microsoft Security στη διεύθυνση http://www.microsoft.com/security/default.asp
- Τεκμηρίωση σχετικά με την ασφάλεια στο Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx

Στρατηγικές ασφάλειας δικτύου

Επειδή ο σχεδιασμός και η εγκατάσταση ενός διαδικτυακού περιβάλλοντος εργασίας IP απαιτεί ισορροπία μεταξύ ζητημάτων ιδιωτικού και δημόσιου δικτύου, τα τείχος προστασίας αποτελεί βασικό στοιχείο για την προστασία της ακεραιότητας του δικτύου. Ένα τείχος προστασίας δεν είναι ένα μεμονωμένο συστατικό στοιχείο. Ο οργανισμός National Computer Security Association (NCSA) ορίζει το τείχος προστασίας ως «ένα σύστημα ή συνδυασμό συστημάτων που επιβάλλουν ένα όριο μεταξύ δύο ή περισσότερων δικτύων.» Παρόλο που χρησιμοποιούνται διαφορετικοί όροι, αυτό το όριο είναι γνωστό και ως περίμετρος δικτύου. Η περίμετρος δικτύου προστατεύει το intranet το τοπικό δίκτυο (LAN) της επιχείρησής σας από εισβολές, ελέγχοντας την πρόσβαση από το Internet ή από άλλα μεγάλα δίκτυα.

Στο ακόλουθο σχεδιάγραμμα απεικονίζεται μια περίμετρος δικτύου συνδεδεμένη με τείχη προστασίας και τοποθετημένη μεταξύ ενός ιδιωτικού δικτύου και του Internet, ώστε να διασφαλιστεί η ασφάλεια του ιδιωτικού δικτύου:

Βασική περίμετρος δικτύου

Οι προσεγγίσεις κάθε οργανισμού σχετικά με τη χρήση τείχους προστασίας ως μέσο ασφάλειας ποικίλλουν. Το φιλτράρισμα πακέτων IP δεν παρέχει επαρκή ασφάλεια, η διαχείρισή του είναι δύσκολη και είναι πολύ εύκολο να «ξεγελαστεί». Οι πύλες εφαρμογών είναι πιο ασφαλείς από τα φίλτρα πακέτων και πιο εύκολα διαχειρίσιμες γιατί αφορούν μόνο λίγες συγκεκριμένες εφαρμογές, όπως ένα συγκεκριμένο σύστημα ηλεκτρονικής αλληλογραφίας. Οι πύλες κυκλωμάτων είναι πιο αποτελεσματικές όταν ο χρήστης μιας εφαρμογής δικτύου θεωρείται πιο σημαντικός από τα δεδομένα που περνάνε από αυτήν την εφαρμογή. Ο διακομιστής μεσολάβησης είναι ένα ολοκληρωμένο εργαλείο ασφάλειας που περιλαμβάνει μια πύλη εφαρμογής, ασφαλή πρόσβαση σε ανώνυμους χρήστες και άλλες υπηρεσίες. Ακολουθούν κάποιες πληροφορίες σχετικά με τις διάφορες επιλογές:

- **Φιλτράρισμα πακέτων IP**
  Το φιλτράρισμα πακέτων IP ήταν ο προπομπός εφαρμογής της τεχνολογίας τείχους προστασίας. Οι κεφαλίδες πακέτων εξετάζονται ως προς τις διευθύνσεις προέλευσης και προορισμού, το πρωτόκολλο TCP, τους αριθμούς θύρας του πρωτοκόλλου UDP και άλλες πληροφορίες. Το φιλτράρισμα πακέτων αποτελεί μια περιορισμένη τεχνολογία που δουλεύει καλύτερα σε ένα σαφώς ορισμένο περιβάλλον ασφάλειας όπου, για παράδειγμα, ο,τιδήποτε βρίσκεται έξω από την περίμετρο ασφαλείας δεν θεωρείται αξιόπιστο σε αντίθεση με ο,τιδήποτε βρίσκεται εντός. Τα τελευταία χρόνια, διάφοροι προμηθευτές έχουν βελτιώσει τις μεθόδους φιλτραρίσματος πακέτων, προσθέτοντας στον πυρήνα τους έξυπνες δυνατότητες για λήψη αποφάσεων. Με αυτό τον τρόπο, δημιουργήθηκε μια νέα μορφή φιλτραρίσματος πακέτων που ονομάζεται *stateful protocol inspection* (έλεγχος πρωτοκόλλου σε κάθε κατάσταση). Μπορείτε να ρυθμίσετε το φιλτράρισμα πακέτων έτσι ώστε είτε να γίνονται αποδεκτοί συγκεκριμένοι τύποι πακέτων ενώ όλοι οι υπόλοιποι θα απορρίπτονται είτε να απορρίπτονται συγκεκριμένοι τύποι πακέτων ενώ όλοι οι υπόλοιποι θα γίνονται αποδεκτοί.
- **Πύλες εφαρμογών**
  Οι πύλες εφαρμογών χρησιμοποιούνται όταν το περιεχόμενο μιας εφαρμογής έχει πολύ μεγάλη σημασία. Το πλεονέκτημα αλλά ταυτόχρονα και το μειονέκτημά τους είναι ότι αφορούν συγκεκριμένη εφαρμογή, καθώς πολύ δύσκολα προσαρμόζονται σε αλλαγές στην τεχνολογία.
- **Πύλες κυκλωμάτων**
  Οι πύλες κυκλωμάτων είναι σήραγγες ενσωματωμένες μέσα σε ένα τείχος προστασίας, οι οποίες συνδέουν συγκεκριμένες διαδικασίες ή συστήματα από τη μία πλευρά με συγκεκριμένες διαδικασίες ή συστήματα από την άλλη. Οι πύλες κυκλωμάτων θεωρούνται καταλληλότερες σε περιπτώσεις όπου το άτομο που χρησιμοποιεί την εφαρμογή αποτελεί μεγαλύτερο κίνδυνο από ό,τι οι πληροφορίες που περιέχονται στην εφαρμογή. Η διαφορά μεταξύ των πυλών κυκλωμάτων και ενός φίλτρου πακέτων συνίσταται στη δυνατότητα σύνδεσης με μια διάταξη εφαρμογής εκτός ζώνης που μπορεί να προσθέσει επιπλέον πληροφορίες.

- **Διακομιστές μεσολάβησης**
  Οι διακομιστές μεσολάβησης είναι ολοκληρωμένα εργαλεία ασφάλειας, που περιλαμβάνουν λειτουργίες τείχους προστασίας και πύλης εφαρμογών για τη διαχείριση της κυκλοφορίας Internet από και προς ένα τοπικό δίκτυο LAN. Οι διακομιστές μεσολαβήσεις προσφέρουν επίσης δυνατότητες αποθήκευσης σε προσωρινή μνήμη και ελέγχου πρόσβασης. Ένας διακομιστής μεσολάβησης μπορεί να βελτιώσει την απόδοση αποθηκεύοντας προσωρινά και παρέχοντας απευθείας δεδομένα που ανακαλούνται συχνά, όπως μια δημοφιλή σελίδα Web. Ένας διακομιστής μεσολάβησης μπορεί επίσης να φιλτράρει και να απορρίπτει αιτήσεις που ο κάτοχος δεν θεωρεί κατάλληλες, όπως είναι οι αιτήσεις για μη εξουσιοδοτημένη πρόσβαση σε αρχεία που του ανήκουν.

Διασφαλίστε ότι ο πελάτης θα εκμεταλλευτεί όλες τις δυνατότητες ασφαλείας του τείχους προστασίας που του χρειάζονται. Προβλέψτε μια περίμετρο δικτύου στην τοπολογία δικτύου στο σημείο όπου όλη η κυκλοφορία εκτός των ορίων του εταιρικού δικτύου πρέπει να διαπεράσει την περίμετρο που ορίζεται από το εξωτερικό τείχος προστασίας. Μπορείτε να ρυθμίσετε λεπτομερώς τον έλεγχο πρόσβασης για το τείχος προστασίας ανάλογα με τις ανάγκες του πελάτη σας καθώς και να ρυθμίσετε τις παραμέτρους του τείχους προστασίας ώστε να αναφέρονται όλες οι απόπειρες μη εξουσιοδοτημένης πρόσβασης.

Για να ελαχιστοποιήσετε τον αριθμό των θυρών που θα πρέπει να ανοίξουν στο εσωτερικό τείχος προστασίας, μπορείτε να χρησιμοποιήσετε ένα τείχος προστασίας σε επίπεδο εφαρμογής, όπως το ISA Server 2000.

Για περισσότερες πληροφορίες σχετικά με τα πρωτόκολλα TCP/IP, ανατρέξτε στο άρθρο «Designing a TCP/IP Network» (Σχεδιασμός δικτύου TCP/IP) στη διεύθυνση:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

Ασύρματα δίκτυα

Από προεπιλογή, τα ασύρματα δίκτυα τυπικά ρυθμίζονται έτσι ώστε να επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση στα ασύρματα σήματα. Είναι εκτεθειμένα σε κακόβουλα άτομα που μπορούν να πραγματοποιήσουν πρόσβαση λόγω της προεπιλεγμένης ρύθμισης σε ορισμένα ασύρματα τμήματα υλικού, της προσβασιμότητας που προσφέρουν τα ασύρματα δίκτυα και των μεθόδων κρυπτογράφησης που υπάρχουν. Υπάρχουν επιλογές ρύθμισης και εργαλεία που παρέχουν προστασία από μη εξουσιοδοτημένη πρόσβαση αλλά να θυμάστε ότι δεν μπορούν να προστατέψουν τους υπολογιστές σας από εισβολείς και ιούς που εισχωρούν μέσω της σύνδεσης Internet. Γι' αυτό το λόγο είναι απαραίτητο να συμπεριλάβετε ένα τείχος προστασίας για την ασφάλεια των υπολογιστών σας από ανεπιθύμητους εισβολείς του Internet.

Για περισσότερες πληροφορίες σχετικά με την προστασία ενός ασύρματου δικτύου, ανατρέξτε στο άρθρο «How to Make Your 802.11b Wireless Home Network More Secure» (Πώς να κάνετε πιο ασφαλές το ασύρματο οικιακό σας δίκτυο 802.11b) στη διεύθυνση: http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Σενάρια ασφάλειας δικτύου

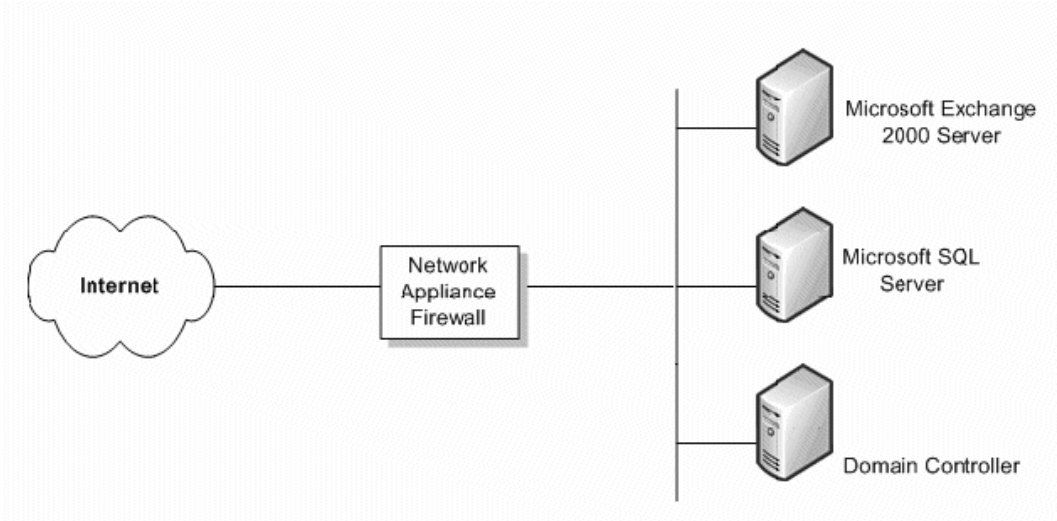
Το επίπεδο της ασφάλειας δικτύου, που απαιτεί ο οργανισμός του πελάτη σας, εξαρτάται από διάφορους παράγοντες. Συνήθως προκύπτει από κάποιο συμβιβασμό μεταξύ του προϋπολογισμού και της ανάγκης για ασφάλεια των εταιρικών δεδομένων. Μια μικρή επιχείρηση μπορεί να έχει μια πολύ περίπλοκη δομή ασφάλειας που να παρέχει το υψηλότερο δυνατό επίπεδο ασφάλειας, αλλά ενδέχεται αυτή η επιχείρηση να μην μπορεί να αντεπεξέλθει οικονομικά σε μια τέτοια προοπτική. Σε αυτήν την ενότητα, εξετάζουμε τέσσερα σενάρια, παρουσιάζοντας προτάσεις για το καθένα ώστε να παρέχονται διάφορα επίπεδα ασφάλειας.

Χωρίς τείχος προστασίας

Αν ο πελάτης σας έχει σύνδεση στο Internet αλλά δεν διαθέτει τείχος προστασίας, τότε θα πρέπει να εφαρμοστούν κάποια μέτρα προστασίας του δικτύου. Υπάρχουν κάποιες απλές συσκευές τείχους προστασίας για δίκτυο που προσφέρουν επαρκή ασφάλεια για την αντιμετώπιση των περισσότερων πιθανών εισβολέων.

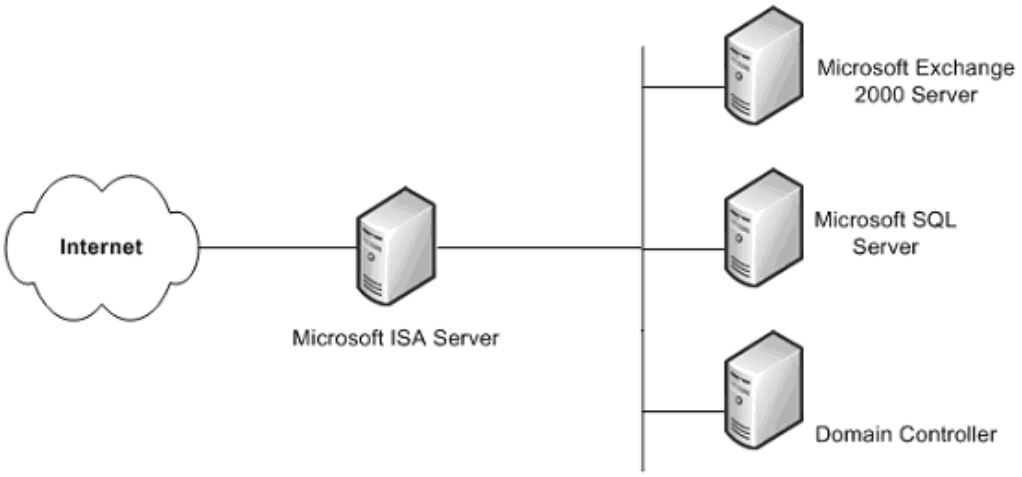
Ένα απλό τείχος προστασίας

Το ελάχιστο επίπεδο ασφάλεια που συστήνεται είναι ένα απλό τείχος προστασίας μεταξύ του Internet και των δεδομένων του πελάτη σας. Αυτό το τείχος προστασίας ενδέχεται να μην παρέχει όλα τα επίπεδα προηγμένης ασφάλειας και δεν θα πρέπει να θεωρείται επαρκής λύση. Είναι όμως καλύτερο από το να μην υπάρχει τίποτα.



Απλό τείχος προστασίας

Στις περισσότερες περιπτώσεις, ο προϋπολογισμός του πελάτη επιτρέπει την εφαρμογή μιας περισσότερο ασφαλούς λύσης που θα προστατεύει τα εταιρικά τους δεδομένα. Μια τέτοια λύση είναι ο διακομιστής ISA Server. Αυτός ο πρόσθετος διακομιστής έχει αυξημένο κόστος αλλά προσφέρει πολύ περισσότερη ασφάλεια από ό,τι το μέσο τείχος προστασίας που διαθέτετε, το οποίο παρέχει μόνο αντιστοίχιση διευθύνσεων δικτύου (NAT) και φιλτράρισμα πακέτων.



Τείχος προστασίας του ISA Server

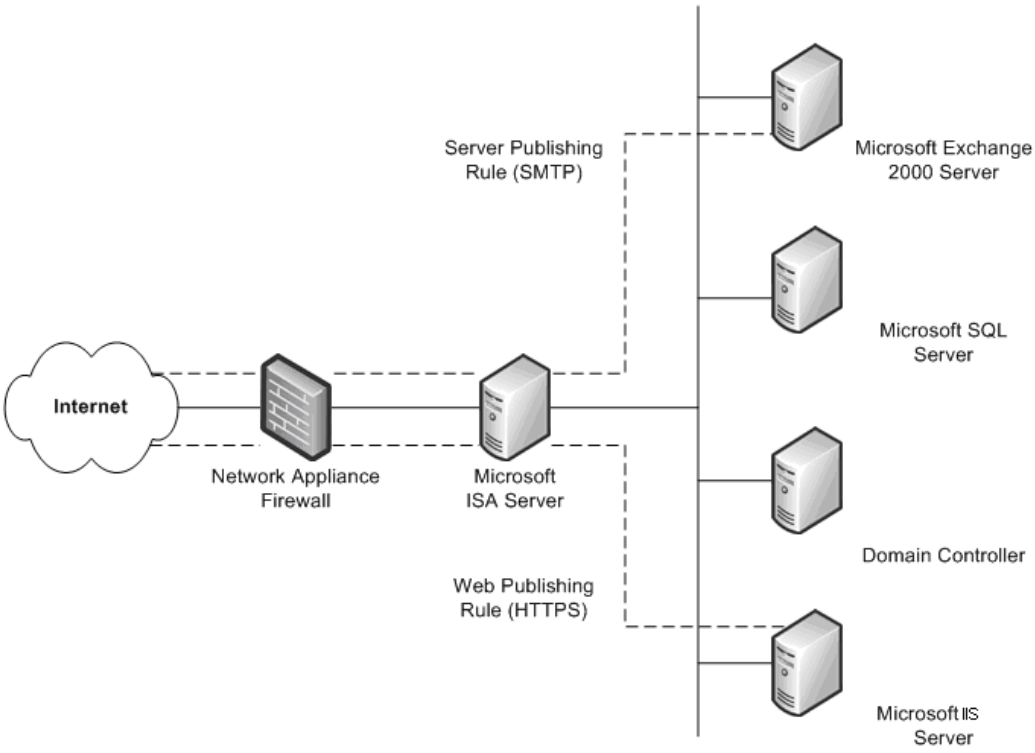
Η λύση του απλού τείχους προστασίας θεωρείται πιο ασφαλής από ό,τι η συσκευή τείχους προστασίας που εφαρμόζεται στο σημείο εισόδου, και παρέχει υπηρεσίες ασφαλείας ειδικά για Windows.

Ένα υπάρχον τείχος προστασίας

Αν ο πελάτης διαθέτει ένα τείχος προστασίας που διαχωρίζει το intranet από το Internet, μπορεί να χρειαστεί να προσθέσετε ένα επιπλέον τείχος προστασίας που να παρέχει διάφορους τρόπους διαμόρφωσης των εσωτερικών πόρων στο Internet.

Μια τέτοια μέθοδος είναι η δημοσίευση στο Web. Αυτό συμβαίνει κατά την εγκατάσταση ενός διακομιστή ISA Server μπροστά από το διακομιστή Web ενός οργανισμού που επιτρέπει την πρόσβαση των χρηστών στο Internet. Όταν εισέρχονται αιτήσεις Web, ο ISA Server εκπροσωπεί το διακομιστή Web προς τα έξω, ικανοποιώντας τις αιτήσεις πελατών για περιεχόμενο Web από την προσωρινή του μνήμη. Ο ISA Server προωθεί αιτήσεις στο διακομιστή Web μόνο όταν η προσωρινή του μνήμη δεν μπορεί να τις εξυπηρετήσει.

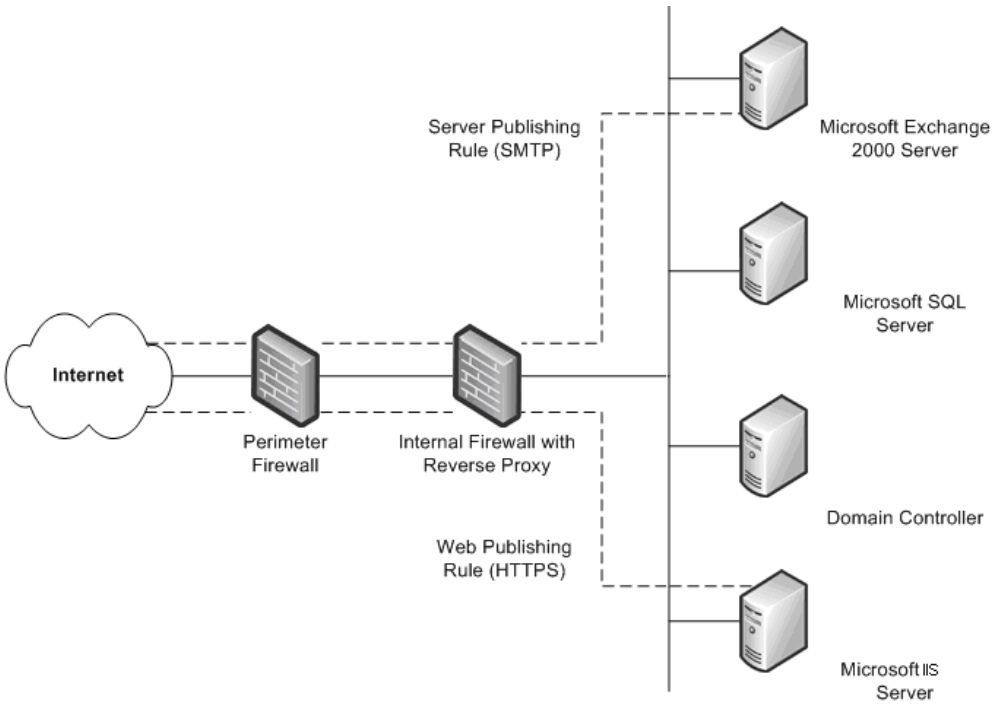
Μια άλλη μέθοδος είναι η δημοσίευση διακομιστή. Ο ISA Server επιτρέπει τη δημοσίευση εσωτερικών διακομιστών στο Internet χωρίς να θέτει σε κίνδυνο την ασφάλεια του εσωτερικού δικτύου. Μπορείτε να ρυθμίσετε κανόνες δημοσίευσης στο Web και δημοσίευσης διακομιστή που να καθορίζουν ποιες αιτήσεις θα αποστέλλονται στο διακομιστή του τοπικού δικτύου, παρέχοντας ένα αυξημένο επίπεδο ασφάλειας για τους εσωτερικούς διακομιστές.



Υπάρχον τείχος προστασίας με προσθήκη διακομιστή ISA Server

Δύο υπάρχοντα τείχη προστασίας

Το τέταρτο σενάριο αφορά την περίπτωση όπου ο οργανισμός έχει δύο τείχη προστασίας σε συνδυασμό με μια περίμετρο δικτύου (DMZ). Ένας ή περισσότεροι από αυτούς τους διακομιστές παρέχουν υπηρεσίες ανάστροφου διακομιστή μεσολάβησης ώστε οι πελάτες μέσω Internet να μην προσπελαύνουν απευθείας τους διακομιστές στο intranet. Αντ' αυτού, ένα από τα τείχη προστασίας (θα ήταν προτιμότερο να είναι το εσωτερικό τείχος προστασίας), διακόπτει τη ροή των αιτήσεων δικτύου προς τους εσωτερικούς διακομιστές, ελέγχει αυτά τα πακέτα και στη συνέχεια τα προωθεί εκ μέρους του κεντρικού υπολογιστή Internet.



Δύο υπάρχοντα τείχη προστασίας

Με την προσθήκη δεύτερου τείχους προστασίας, τότε αυτό το σενάριο παρουσιάζει ομοιότητες με το προηγούμενο. Η μόνη διαφορά είναι ότι το εσωτερικό τείχος προστασίας που υποστηρίζει ανάστροφο διακομιστή μεσολάβησης δεν είναι ένα ISA Server. Σε αυτό το σενάριο, θα πρέπει να συνεργαστείτε στενά με τους διαχειριστές κάθε τείχους προστασίας για τον καθορισμό των κανόνων δημοσίευση διακομιστή που θα συμπληρώνουν την πολιτική ασφάλειας.

Διαχείριση συμπληρώσεων κώδικα ασφαλείας

Τα λειτουργικά συστήματα και οι εφαρμογές είναι συχνά ιδιαίτερα πολύπλοκα. Μπορεί να αποτελούνται από εκατομμύρια γραμμές κώδικα που έχουν συνταχθεί από διαφορετικούς προγραμματιστές. Το λογισμικό πρέπει να λειτουργεί αξιόπιστα και να μην θέτει σε κίνδυνο την ασφάλεια ή τη σταθερότητα του περιβάλλοντος IT. Για την ελαχιστοποίηση ενδεχόμενων προβλημάτων, τα προγράμματα ελέγχονται διεξοδικά πριν την έκδοσή του. Ωστόσο, οι εισβολείς κάνουν τα πάντα διαρκώς για να εντοπίσουν αδυναμίες στο λογισμικό, με αποτέλεσμα η να μην είναι δυνατή η αντιμετώπιση μελλοντικών απειλών.

Σε πολλούς οργανισμούς, η διαχείριση συμπληρώσεων κώδικα αποτελεί ξεχωριστό κομμάτι της συνολικής στρατηγικής διαχείρισης των αλλαγών και της ρύθμισης παραμέτρων. Οποιαδήποτε και αν είναι η φύση ή το μέγεθος του οργανισμού, είναι απαραίτητη μια σωστή στρατηγική διαχείρισης συμπληρώσεων κώδικα, ακόμα και αν ο οργανισμός δεν διαθέτει, επί του παρόντος, αποτελεσματική διαχείριση αλλαγών και ρύθμισης παραμέτρων. Η πλειονότητα των επιτυχημένων επιθέσεων κατά υπολογιστών έχουν συμβεί σε συστήματα όπου δεν είχαν εγκατασταθεί τα συμπληρώματα κώδικα ασφαλείας.

Τα συμπληρώματα κώδικα ασφαλείας αποτελούν μια πρόκληση για τους περισσότερους οργανισμούς. Μόλις αποκαλυφθεί μια αδυναμία στο λογισμικό, οι εισβολείς διαδίδουν την πληροφορία σε ολόκληρη την κοινότητά τους. Όταν εμφανίζεται μια αδυναμία, η Microsoft προσπαθεί να εκδώσει όσο το δυνατόν γρηγορότερα μια συμπλήρωση κώδικα. Μέχρι να εγκαταστήσει ο πελάτης αυτήν τη συμπλήρωση, η ασφάλεια στην οποία βασίζεται και την οποία περιμένει ενδέχεται να είναι μικρότερη.

Στο περιβάλλον το Navision, θα πρέπει να διασφαλίσετε ότι οι πελάτες σας εγκαθιστούν τις πιο πρόσφατες συμπληρώσεις κώδικα ασφαλείας στο σύστημά τους. Βεβαιωθείτε ότι ο πελάτης χρησιμοποιεί μόνο τις τεχνολογίες που διαθέτει η Microsoft. Αυτές περιλαμβάνουν τα εξής:

- **Microsoft Security Notification Service**
  Η υπηρεσία ειδοποίησης ασφαλείας Security Notification Service είναι μια λίστα ηλεκτρονικού ταχυδρομείου η οποία διανέμεται κάθε φορά που υπάρχει διαθέσιμη μια ενημέρωση. Αυτές οι ειδοποιήσεις αποτελούν σημαντικό στοιχείο για μια προληπτική στρατηγική ασφαλείας. Διατίθενται επίσης και στην τοποθεσία TechNet Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx.

- **Αυτόματες ενημερώσεις της Microsoft**
  Τα Windows έχουν τη δυνατότητα να εγκαθιστούν αυτόματα ενημερώσεις ασφαλείας στους υπολογιστές σας.

- **Εργαλείο Microsoft Security Bulletin Search**
  Το εργαλείο αναζήτησης Security Bulletin είναι διαθέσιμο στην τοποθεσία Security Bulletin Service: http://www.microsoft.com/technet/security/current.aspx. Ο πελάτης μπορεί να καθορίσει ποιες ενημερώσεις χρειάζεται με βάση το λειτουργικό σύστημα, τις εφαρμογές και τα service pack που χρησιμοποιεί.

- **Microsoft Baseline Security Analyzer (MBSA)**
  Αυτό το εργαλείο γραφικών είναι διαθέσιμο στην τοποθεσία Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Αυτό το εργαλείο δουλεύει συγκρίνοντας την τρέχουσα κατάσταση ενός υπολογιστή με μια λίστα ενημερώσεων που ανήκει στη Microsoft. Το MBSA εκτελεί επίσης κάποιους βασικούς ελέγχους ασφαλείας για το βαθμό δυσκολίας των κωδικών πρόσβασης και τις ρυθμίσεις λήξης, τις πολιτικές λογαριασμών Guest και για πολλούς άλλους τομείς. Το MBSA αναζητά επίσης τρωτά σημεία στις υπηρεσίες Microsoft Internet Information Services (IIS), τον SQL Server™ 2000, το Exchange 5.5, το Exchange 2000 και τον Exchange Server 2003.

- **Microsoft Software Update Services (SUS)**
  Προηγουμένως ήταν γνωστό ως Windows Update Corporate Edition. Αυτό το εργαλείο επιτρέπει στις επιχειρήσεις να αποθηκεύουν σε τοπικούς υπολογιστές όλες τις κρίσιμες ενημερώσεις και τα πακέτα ασφαλείας SRP που υπάρχουν διαθέσιμα στην τοποθεσία Windows Update. Αυτό το εργαλείο δουλεύει με μια νέα έκδοση εφαρμογών-πελατών αυτόματης ενημέρωσης (AU) που σχηματίζουν τη βάση για μια ισχυρή στρατηγική αυτόματης λήψης και εγκατάστασης. Αυτό το νέο σύνολο εφαρμογών-πελατών AU περιλαμβάνει μια εφαρμογή για λειτουργικά συστήματα Windows 2000 και Windows Server 2003 και προσφέρει τη δυνατότητα αυτόματης εγκατάστασης ενημερώσεων που έχουν ληφθεί. Για περισσότερες πληροφορίες σχετικά με το Microsoft SUS, μεταβείτε στη διεύθυνση http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

- **Software Update Services Feature Pack του Microsoft Systems Management Server (SMS)**
  Το Software Update Services Feature Pack του SMS περιλαμβάνει μια πληθώρα εργαλείων που στόχο έχουν τη διευκόλυνση της διαδικασίας διανομής των ενημερώσεων λογισμικού σε όλη την επιχείρηση. Τα εργαλεία περιλαμβάνουν το Security Update Inventory Tool, το Microsoft Office Inventory Tool for Updates, το Distribute Software Updates Wizard και το SMS Web Reporting Tool with Web Reports Add-in for Software

Updates. Για περισσότερες πληροφορίες σχετικά με κάθε εργαλείο, μεταβείτε στη διεύθυνση http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Ενημερώστε τους πελάτες σας για τα παραπάνω εργαλεία και προτείνετέ τους τη χρήση τους. Είναι πολύ σημαντικό τα ζητήματα ασφάλειας να αντιμετωπίζονται το ταχύτερο δυνατό, ενώ διατηρείται η σταθερότητα του συστήματος.

Ρυθμίσεις ασφαλείας του SQL Server 2000

Επειδή η εκτέλεση του Navision είναι δυνατή και στον SQL Server 2000, είναι σημαντικό να λάβετε τα κατάλληλα μέτρα για την αύξηση της ασφάλειας της εγκατάστασης του SQL Server 2000 του πελάτη. Οι ακόλουθες οδηγίες μπορούν να αυξήσουν την ασφάλεια του SQL Server:

- Βεβαιωθείτε ότι τα τελευταία service pack και οι τελευταίες ενημερώσεις του λειτουργικού συστήματος και του SQL Server 2000 έχουν εγκατασταθεί. Για τις πιο πρόσφατες λεπτομέρειες, ελέγξτε τη τοποθεσία της Microsoft για την ασφάλεια:http://www.microsoft.com/security/default.asp
- Για ασφάλεια σε επίπεδο αρχείων, βεβαιωθείτε ότι τα αρχεία του SQL Server 2000 και τα αρχεία συστήματος έχουν εγκατασταθεί σε διαμερίσματα NTFS. Τα αρχεία πρέπει να είναι προσπελάσιμα μόνο στους διαχειριστές και σε χρήστες σε επίπεδο συστήματος μέσω δικαιωμάτων NTFS. Με αυτόν τον τρόπο διασφαλίζεται η προστασία από χρήστες που προσπελαύνουν αυτά τα αρχεία ενώ η υπηρεσία MSSQLSERVER δεν εκτελείται.
- Χρησιμοποιήστε έναν λογαριασμό τομέα χαμηλών δικαιωμάτων, όπως τον λογαριασμό NT Authority\Network Service ή τον LocalSystem (προτείνεται) για την υπηρεσία SQL Server 2000 (MSSQLSERVER). Αυτός ο λογαριασμός θα παρέχει τα ελάχιστα δικαιώματα στον τομέα και θα προφυλάσσει (αλλά δεν θα σταματά) το διακομιστή από μια επίθεση σε περίπτωση συμβιβασμού. Με άλλα λόγια, αυτός ο λογαριασμός θα παρέχει δικαιώματα χρήστη μόνο σε τοπικό επίπεδο στον τομέα. Αν ο SQL Server 2000 χρησιμοποιεί ένα λογαριασμό Domain Administrator για την εκτέλεση των υπηρεσιών, ένας συμβιβασμός του διακομιστή θα οδηγήσει σε συμβιβασμό ολόκληρου του τομέα. Για να αλλάξετε αυτή τη ρύθμιση, χρησιμοποιήστε τον SQL Server Enterprise Manager για να κάνετε την αλλαγή. Οι λίστες ελέγχου πρόσβασης (ACL) αρχείων, το μητρώο και τα δικαιώματα χρήστη θα αλλάξουν αυτόματα.
- Οι περισσότερες εκδόσεις του SQL Server 2000 εγκαθίστανται με δύο προεπιλεγμένες βάσεις δεδομένων, **Northwind** και **pubs**. Και οι δύο βάσεις δεδομένων αποτελούν δείγματα που χρησιμοποιούνται για τον έλεγχο, την εκπαίδευση και ως γενικά παραδείγματα. Δεν θα πρέπει να εγκατασταθούν μέσα σε ένα σύστημα παραγωγής. Αν γίνει γνωστό ότι αυτές οι βάσεις δεδομένων υπάρχουν, τότε ένας εισβολέας μπορεί να επιχειρήσει να εκμεταλλευτεί τις προεπιλεγμένες ρυθμίσεις και την προεπιλεγμένη διαμόρφωση παραμέτρων. Αν τα **Northwind** και **pubs** υπάρχουν στον υπολογιστή παραγωγής SQL Server 2000, θα πρέπει να αφαιρεθούν.
- Ο έλεγχος του συστήματος SQL Server 2000 είναι απενεργοποιημένος από προεπιλογή, συνεπώς καμία συνθήκη δεν ελέγχεται. Αυτό έχει ως αποτέλεσμα να μην είναι εύκολος ο εντοπισμός μιας παραβίασης και οι εισβολείς να καλύπτουν τα ίχνη τους. Το λιγότερο που μπορείτε να κάνετε είναι να ενεργοποιήσετε τον έλεγχο των αποτυχημένων συνδέσεων.

Για τις πιο ενημερωμένες πληροφορίες σχετικά με την ασφάλεια του SQL Server 2000, μεταβείτε στη διεύθυνση:
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

Πληροφορίες για το Microsoft Business Solutions

Το Microsoft Business Solutions, τμήμα της Microsoft, προσφέρει μια πληθώρα ολοκληρωμένων επιχειρησιακών εφαρμογών και υπηρεσιών που στόχο έχουν την υποστήριξη μικρών, μικρομεσαίων και εταιρικών επιχειρήσεων ώστε να ενισχυθούν οι τρόποι σύνδεσής τους με τους πελάτες, τους εργαζομένους, τους συνεργάτες και τους προμηθευτές τους. Οι εφαρμογές του Microsoft Business Solutions βελτιστοποιούν τις στρατηγικές επιχειρησιακές διαδικασίες στον τομέα της οικονομικής διαχείρισης, της ανάλυσης, της διαχείρισης ανθρώπινων πόρων, της διαχείρισης έργων, της διαχείρισης πελατειακών σχέσεων, της διαχείρισης υπηρεσιών πεδίου, της διαχείρισης της αλυσίδας παραγωγής, του ηλεκτρονικού εμπορίου, των κατασκευών και της διαχείρισης πωλήσεων λιανικής. Οι εφαρμογές έχουν σχεδιαστεί για να παρέχουν βαθιά γνώση ώστε να επιτυγχάνουν οι πελάτες στις επιχειρησιακές τους δραστηριότητες. Μπορείτε να βρείτε περισσότερες πληροφορίες σχετικά με το Microsoft Business Solutions στη διεύθυνση: http://www.microsoft.com/BusinessSolutions/