Microsoft Security Advisor

Εισαγωγή

Microsoft Security Advisor είναι ένα site όπου τοποθετεί η Microsoft τις ανακοινώσεις της σχετικά με θέματα ασφαλείας που αφορούν τα προϊόντα της καθώς και πληροφορίες για τα προϊόντα της εταιρίας και τα χαρακτηριστικά τους. Στο πρώτο μέρος της εργασίας παρουσιάζεται μία λίστα από προβλήματα που εμφανίστηκαν στα προϊοντα της Microsoft στον τομέα της ασφάλειας και συστήνονται τρόποι αντιμετώπισής τους. Στη συνέχεια γίνεται μία αναφορά στα ίδια τα προϊόντα της εταιρίας και των χαρακτηριστικών τους καθώς και στις τεχνολογίες που χρησιμοποεί, ενώ στο τελευταίο μέρος παρουσιάζονται όλα τα τελευταία νέα που αφορούν την Microsoft καθώς και άρθρα και αναφορές πάνω σε ζητήματα ασφαλείας.

1. Λίστα προβλημάτων

1.1 Εξουδετέρωση της δημιουργίας local groups στο domain από μη διαχειριστικοκούς χρήστες.

Τα Microsoft Windows NT επιτρέπουν στους μη διαχειριστικούς χρήστες να δημιουργήσουν domain local groups τα οποία ανήκουν μόνο στους Domain Controllers, που μοιράζονται εναν απλό security account manager (SAM). Η ικανότητα αυτή των μη διαχειριστικών χρηστών να δημιουργούν ψευδώνυμα στο domain θα μπορούσε να προκαλέσει προβλήματα αν αυτοί δημιουργήσουν ένα μεγάλο αριθμό local groups στο domain και να μεγαλώσει έτσι το μέγεθος της account database. Η δημιουργία αυτή απεριόριστων local groups θα μπορούσε καταστρέψει τον domain controller και να οδηγήσει σε υπερβολική κίνηση στο δίκτυο εξαιτίας των επαναλήψεων των πληροφοριών των local groups για να κάνουν backup στους domain controllers. Η εξ' ορισμού προστασία πρόσβασης που ελέγχει το domain των Windows NT επιτρέπει στους χρήστες να δημιουργούν local groups στον domain controller. Το δικαίωμα αυτό πρόσβασης πάνω στο domain είναι γνωστό σαν DOMAIN_CREATE_ALIAS.

Η ικανότητα των μη διαχειριστικών χρηστών να δημιουργούν local groups στον server είναι κατωχυρωμένο στα Windows NT Server Concepts and Planning manual. Αυτή η δυνατότητα επιτρέπει στους χρήστες καλύτερο έλεγχο στις πηγές που ανήκουν σε αυτούς. Για παράδειγμα, ένας χρήστης που θέλει να πετύχει πρόσβαση στα αρχεία που ανήκουν σε αυτόν και να τα αποθηκεύσει σε έναν server, φτιάχνει ένα local group στο domain και προσθέτει χρήστες σ' αυτό το group. Στη συνέχεια ο χρήστης δίνει το δικαίωμα πρόσβασης στα αρχεία του και τους καταλόγους του σε άλλους χρήστες με το να παρέχει πρόσβαση στο local group object, πράγμα το οποίο είναι πιο επιθυμητό από το να καθορίζει κανόνες πρόσβασης για κάθε χρήστη ξεχωριστά.

Η Microsoft έχει επίγνωση αυτού του χαρακτηριστικού και τις επιπλοκές που μπορεί να δημιουργηθούν από την υπερβολική χρήση αυτού του δικαιώματος από την πλευρά του χρήστη. Γι' αυτό και έχει δημιουργήσει ένα utility που αλλάζει αυτήν την συμπεριφορά και επιτρέπει τη δημιουργία των local groups μόνο στους διαχειριστικούς χρήστες. Αυτό το εργαλείο είναι διαθέσιμο δωρεάν στο site της Microsoft.

Αυτού του είδους τα προβλήματα έχουν παρουσιαστεί στα Windows NT Server 3.1, 3.5, 3.51 και 4.0.

1.2 Διαθέσιμο update σχετικά με το "Error Message Vulnerability" σχετικά με τους Secured Internet Servers.

Η RSA Data Security Inc. ενημέρωσε την Microsoft Product Security Response Team την ύπαρξη ενός τρωτού σημείου που επηρρεάζει τις εκδόσεις του Secure Socket Layer (SSL) Protocol. Ο Daniel Bleichenbacher ένας ερευνητής που εργάζεται στα Bell Labs έκανε αυτήν την ανακάλυψη. Χρησιμοποιώντας πολύπλοκα μαθηματικά και την εμπειρική μέθοδο ο Daniel Bleichenbacher ανακάλυψε ότι μία κρυπτογραφαφημένη με SSL συναλλαγή θα μπορούσε να αποκρυπτογραφηθεί.Το πρόβλημα αφορά μόνο το Internet Server Software και όχι το software του χρήστη όπως ο Microsoft Internet Explorer.

Για να εκμεταλλευτεί το τρωτό σημείο κάποιος θα πρέπει πρώτα να μπορέσει να παρατηρήσει αυτήν την κρυπτογραφημμένη συναλλαγή μεταξύ του χρήστη και του Web server. Μόλις καταγράψει αυτήν την συναλλαγή ο επιτιθέμενος θα πρέπει να στείλει ένα μεγάλο αριθμό από καλά δομημένα μηνύματα στον Web server και να αναλύσει τις αντιδράσεις του. Αφού στείλει περίπου ένα εκατομμύριο μηνύματα θα είναι σε θέση να αποκρυπτογραφήσει την πληροφορία που περιέχεται στην κρυπτογραφημένη συναλλαγή που έχει καταγράψει. Η επιτυχία αυτή του επιτεθέμενου δεν του δίνει το πλεονέκτημα να αποκρυπτογραφεί και τις άλλες συναλλαγές που κάνει ο server ή τις συναλλαγές που γίνονται από τον χρήστη. Εξαιτίας του μεγάλου αριθμού των μηνυμάτων ένας Web server operator θα μπορεί να ανιχνεύσει την επίθεση μέσα από τη παρατήρηση ανώμαλης συμπεριφοράς στο δίκτυο ή στη χρήση της CPU.

Η Microsoft Product Security Response Team δημιούργησε ένα update πρόγραμμα που λύνει το πρόβλημα που εμφανίζεται στο εξής Internet server software:

- Microsoft Windows NT Server's Internet Information Server 3.0 και 4.0
- Microsoft Site 3.0 Commerce Edition
- Microsoft Site Server, Enteprise Edition
- Microsoft Exchange 5.0 και 5.5 (for SSl-enabled POP3 και SMTP)

Το Microsoft Internet server λογισμικό παρέχει SSL 2.0, SSL 3.0, PCT 1.0 και TLS 1.0 για την ασφάλεια των Internet-based επικοινωνιών. Τα πρωτόκολα αυτά εκτελούνται μέσα από ένα αρχείο το SCHANNEL.ddl. Κάνοντας update αυτό το αρχείο θα λυθεί το πρόβλημα στο παραπάνω λογισμικό. Μόνο οι χρήστες που χρημοποιούν το SSL θα πρέπει να κάνουν

αυτήν την αναβάθμιση. Το πρόβλημα παρουσιάζεται και στις εκδόσεις των 40 bit και στις εκδόσεις τωβ 128 bit του SSL.

1.3 Πρόσβαση αρχείου με τα Windows NT Internet Information Server (IIS).

Πρόσφατα ο Paul Aston δημοσίευσε ένα άρθρο για το NTBugtraq mailing list που επηρρεάζει τα Microsoft Windows NT Server's Internet Information Server (IIS). Οι χρήστες μπορούν να διαβάσουν τα περιεχόμενα κάθε Window Server's NT File System (NTFS) αρχείου μέσα από ένα IIS όπου έχει δοθεί το δικαίωμα πρόσβασης. Αυτοί μπορούν να διαβάσουν τα αρχεία ακόμα και όταν αυτά σηματοδοτούνται για " applications mappings".

Το NTFS επιτρέπει πολλαπλά είδη δεδομένων μέσα σε ένα αρχείο. Τα δεδομένα στα οποία αποθηκεύονται τα περιεχόμενα του αρχείου έχουν ένα χαρακτηριστικό που ονομάζεται $DATA. Έχοντας κάποιος πρόσβαση σ' αυτά τα NTFS δεδομένα μέσω ενός IIS browser μπορεί να δει και τα περιεχόμενα του αρχείου που είναι μόνο για Application Mapping.

Για παράδειγμα τα asp αρχεία σηματοδοτούνται έτσι ώστε να εκτελούνται από έναν ASP page scripting agent παρά να συμπεριφέρονται σαν να ήταν htm αρχεία. Κανονικά τα περιεχόμενα αυτών των αρχείων δε θα έπρεπε να επιστρέφονται στον χρήστη. Παρόλα αυτά όταν κάποιος χρήστης ζητήσει ένα αρχείο τότε ο Web browser μπορεί να επιστρέψει και τα περιεχόμενα του script file, και σε πολλές περιπτώσεις το αρχείο αυτό μπορεί να περιέχει σημαντικές πληροφορίες όπως κωδικούς ή άλλες "ευαίσθητες" πληροφορίες της επιχείρησης.

Το πρόβλημα αυτό έχει εμφανιστεί στο εξής λογισμικό :

- Microsoft Windows NT Server's Internet Information Server 1.0, 2.0, 3,0 και 4.0
- Microsoft Peer Web Server 2.0, 3.0
- Microsoft Personal Web Server 4.0 για Windows NT 4.0 Workstation

Η Microsoft Product Security Response Team έχει δημιουργήσει ένα hot fix για τις εκδόσεις 3.0 και 4.0 του Microsoft Internet Information Server.

1.4 Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα με RDS και IIS

Remote Data Service (RDS) είναι στοιχείο του Microsoft Data Access Components (MDAC) το οποίο εγκαθίσταται εξ΄ορισμού όταν τα Windows NT Server's Internet Information Service (IIS) 4.0 εγκαθίσταται μέσω του Microsoft Windows NT Option Pack. Ο σκοπός του RDS είναι να κάνει δυνατή την ελεγχόμενη πρόσβαση σε απομακρυσμένες πηγές δεδομένων μέσω των Windows NT's IIS. Όμως, επειδή το RDS DataFactory (το οποίο είναι ένα στοιχείο του RDS) επιτρέπει την εξ΄ορισμού πρόσβαση σε απομακρυσμένα δεδομένα μπορεί να επιτρέψει και σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε OLE database που είναι διαθέσιμες στον server. Αυτή η

λειτουργία του RDS 1.5 μέσω του DataFactory θα πρέπει να εξουδετερωθεί. Ένας χρήστης που συνδέεται με έναν Windows NT IIS server μπορεί να χρησιμοποιήσει την λειτουργία του RDS έτσι ώστε να κατευθύνει τον εξυπηρέτη για να πάρει τα δεδομένα χρησιμοποιώντας έναν OLE DB provider.

Για παράδειγμα ένας χρήστης μπορεί να εκπέμψει μία SQL command με το όνομα ή την IP διεύθυνση από ένα απομακρυσμένο SQL Server σύστημα, ένα SQL account και τον κωδικό, το όνομα της βασης δεδομένων και μία SQL ερώτηση. Αν η αίτηση είναι έγκυρη τότε τα αποτελέσματα της ερώτησης θα επιστραφούν στον χρήστη μέσω του HTTP. Αν και κάτι τέτοιο απαιτεί τη γνώση σημαντικών εσωτερικών πληροφοριών δε θα πρέπει να υποτιμηθεί αυτή η δυνατότητα πρόσβασης στις πληροφορίες. Οι επιχειρήσεις που δεν εφαρμόζουν καλές υπολογιστικές τακτικές έχουν εύκαλα μαντέψιμους κωδικούς στους SQL administrator accounts. Η λειτουργία του RDS DataFactory με τους άλλους εγκατεστημένους ODBC drivers δημιουργεί και άλλες δυνατότητες όπως πρόσβαση σε μη δημοσιοποιημένα αρχεία.

Ο κίνδυνος που προκαλείται από το DataFactory γίνεται μεγαλύτερος όταν καινούργιοι OLE DB Providers εγκαθίστανται στον server. Οι Microsoft DataShape Provider και Microsoft JET OLE DB Provider επιτρέπουν να εκτελεστούν shell commands. Έτσι οι χρήστες μπορούν να χρησιμοποιήσουν τέτοιους providers για να εκτελέσουν shell commands και να "κρεμάσουν" τον εξυπηρέτη ή να προκαλέσουν προβλήματα στην απόδοσή του. Γι΄αυτό και η Microsoft έχει δημιουργήσει ένα πρόγραμμα έτσι ώστε να βοηθήσει τους πελάτες της να εξουδετερώσουν την λειτουργία αυτή του RDS.

Το λογισμικό που έχει επηρρεαστεί είναι το εξής :

- Microsoft Windows NT Server's Internet Information Server 4.0
- Microsoft Remote Data Services 1.5
- Microsoft Visual Studio 6.0

1.5 Ανεπιθύμητα δεδομένα στο Office 98 για Macintosh

Πρόφατα η Microsoft διαπίστωσε ότι υπάρχει πρόβλημα στον τρόπο που αποθηκεύονται τα αρχεία στους σκληρούς δίσκους στο Microsoft Office 98 για Macintosh. Όταν το Office 98 για Macintosh δημιουργεί ένα αρχείο στον σκληρό δίσκο για αποθήκευση, είναι πιθανό ένας μικρός αριθμός από τυχαία δεδομένα που υπάρχουν από ένα προηγούμενο διαγραμμένο αρχείο να συνεχίζουν να βρίσκονται στο Office 98.

Αν και η πιθανότητα να αποκαλυφτούν σημαντικές πληροφορίες είναι μηδαμινή, αν αυτό το αρχείο σταλθεί σε έναν άλλο χρήστη υπάρχει κίνδυνος να ξεσκεπαστούν δεδομένα από ένα προηγούμενο αρχείο που έχει διαγραφεί.

Το πρόβλημα δημιουργήται από τον τρόπο που το Office 98 κατανέμει το χώρο στον σκληρό δίσκο για αποθήκευση. Το Mac λειτουργικό σύστημα, όπως και άλλα λειτουργικά συστήματα δεν διαγράφει εντελώς τα αρχεία αλλά απλά αφαιρεί από τον κατάλογο του δίσκου την αναφορά των αρχείων αυτών και σημαδεύει το χώρο που καταλάμβαναν σαν ελεύθερο. Το Office 98 δεν καθαρίζει το χώρο του δίσκου που το Mac λειτουργικό σύστημα διαθέτει το

χώρο αυτό για να σώσει ένα αρχείο. Αντίθετα το Office 98 γράφει τα περιεχόμενα ενός αρχείου στον διαθέσιμο χώρο του σκληρού δίσκου πάνω από οτιδήποτε δεδομένα είναι δυνατόν να υπάρχουν στον χώρο αυτό. Επειδή το Mac λειτουργικό σύστημα κατανέμει το χώρο του δίσκου σε clusters, υπάρχει περίπτωση ο αχρησιμοποίητος χώρος του τελευταίου cluster που περιέχει το τέλος ενός αρχείου να έχει δεδομένα από ένα προηγούμενο αρχείο που έχει διαγραφεί. Τα δεδομένα αυτά δεν μπορούν να γίνουν ορατά όταν ανοίγεις το αρχείο αλλά αν χρησιμοποιηθεί ένας ASCII text editor μπορείς να δεις τα ξένα δεδομένα.

Η Microsoft έχει δημιουργήσει ένα update για το Office 98 για Macintosh που εξαλείφει ολοκληρωτικά το πρόβλημα. Το update αυτό είναι διαθέσιμο δωρεάν στο site της Microsoft.

1.6 Πιθανή άρνηση των υπηρεσιών του IIS FTP Server που οφείλεται σε παθητικές συνδέσεις.

Η Microsoft είναι ενήμερη του πρόβλήματος που παρουσιάστηκε στον τρόπο που τα Microsoft Windows Server's Internet Information Server (IIS) επεξεργάζονται τις παθητικές FTP σύνδεσης αιτήσεις. Σε ορισμένες περιπτώσεις όπου χρησιμοποιούνται παθητικές FTP συνδέσεις εμφανίζονται λάθη, προβλήματα στην απόδοση του συστήματος καθώς και άρνηση για FTP και WWW υπηρεσίες που τρέχουν στον ίδιο υπολογιστή. Το πρόβλημα αφορά την άρνηση των υπηρεσιών και όχι την καταστροφή του FTP server. Όταν πολλαπλές παθητικές συνδέσεις γίνονται σ΄ένα FTP server μέσω του PASV FTP command είναι πιθανό να χρησιμοποιηθούν όλες οι γραμμές του συστήματος για την εξυπηρέτηση των πελατών. Μόλις αυτό συμβεί τότε οι αιτήσεις για πρόσθετες συνδέσεις θα απορρίπτονται μέχρι κάποια γραμμή να είναι διαθέσιμη και πάλι. Οι FTP και WWW υπηρεσίες σε έναν υπολογιστή μοιράζονται ένα κοινό σύνολο γραμμών και όταν υπερφορτωθούν θα προκαλέσουν απόρριψη στις αιτήσεις σύνδεσης για WWW υπηρεσίες.

Το λογισμικό που επηρρεάζεται από αυτό το πρόβλημα είναι τα Microsoft Windows NT Server's IIS 2.0, 3.0 και 4.0, γι' αυτό και η Microsoft έχει διαθέσει στην αγορά ένα update για το παραπάνω software.

1.7 Πιθανή SMTP και NNTP άρνηση υπηρεσιών του Microsoft Exchange Server

Η Microsoft πρόσφατα ενημερώθηκε από την Internet Security Systems Inc.'s X-Force team σχετικά με ένα πρόβλημα που παρουσιάστηκε στον τρόπο που ο Microsoft Exchange Server 5.5 και 6.0 επεξεργάζεται τις SMTP και NNTP εντολές. Κάποιος χρήστης μπορεί να ακμεταλλευτεί το τρωτό αυτό σημείο και κάνει ορισμένες συγκεκριμένες υπηρεσίες να σταματήσουν να ανταποκρίνονται. Το πρόβλημα αυτό δεν επηρρεάζει τον Microsoft Exchange Server 4. Συγκεκριμένα :

Για το SMTP πρωτόκολο:

Αν κάποιος χρήστης συνδεθεί με τον Microsoft Exchange Server που τρέχει TCP/IP port 25 και εκπέμψει μία σειρά από ανακριβή δεδομένα τότε ένα λάθος εφαρμογής προκαλεί την Internet Mail υπηρεσία να σταματά να ανταποκρίνεται. Αυτό δεν επηρρεάζει και τις άλλες Exchange υπηρεσίες.

Για το NNTP πρωτόκολο:

Αν κάποιος χρήστης συνδεθεί με έναν Microsoft Exchange Server που τρέχει το πρωτόκολο NNTP και εισάγει μία σειρά από εσφαλμένα δεδομένα τότε ένα λάθος εφαρμογής είναι δυνατόν να κάνει τον Server Information Store να σταματήσει να ανταποκρίνεται με αποτέλεσμα να μην λειτουργούν και οι άλλες Exchancge υπηρεσίες, ενώ ο χρήστης να μην μπορεί να συνδεθεί με τους καταλόγους ή το mail του.

Όταν συμβεί κάτι τέτοιο τότε θα πρέπει οι υπηρεσίες που έχουν προσβληθεί να εγκατασταθούν ξανά και δε χρειάζεται να κάνεις reboot το λειτουργικό σύστημα.

1.8 Update για αρχεία με μεγάλο ονόμα που επηρρεάζουν το Microsoft Outlook 98 και το Microsoft Outlook Express 4.x

Η Microsoft πρόσφατα ενημερώθηκε για ένα πρόβλημα που επηρρεάζει τον τρόπο που οι χρήστες που χρησιμοποιούν την email υπηρεσία χειρίζονται τις συνδέσεις αρχείων που έχουν μεγάλα ονοματα.

Στις 27 Ιουλίου η Microsoft διέθεσε προγράμματα για το Outlook 98 και το Outlook Express 4.x που διόρθωνε το πρόβλημα που παρουσιάστηκε. Η Microsoft συνιστά σε όλους τους χρήστες της να κατεβασουν τα κατάλληλα προγράματα από το site της εταιρίας. Όταν ένας χρήστης λάβει ένα mail ή μηνυματα που περιέχουν σύνδεση με ένα αρχείο μεγάλου ονόματος τότε υπάρχει περίπτωση το αρχείο αυτό να κλείσει το email του χρήστη απροειδοποίητα. Για παράδειγμα ένας hacker μπορεί να χρησιμοποιήσει το email μήνυμα για να τρέξει αυθαίρετο κώδικα που περιέχεται στο long string.

Το λογισμικό στο οποίο εμφανίζεται το πρόβλημα είναι:

- Outlook 98 για Windows 95, Windows 98 και Microsoft Windows NT 4.0
- Outlook Express 4.0, 4.01 (συμπεριλαβάνεται η έκδοση 4.01 με Service Pack 1) για Windows 95, Windows 98 και Windows NT 4.0.
- Outlook Express 4.01 on Solaris
- Outlook Express 4.01 για Macintosh

1.9 Update για την Windows NT Privilege Elevation επίθεση

Ο Mark Joseph Edwards ενημέρωσε την Microsoft για το αδύνατο σημείο του Microsoft Windows NT λειτουργικού συστήματος σχετικά με την ανύψωση προνομίων.Το πρόγραμμα sechole.exe που γράφτηκε από τους Prasad Dabak, Sandeep Phadke και Milind Borate εκμεταλεύεται το τρωτό αυτό σημείο και εκτελεί μία σειρά από βήματα που επιτρέπουν σε μη διαχειριστικούς χρήστες που είναι logged on να κερδίσουν πρόσβαση στο σύστημα. Χρησιμοποιώντας αυτό το πρόγραμμα κάποιος μη διαχειριστικός χρήστης μπορεί να εκτελέσει αυθαίρετο κώδικα που θα τον επιτρέψει να αποκτήσει τοπικά διαχειριστικά προνόμια στο σύστημα. Προκειμένου να πραγματοποιήσει την επίθεση θα πρέπει ο χρήστης να έχει έναν έγκυρο λογαριασμό στο σύστημα . Ευαίσθητα συστήματα όπως τα Windows NT Domain Controllers όπου μη διαχειριστικοί χρήστες δεν έχουν εξ' ορισμού τοπικά δικαιώματα δεν είναι επιρρεπή σε τέτοιου είδους επιθέσεις.

Το λογισμικό που επηρρεάζεται είναι:

- Microsoft Windows NT Workstations 3.51και 4.0
- Microsoft Windows NT Server 3.51 και 4.0
- Microsoft Windows NT Server, Terminal Server Edition 4.0

1.10 Πληροφορίες σχετικά με το "Back Orifice" πρόγραμμα

Στις 21 Ιουλίου μία αυτοαποκαλούμενη ομάδα από hackers γνωστή ως Cult of the Dead Cow κυκλοφόρησε ένα πρόγραμμα το "Back Orifice" και ενημέρωσε τους χρήστες του Microsoft Windows λειτουργικού συστήματος ότι κινδύνευαν από τυχόν επιθέσεις. Η Microsoft έλαβε το θέμα σοβαρά και πληροφόρησε τους πελάτες της ότι αν χρησιμοποιούν ασφαλείς υπολογιστικές μεθόδους δεν βρίσκονται σε κίνδυνο. Επίσης οι χρήστες του Microsoft Windows λειτουργικού συστήματος δεν κινδυνεύουν επειδή το πρόγραμμα αυτό δεν τρέχει στα Windows NT Server.

Δεν είναι ακόμα ξεκάθαρο τι προτίθεται να κάνει το "Back Orifice". Το "Back Orifice" έχει περιγραφεί σαν ένα διαχειριστικό εργαλείο που προκαλεί κάποια ρήγματα στην ασφάλεια των Windows. Σύμφωνα με την ομάδα των hackers το πρόγραμμα μπορεί να προκαλέσει τα εξής :

- Την εξ' αποστάσεως παρακολούθηση και έλεγχο του υπολογιστή που τρέχει τα Microsoft Windows.
- Να διαβάζει καθετί που πληκτρολογεί ο χρήστης
- Να συλλαμβάνει τα images που εκθέτονται στην οθόνη
- Να κατεβάζει αρχεία εξ' αποστάσεως
- Να κατευθύνει πληροφορίες σε ένα απομακρυσμένο site στο δίκτυο

Θα πρέπει να γίνει κατανοητό σε αυτό το σημείο ότι τα προγράμματα που επιτρέπουν τον εξ' αποστάσεως έλεγχο των υπολογιστών τους θα πρέπει να εγκαθίστανται με προσοχή. Οι χρήστες δεν θα πρέπει να εγκαθιστούν αυτού

του είδους τα προγράμματα από τα site των hackers. Υπάρχουν πολλά εμπορικά εργαλεία που δίνουν αυτήν την δυνατότητα στους χρήστες.

1.11 Update διαθέσιμο για το "Windows.External" στο Microsoft Internet Explorer 4.0

Πρόσφατα η Microsoft ενημερώθηκε από τον George Guninski και NTBugTraq σχετικά με τον τρόπο που ο Microsoft Internet Explorer 4.0, 401 και 4.01 SP 1 χειρίζεται τα JScript που κατεβάζει από τα διάφορα sites. Ο Microsoft Internet Explorer 4.0, 401 και 401 SP1 χρησιμοποιεί JScript Scripting Engine 3.1 για να επεξεργαστεί scripts των Web σελίδων. Όταν ο Internet Explorer συναντήσει μία Web σελίδα που χρησιμοποιεί JScript για να θέσει σε λειτουργία την Window.External συνάρτηση με ένα πολύ μεγάλο string, τότε ο Internet Explorer τερματίζεται. Μεγάλα strings δεν συναντούνται φυσιολογικά σε scripts και λογικά θα πρέπει να δημιουργούνται από κάποιον που έχει ύπουλο κίνητρο. Ένας έμπειρος hacker μπορεί να χρησιμοποιήσει το script μήνυμα για να εκτελέσει αυθαίρετο κώδικα που περιέχεται στο μεγάλο string.

Η Microsoft στις 17 Αυγούστου κυκλοφόρησε ένα πρόγραμμα που αντιμετωπίζει το πρόβλημα. Αυτό το πρόγραμμα μπορεί να το κατεβάσει από το site της Microsoft.

Προβλήματα έχουν εμφανιστεί στο εξής λογισμικό:

- Microsoft Internet Explorer 4.0,4.01.4.01 SP1 στα Windows 95 και Windows NT 4.0 λειτουργικά συστήματα
- Microsoft Windows 98

Τέλος θα πρέπει να σημειωθεί ότι το πρόβλημα δεν παρουσιάζεται στον Internet Explorer 4.0 για Windows 3.1, Windows NT 3.51, Macintosh, Unix(Solaris) και Internet Explorer 3.x.

1.12 Διαθέσιμο πρόγραμμα που διορθώνει τον Internet Explorer μέσω του Cross Frame Navigate

Η Microsoft έχει κυκλοφορήσει ένα πρόγραμμα που διορθώνει ένα πρόσφατο πρόβλημα που ανακαλύφτηκε με την εφαρμογή του cross frame security στον Microsoft Internet Explorer. Η cross frame navigate ανακάλυψε ένα τρωτό σημείο στον Internet Explorer που επιτρέπει σε έναν hacker να καταστρατηγήσει τα προφυλακτικά μέτρα του Explorer. Συγκεκριμένα, ένας Web site operator μπορεί να διαβάσει τα περιεχόμενα των αρχείων στο υπολογιστή κάποιου χρήστη. Πάντως μέχρι σήμερα δεν έχουν αναφερθεί τέτοια κρούσματα.

Το λογισμικό που παρουσιάζει αυτό το αδύνατο σημείο είναι:

- Microsoft Internet Explorer 4.0, 4.01, και 4.01 SP1 στα Windows NT 4.0, Windows 95

- Microsoft Windows 98 με ενσωματωμένο τον Internet Explorer (την έκδοση 4.01 SP1)
- Microsoft Internet Explorer 4.0 και 4.01 για Windows 3.1 και Windows NT 3.51
- Microsoft Internet Explorer 4.0 και 4.01 για Macintosh

Το πρόβλημα δεν επηρρεάζει τον Internet Explorer 3.x. Επίσης επηρρεάζεται και το λογισμικό που χρησιμοποιεί HTML functionality που παρέχεται από τον Internet Explorer. Ο κάθε χρήστης που χρησιμοποιεί το παραπάνω λογισμικό θα πρέπει να κατεβάσει από το site της Microsoft τα ανάλογα προγράμματα που διορθώνουν το πρόβλημα.

Παρακάτω παρέχονται συμβουλές στους χρήστες για να διαπιστώσουν αν έχουν μία προσβεβλημένη έκδοση του mshtml.dll.

Για τα Windows 98, Windows 95 και στα Windows NT 4.0

1. Από το start menu επέλεξε Find και διάλεξε Files of Folders.
2. Στο Named box γράψε mshtml.dll.
3. Στο Look in box, click το κάτω βέλος και επέλεξε τον τοπικό σκληρό δίσκο από τη λίστα.
4. Κλίκαρε Find Now.
5. Αν το mshtml.dll δεν βρεθεί, τότε το σύστημα δεν χρειάζεται να αποκτήσει το πρόγραμμα.
6. Αν το mshtml.dll βρεθεί τότε right-click το αρχείο, επέλεξε Properties και επέλεξε Version tab.
7. Αν η έκδοση του αρχείου είναι μικρότερη από 4.72.3509.0100 τότε το σύστημα θα πρέπει να έχει προσβληθεί και θα πρέπει ο χρήστης να κατεβάσει το πρόγραμμα.

Για τα Windows 3.1x

1. Από το File Menu στον File Manager επέλεξε search.
2. Στο Search For box γράψε mshtml16.dll.
3. Στο Start From box γράψε το drive:\windows directory\SYSTEM
4. Κλίκαρε ok.
5. Αν το mshtml16.dll δεν βρεθεί, τότε το σύστημα δεν χρειάζεται το διορθωτικό πρόγραμμα.
6. Αν βρεθεί, κλίκαρε το αρχείο, πάτησε Alt-Enter και στη συνέχεια έλεγξε την έκδοση.
7. Αν η έκδοση του αρχείου είναι ίση ή μικρότερη από 4.01.2509.0200 τότε το σύστημα θα πρέπει να έχει προσβληθεί και θα πρέπει ο χρήστης να κατεβάσει το πρόγραμμα.

Για Macintosh

1. Στον Internet Explorer κλίκαρε το Apple icon και επέλεξε About Internet Explorer
2. Κοίταξε τον αριθμό της έκδοσης του Internet Explorer στην κάτω αριστερή γωνία του dialog box.
3. Αν η έκδοση είναι 4.01 (Power PC) ή 4.01 (68K) τότε το σύστημα θα πρέπει να έχει προσβληθεί και θα πρέπει ο χρήστης να κατεβάσει το πρόγραμμα.
4. Αν η έκδοση είναι 4.0 τότε το σύστημα θα πρέπει να έχει προσβληθεί και θα πρέπει ο χρήστης να κατεβάσει το διορθωτικό πρόγραμμα.
5. Αν η έκδοση είναι 4.01 (310), τότε ο χρήστης έχει ήδη το διορθωτικό πρόγραμμα.

1.13 Update διαθέσιμο για "Unstructured Scripted Paste" στον Microsoft Internet Explorer 4.01

Στις 18 Νοεμβρίου η Microsoft κυκλοφόρησε μία updated έκδοση του διορθωτικού προγράμματος για το "Unstructured Script Paste" πρόβλημα. Το τρωτό αυτό σημείο που είναι γνωστό και σαν "Cuartango" δίνει τη δυνατότητα σε κάποιον web site operator να χρησιμοποιήσει scripted paste operations για να διαβάσει αρχεία που ανήκουν σε μια γνωστά τοποθεσία στο σύστημα ενός χρήστη.

Η Microsoft συνιστά σε όλους τους χρήστες που το σύστημά τους έχει προσβληθεί - ακόμα και σ΄αυτούς που έχουν κατεβάσει το διορθωτικό πρόγραμμα πριν τις 18 Νοεμβρίου - να κατεβάσουν και να εγκαταστήσουν την ανανεωμένη έκδοση ώστε να προστατεύσουν τους υπολογιστές.

Συγκεκριμένα το αδύνατο αυτό σημείο στον Internet Explorer επιτρέπει σε έναν web site operator να υπερπηδήσει τα μέτρα προστασίας του Explorer και να διαβάσει τα περιεχόμενα ενός καταλόγου που υπάρχουν στον υπολογιστή ενός χρήστη αν αυτός ξέρει το όνομα και το μονοπάτι που βρίσκεται το συγκεκριμένο αρχείο.

Το λογισμικό που εμφανίζει αυτού του είδους τα προβλήματα είναι :

- Microsoft Internet Explorer 4.01 και 4.01 SP1 στα Windows NT 4.0 και Windows 95
- Microsoft Windows 98 που έχουν ενσωματωμάνο τον Internet Explorer
- Microsoft Internet Explorer 4.01 για Windows 3.1 και Windows NT 3.51

Επίσης επηρρεάζεται και το λογισμικό που χρησιμοποιεί HTML functionality που παρέχεται από τον Internet Explorer ακόμα και όταν ο Internet Explorer δεν χρησιμοποιήται σαν εξ' ορισμού browser. Αυτό το πρόβλημα δεν συναντάται στον Internet Explorer 3.x ή 4.0 καθώς και στις εκδόσεις του Explorer για Macintosh και UNIX.

1.14 Διαθέσιμο πρόγραμμα για το "Dotless IP Address" πρόβλημα στον Microsoft Internet Explorer

Η Microsoft έχει διαθέσει στην αγορά ένα πρόγραμμα που διορθώνει το πρόβλημα που παρουσιάζεται στον Internet Explorer 4 σχετικά με τον τρόπο που αυτός καθορίζει σε ποια ζώνη ασφαλείας βρίσκεται ένας συγκεκριμένος εξυπηρέτης. Είναι δυνατόν ένας hacker να εκμεταλλευτεί το αδύνατο αυτό σημείο ώστε να παραπλανήσει το URL του website και να συμπεριφέρεται το site σαν να είναι τοποθετημένο στο intranet. Αυτό δεν μπορεί να γίνει τυχαία εκτός και αν ένας website operator επίτηδες παραπλανήσει το URL του site δημιουργώντας κώδικα για να προσβάλει τους χρήστες. Ο Internet Explorer έχει την ικανότητα να θέσει διαφορετικά security settings μεταξύ διαφορετικών ζωνών.΄Αυτό σημαίνει ότι ένα ύποπτο site θα μπορεί να εκτελεί ενέργειες που εξουδετερώνονται στην Internet ζώνη ή στη Restricted Sites Zone αλλά επιτρέπονται στην Local Intranet Zone. Η ουσία του προβλήματος έγκειται στο γεγονός ότι κατά τον καθορισμό της ζώνης που ένα web site ανήκει, ο Internet Explorer μεταφράζει το 32 bit νούμερο σαν ένα αριθμητικό host name, ενώ το IP stack αναλύει τη διεύθυνση στο ισοδύναμό του IP format. Ο Explorer θεωρεί λαθεμένα ότι η μηχανή βρίσκεται στην Local Intranet Zone αντί να είναι στην Internet Zone και έτσι εφαρμόζει ανακριβής security settings του web server.

Το λογισμικό που παρουσιάζει αυτό το αδύνατο σημείο είναι:

- Microsoft Internet Explorer 4.0, 4.01 και 4.01 SP1 στα Windows NT 4.0 και Windows 95
- Microsoft Windows 98 που έχουν ενσωματωμένο τον Internet Explorer
- Microsoft Internet Explorer 4.0 και 4.01 για τα Windows 3.1 και Windows NT 3.51
- Microsoft Internet Explorer 4.01 για UNIX

Ο Internet Explorer 3 και ο Internet Explorer 4 για Macintosh δεν παρουσιάζει αυτό το πρόβλημα.

Αν κάποιος χρήστης δεν μπορεί να εφαρμόσει το διορθωτικό πρόγραμμα, τότε αυτός μπορεί να μειώσει τον κίνδυνο από το να προσβληθεί από το πρόβλημα με να ρυθμίσει τις Intranet Zone settings έτσι ώστε να είναι ίδιες με αυτές που χρησιμοποιπύνται στην Internet Zone. Για να το κάνει αυτό θα πρέπει να εκτελέσει τα παρακάτω βήματα:

1. Κλίκαρε start, επέλεξε τα settings και μετά κάντε κλικ στο Control Panel.
2. Double-cick Internet και μετά επέλεξε Security tab.
3. Στο Zone box επέλεξε local Intranet Zone.
4. Τροποποιήσε το local Intranet zone security επίπεδο ή τα custom settings ώστε να ταιριάζουν με αυτά στην Internet Zone.
5. Επέλεξε ok για να κλείσει το Internet Properties sheet.

1.15 Πρόγραμμα που φτάχνει το "Named Pipes Over RPC" πρόβλημα

Η Microsoft έχει κυκλοφορήσει ένα πρόγραμμα που διορθώνει τον τρόπο που τα Windows NT χειρίζονται τα named pipes over των Remote

Procedure Call (RPC) υπηρεσιών. Κάποιος χρήστης μπορεί να προκαλέσει τη διακοπή των υπηρεσιών ενός συστήματος που χρησιμοποιεί Windows NT 4.0 ανοίγοντας πολλαπλές named pipe συνδέσεις και να στείλει τυχαία δεδομένα.

Το πρόβλημα έγκειται στον τρόπο που τα Windows NT 4.0 κλείνουν τις άκυρες RPC συνδέσεις. Όταν η RPC υπηρεσία επιχειρεί να κλείσει μία άκυρη σύνδεση αυτή καταναλώνει όλους τους πόρους της CPU και πολλή μνήμη με αποτέλεσμα το σύστημα να κρεμάει.

Διαφορετικά προγράμματα προσβάλλουν διαφορετικές υπηρεσίες του συστήματος. Δύο από αυτές τις υπηρεσίες που συχνά γίνονται στόχος επιθέσεων είναι οι SPOOLS και LSASS.

Το λογισμικό που έχει αυτά τα προβλήματα είναι:

- Microsoft Windows NT Workstation 4.0
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0 Enterprise edition
- Microsoft Windows NT Server 4.0 Terminal Server Edition

1.16 Πρόγραμμα που διορθώνει το πρόβλημα στο Excel

Στις 7 Δεκεμβρίου η Microsoft διάθεσε στην αγορά ένα πρόγραμμα που διόρθωνει τον τρόπο που το Excel εκτελεί κάποιες εντολές χωρίς να στείλει προειδοποίηση στον χρήστη. Κάτι τέτοιο εγκυμονεί κινδύνους για το σύστημα του χρήστη αν οι εντολές αυτές καλούνται από μια συνάρτηση που έχει σαν σκοπό να προκαλέσει προβλήματα.

Συγκεκριμένα η CALL είναι μία advanced συνάρτηση στο Excel που επιτρέπει σε ένα worksheet να καλέσει μία procedure DDl. Το Excel πάντα προειδοποιεί το χρήστη πριν εκτελέσει τις macro εντολές έτσι ώστε να αποφασίσει αυτός αν θα πρέπει να τις τρέξει ή όχι. Όμως το Excel δεν προειδοποιεί το χρήστη προτού εκτελέσει τις worksheet συναρτήσεις. Έτσι είναι δυνατόν κάποιος χρήστης να εκμεταλλευτεί τη λειτουργία αυτή του Excel και να τοποθετήσει μία CALL συνάρτηση μέσα σ΄ένα spreadsheet και να τη στείλει σε έναν ανυποψίαστο χρήστη και να αποκτήσει τον έλεγχο όταν η συνάρτηση αυτή πυροδοτηθεί μόλις ανοίξει ο user το spreadsheet ή συμβει κάποιο άλλο γεγονός.

Αν και δεν έχουν παρουσιαστεί ακόμη τέτοιου είδους κρούσματα, η Microsoft είναι ενήμερη του προβλήματος και έχει φτιάξει ένα πρόγραμμα που εξουδετερώνει την CALL συνάρτηση στο worksheet. Όμως δεν εξουδετερώνει την CALL συνάρτηση όταν τρέχει μέσα από τις macro εντολές.

1.17 Πρόγραμμα που διορθώνει το πρόβλημα στη μέθοδο “GET” του Internet Information Server

Το πρόβλημα αυτό παρουσιάστηκε στην HHTP GET μέθοδο που χρησιμοποιήται για να πάρει πληροφορίες από έναν IIS web server. Ειδικά σχεδιασμένες get αιτήσεις μπορούν να καταναλώσουν όλους τους πόρους του

server με αποτέλεσμα να "κρεμάσει" το σύστημα. Σε αυτήν την περίπτωση θα πρέπει να κάνεις reboot το server. Το πρόγραμμα που διορθώνει το πρόβλημα βρίσκεται στο site της Microsoft ενώ το λοφισμικό που εμφανίζει αυτά τα προβλήματα είναι:

- Microsoft Internet Information Server 3.0 και 4.0 για x86 και Alpha πλατφόρμες.

1.18 Πρόγραμμα που αντιμετωπίζει το "Frame Spoof" πρόβλημα

Η Microsoft έχοντας επίγνωση του αδύνατου αυτού σημείου σον Internet Explorer δημιούργησε ένα πρόγραμμα που βάζει τέλος στην δυνατότητα που έχει ένας web site operator να υποδυθεί ένα παράθυρο σε ένα νόμιμο web site. Το ψεύτικο αυτό παράθυρο θα μπορεί να μαζεύει πληροφορίες από τον ανυποψίαστο χρήστη και να τις στέλνει στο ύποπτο site. Το πρόβλημα υπάρχει γιατί η Internet Explore's cross domain προστασία δεν επεκτείνεται και στη πλοήγηση των πλαισίων (navigation of frames). Έτσι είναι δυνατόν ένα ύποπτο web site να εισάγει δεδομένα μέσα στο πλαίσιο ενός άλλου web site. Αν το καταφέρει, τότε ο χρήστης δεν είναι σε θέση να δει αν τα περιεχόμενα του πλαισίου δεν είναι από το νόμιμο site και να δώσει προσωπικά δεδομένα στο ύποπτο site.

Το λογισμικό που έχει αυτά τα προβλήματα είναι:

- Microsoft Internet Explorer 3.x, 4.0,4.01, 4.01 Service Pack1 γαι Windows 95
- Microsoft Internet Explorer 4.01 Service Pack1 για Windows 98
- Microsoft Internet Explorer 3.x, 4.0,4.01, 4.01 Service Pack1 γαι Windows NT 4.0
- Microsoft Internet Explorer 3.x, 4.0,4.01 για Windows 3.1
- Microsoft Internet Explorer 3.x, 4.0,4.01 για Windows NT 3.51
- Microsoft Internet Explorer 4 για UNIX on HPUX
- Microsoft Internet Explorer 3.x,4.x για Macintosh
- Microsoft Internet Explorer 4 για UNIX on Sun Solaris.

2. Προϊόντα της Microsoft

2.1 Microsoft Windows NT Server and Windows NT Workstation

Η οικογένεια της Microsoft παρέχει ένα ισχυρό multipurpose λειτουργικό σύστημα. Παρέχει μία αξιόπιστη και βαθμωτή πλατφόρμα για Intranet και line-of-business εφαρμογές και δίνει στους χρήστες τη δυνατότητα να έχουν πρόσβαση σε σημαντικές πληροφορίες και πηγές πολύ εύκολα και αποδοτικά.

Χαρακτηριστικά ασφαλείας

- Εύκολα διαχειρίσιμο με βαθμωτή αρχιτεκτονική ασφαλείας

- Standards βασισμένα σε κανόνες ασφαλείας
- Fine-grained file access control
- Εκτεταμένες αναφορές και συναρτήσεις παρακολούθησης

2.2 Microsoft Certificate Server

Microsoft Certificate Server είναι μέρος του Microsoft Windows NT 4.0 Option Pack. Παρέχει προσαρμοζόμενες υπηρεσίες για την εκπομπή και διαχείριση digital certificates που χρησιμοποιούνται στα συστήματα ασφαλείας χρησιμοποιώντας public-key κρυπτογραφία. Ο Certificate Server διαδραματίζει ένα σημαντικό ρόλο στη διαχείριση των συστημάτων ασφαλείας και καθιστά δυνατή την ασφαλή επικοινωνία στο Internet, σε corporate Intranets ή σε άλλα μη ασφαλή δίκτυα.

Χαρακτηριστικά ασφαλείας

- Επίτρέπει την εταιρία να χρησιμοποιήσει την εξουσία της καλύτερα
- Επιτρέπει strong authentication μέσα σε επιχειρησιακά Intranets και Extranets
- Επιτρέπει επιχειρησιακό code-signing και αποτρέπει τυχόν εισβολές στο δίκτυο
- Υποστηρίζει την έκδοση του Certificate Revocation List
- Standards βασισμένα στην x.509 έκδοσης 3 certificate format και PCKS#7 και #10 κρυπτογραφικά μηνύματα.

2.3 Microsoft Exchange Server

Microsoft Exchange Server είναι ένας enterprise-ready messaging εξυπηρέτης που τρέχει μέσω του Microsoft Windows NT Server. Η ανταλλαγή έχει δημιουργηθεί πάνω στην αρχιτεκτονική των Internet προτύπων και παρέχει μία δική της αρχιτεκτονική ασφαλείας συν αυτή που χρησιμοποιούν τα Windows NT.

Χαρακτηριστικά ασφαλείας

- Ενοποιεί τον Microsoft Exchange με το Windows NT logon
- Παρέχει ασφαλή κώδικα χρησιμοποιώντας SASL
- Υποστηρίζει Secure Socket Layer (SSL) και encrypted SMTP (E/SMTP)
- Υποστηρίζει digital signatures.

2.4 Microsoft Front Page

Το Microsoft Front Page 98 εργαλείο δίνει τη δυνατότητα στο χρήστη να δημιουργεί web sites χωρίς προγραμματισμό.

Χαρακτηριστικά ασφαλείας

- Προσφέρει ασφάλεια αφού χρησιμοποιεί Secure Socket Layer

2.5 Microsoft Internet Explorer

Microsoft Internet Explorer είναι ένας ολοκληρωμένος Internet browser και αποτελεί μέρος του Microsoft Windows 95, του Windows 98 και του Windows NT λειτουργικού συστήματος που παρέχει ασφάλεια με τις ζώνες ασφαλείας και τον Authenticode που υποστηρίζει.

Χαρακτηριστικά ασφαλείας

- Οι ζώνες ασφαλείας επιτρέπουν στον χρήστη να καθορίσει κατά πόσο εμπιστεύεται web sites και περιορίζει τι μπορούν να κάνουν αυτά τα sites
- Περιέχει τον Advisor που επιτρέπει στον χρήστη να διαλέξει τα sites που ο browser μπορεί να παρουσιάσει ανάλογα με το βαθμό της βίας, του sex και της γλώσσας που έχουν.
- Υποστηρίζει digital certificates
- Υποστηρίζει Secure Socket Layer
- Server Gated Cryptography

2.6 Microsoft Internet Information Server

Microsoft Internet Information Server παρέχει πρόσβαση σε Web αρχεία καθώς και διάφορες εφαρμογές για τον Microsoft Windows NT Server. Ο Internet Information Server χρησιμοποιεί όλα τα εργαλεία διαχείρισης και ασφαλείας του Windows NT Server κι έτσι η πρόσβαση στο Web είναι εύκολη και αφαλής.

Χαρακτηριστικά ασφαλείας

- Ικανότητα να περιορίσει το bandwidth του δικτύου που χρησιμοποιεί
- Ικανότητα να μοιράσει ή να προστατεύσει τα αρχεία σε ατομική βάση
- Χρησιμοποιεί τα εργαλεία διαχείρισης και ασφάλειας των Windows NT

2.7 Microsoft Proxy Server

Microsoft Proxy Server είναι ένας ολοκληρωμένος firewall και Web cashe server. Τα firewall στοιχεία του παρέχουν εμπόδια σε τυχόν εισβολές από ύποπτους χρήστες όταν συνδέσεις το δίκτυο σου με ένα εξωτερικό δίκτυο όπως είναι το Internet. Τα web cashing στοιχεία του βελτιώνουν την απόδοση του δικτύου με το να σώζει τις πιο συχνά εμφανιζόμενες web σελίδες και στη συνέχεια να τις παρέχει άμεσα παρά να τις φορτώνει από τα απομακρυσμένα

sites. Επίσης τα Microsoft Proxy Server plug-in modules παρέχουν πρόσθετες λειτουργίες όπως virus scanning των εισερχόμενων αρχείων καθώς και content filtering.

Χαρακτηριστικά ασφαλείας

- Προστατεύει το εσωτερικό δίκτυο από εξωτερικές εισβολές
- Application-layer, circuit-layer και packet-layer firewall
- Δυναμική διύλιση των εισερχόμενων και των εξερχόμενων πακέτων
- Υποστηρίζει SSL tunneling, full-access control και strong authentication
- Συνεχή παρακολούθηση του υπάρχον δυναμικού.

2.8 Microsoft SNA Server

Ο Microsoft SNA Server επιτρέπει στους χρήστες να εκμεταλλευτούν τα πλεονεκτήματα του μοντέρνου client-server software.

Χαρακτηριστικά ασφαλείας

- Single sign on to AS/400 and mainframe systems
- Συγχρονισμός του κώδικα από τα Windows NT domains με τα AS/400 partner προϊόντα που μπορούν να χρησιμοποιηθούν για τον εμπλουτισμό της συνολικής λύσης
- Bulk migration εργαλείο που επιτρέπει πολλαπλούς mainframe user λογαριασμούς να συνδυαστούν με το Windows operating system domain
- Link encryprion of terminal emulation sessions

2.9 Microsoft SQL Server

Ο Microsoft SQL Server είναι μία υψηλής απόδοση σχεσιακή βάση δεδομένων για το λειτουργικό σύστημα των Windows NT. Εκτός του ότι συμβάλει στην ασφάλεια των Windows NT, έχει ένα δικό του μοντέλο ασφαλείας που επιτρέπει τηνρυθμιζόμενη πρόσβαση στα δεδομένα καθώς και τη συνεχή παρακολούθησή τους.

Χαρακτηριστικά ασφαλείας

- Single login ID για δίκτυα και database logins παρέχοντας περισσότερη ασφάλεια και μειώνει την πολυπλοκότητα της διαχείρισης.
- Ικανότητα να αποκρύπτει κωδικούς και δικτυακά δεδομένα για τη βελτίωση της ενδοδικτυακής ασφάλειας
- Απόκρυψη των αποθηκευμένων procedures για να εξασφαλίσει την ακεραιότητα και ασφάλεια του server-based application κώδικα.

2.10 Microsoft Systems Management Server

Ο Microsoft Systems Management Server δίνει τη δυνατότητα στους χρήστες να διαχειρίζονται καλύτερα το δίκτυο. Δίνει στους διαχειριστές τον κεντρικό έλεγχο του hardware και software στην επιχείρησή τους ώστε να μπορούν να εγκαθιστούν εξ' αποστάσεως το νέο λογισμικό στους εξυπηρέτες και να παρακολουθούν το δίκτυο.

Χαρακτηριστικά ασφαλείας

- Ελεγχόμενη πρόσβαση στις λειτουργίες του Systems Management Server
- Παρακολούθηση της απόδοσης και της χρήσης του δικτύου
- Η αποκρυπτογράφηση των δικτυακών πακέτων επιτρέπει την ανάλυση των δικτυακών επικοινωνιών
- Fully leverages Microsoft Windows NT security architecture

3 Τεχνολογίες της Microsoft

3.1 Authenticode

Η Microsoft Authenticode τεχνολογία, ένα στοιχείο ασφάλειας του Microsoft Internet Explorer εξασφαλίζει υπευθυνότητα και αυθεντικότητα του software στο Internet.

Χαρακτηριστικά ασφαλείας

- Υποστηρίζει X.509 έκδοση 3 digital certificates
- Digital signatures υποστηρίζονται σύμφωνα με τα πρότυπα PKCS #7 και #10
- Strong 128-bit digital signatures

3.2 Crypto API

Crypto API είνα μία εφαρμογή που αποτελεί μέρος των Microsoft Windows 95, 98 και των Windows NT. Παρέχει ένα πλαίσιο εργασίας όπου τα προγράμματα μπορούν να το χρησιμοποιήσουν για να αποκτήσουν κρυπτογραφικές και digital certificate υπηρεσίες.

Χαρακτηριστικά ασφαλείας

- Υποστηρίζει κρυπτογραφικούς αλγόριθμους για public-key και shared-secret key
- Υποστήριξη για certificate handling services

- Υποστηρίζει κρυπτογραφικά πρότυπα όπως IETF, (PKIX, S/MIME), PKCS, X.509 κτλ.

3.3 Digital Certificates

Digital Certificates είναι μέσο παρεμπόδισης στο να δοθούν λεπτομέρειες σχετικά με το public-key ενός χρήστη ή μιας επιχείρησης. Digital Certificates εξυπηρετεί δύο σκοπούς. Πρώτον παρέχει ένα κρυπτογραφικό κλειδί έτσι ώστε ο χρήστης να αποκρύψει πληροφορίες σχετικές με αυτόν και δεύτερον αποτελεί ένα μέτρο αναγνώρισης του χρήστη. Η Microsoft χρησιμοποιεί το πρότυπο X.509 στα προϊόντα της όπως Microsoft Windows NT , Microsoft Internet Explorer και Microsoft Internet Information Server.

3.4 Kerberos Authentication Protocol

Kerberos είναι ένα πρωτόκολο αυθεντικότητας που παρέχει υψηλη ασφάλεια. Στην καρδιά του πρωτόκολου είναι ένας έμπιστος εξυπηρέτης που ονμάζεται Key Distribution Center (KDC). Όταν ο χρήστης κάνει log in σ΄ένα δίκτυο τότε το KDC επαληθεύει την ταυτότητα του χρήστη και δίνει πιστοποιητικά ή "εισητήρια" για κάθε μία υπηρεσία του δικτύου θέλει να χρησιμοποιήσει. Κάθε εισητήριο εισάγει το χρήστη στην κατάλληλη υπηρεσία ενώ ταυτόχρονα κρατά πληροφορίες σχετικά με τα προνόμια που έχει ο χρήστης γι΄αυτήν την υπηρεσία.

Το Kerberos πρωτόκολο είναι ο βασικός μηχανισμός αυθεντικότητης για το λειτουργικό σύστημα των Microsoft Windows NT 5.0. Επιπλέον η Microsoft επιτρέπει επεκτάσεις του πρωτοκόλου για να χρησιμοποιηθούν smart cards κατά τη διάρκεια του network logon. Αυτό δίνει το διπλό πλεονέκτημα της ενίσχυσης της αυθεντικότητας και της εισαγωγής της υποδομής του public key των Windows NT.

3.5 Secure Sockets Layer/Transport Layer Security

Secure Sockets Layer είναι ένα πρωτόκολο που έχει σχεδιαστεί για να προσφέρει μυστικότητα μεταξύ του Web client και του Web server. Το πρωτόκολο αρχίζει με μια φάση διαπραγμάτευσης μεταξύ τπυ κλειδιού και του αλγόριθμου απόκρυψης και στη συνέχεια πιστοποιεί την αυθεντικότητα του εξυπηρέτη στον client. Μόλις τελειώσει αυτή η διαδικασία αρχίζουν να μεταδίδονται τα δεδομένα.

Το SSL/TLS πρωτόκολο υλοποιήται στον Microsoft Internet Explorer και στον Microsoft Internet Information Server και επιτρέπει στους χρήστες να εγκαθιστήσουν ασφαλείς World Wide Web sessions.

3.6 Server Gated Cryptography

Η Server Gated Cryptography (SGS) παρέχεται στα Microsoft Windows 95, 98 και των Windows NT λειτουργικά συστήματα και προσφέρει μία 128-bit κρυπτογραφία για online banking.

Χαρακτηριστικά ασφαλείας

- Υποστηρίζει 128-bit απόκρυψη για online banking sessions.
- Ενδολειτουργεί με όλες τις vendor's implementation of SGS

3.7 Smart Cards

Μία Smart Card είναι μία συσκευή που περιέχει ένα μικριεπεξεργαστή, ένα μικρό μέγεθος μνήμης και ένα interface που επιτρέπει σε αυτή να επικοινωνεί με ένα workstation ή ένα δίκτυο. Δύο χαρακτηριστικά κάνει την Smart Card κατάλληλη για εφαρμογές που σχετίζονται με την ασφάλεια των δεδομένων. Πρώτον, επειδή η Smart Card έχει τα δεδομένα και τους τρόπους να τα επεξεργαστεί ενώ ο επεξεργαστής μπορεί να εξυπηρετήσει τις αιτήσεις του δικτύου και να επιστρέψει τα αποτελέσματα χωρίς να αποκαλύψει ευαίσθητα δεδομένα. Δεύτερον επειδή οι Smart Cards είναι φορητές, ο χρήστης μπορεί να μεταφέρει τα δεδομένα παρά να είναι εγκατεστημένα στο δίκτυο. Για παράδειγμα, ένας χρήστης μπορεί να χρησιμοποιήσει την Smart Card για να μεταφέρει τις προσωπικές του πληροφορίες.

Τα Microsoft Windows 95, 98 και των Windows NT 4.0 υποστηρίζουν την τεχνολογία Smart Cards και μπορουν να χρησιμοποιηθούν στον Microsoft Internet Explorer και κυρίως στο Outlook Express ή Outlook 98 για να στείλει και να λάβει ασφαλή μηνύματα. Στα Windows NT 5.0 οι Smart Cards μπορούν να χρησιμοποιηθούν για logon στο δίκτυο αφού χρησιμοποιεί την X.509 εκδοση 3 που αποθηκεύεται πάνω της.

Στις 27 Οκτωβρίου 1998 η Microsoft το Smart Card για Windows, ένα λειτουργικό σύστημα για Smart Cards με 8K ROM τρέχει τις Visual Basic εφαρμογές και σχεδιάστηκε για να επεκτείνει το περιβάλλον του υπολογιστή μέσα από τη χρήση της Smart Card.

Χαρακτηριστικά ασφαλείας

- Μπορεί να μεταφέρει σημαντικές πληροφορίες
- Απομονώνει σημαντικούς υπολογισμούς ασφαλείας όπως authentication, digital signatures και key exchange από τα άλλα μέρη του συστήματος
- Tamper-resistant αποθήκευση για προστασία των μυστικών κλειδιών και άλλων προσωπικών πληροφοριών.

3.8 Virtual Private Networks

Μέχρι πρόσφατα οι επιχειρήσεις που έπρεπε να μοιράσουν τα δεδομένα τους με τους χρήστες ή με εξωτερικά δίκτυα είχαν δύο επιλογές: ή να αφήσει η

επιχείρηση να ταξιδέψουν τα μυστικά της μέσα στο Internet με την ελπίδα ότι κανένας δε θα παρακολουθεί ή να νοικιάσουν ασφαλείς επικοινωνιακές γραμμές και να δημιουργλησουν ένα ιδιωτικό δίκτυο. Μία καλύτερη λύση είναι να φτιάξουν ένα Virtual Private Network (VPN). Στο Virtual Private Network τα δεδομένα ταξιδεύουν μέσα από δημόσια δίκτυα όπως το Internet αλλά γίνονται φανερές μόνο οι πληροφορίες που χρειάζεται ο χρήστης, ενώ όλες οι άλλες πληροφορίες κρυπτογραφημένες.

Υπάρχουν τρία βασικά πρωτόκολα για τη δημιουργία VPNs

- **Point-to-Point Tunneling Protocol (PPTP)**, το πιο γνωστό tunneling protocol σήμερα.PPTP παρέχεται μέσα από τις Remote Access Services (RAS) στα Windows NT 4.0 και Windows 2000 λειτουργικά συστήματα και χρησιμοποιεί την υπαρχουσα Microsoft Windows κρυπτογράφηση, την user authentication και configuration infrastructure του Point-to-Point Protocol για τη δημιουργία κρυπτογραφικών κλειδιών
- **Layer 2 Tunneling Protocol (L2TP)** ένα Internet Engineering Task Force πρωτόκολο που χρησιμοποιεί την τεχνολογία του public key για να πιστοποιήσει την αυθεντικότητα του χρήστη και το οποίο χρησιμοποιήται σε περισσότερα μέσα επικοινωνίας από ότο το PPTP. Θα πρέπει να σημειωθεί ότι το L2TP δεν εκτελεί κρυπτογράφηση. Το L2TP παρέχεται στις RAS στα Windows 2000.
- **IPSec**, ένα IETF πρωτόκολο που παρέχει απόκρυψη και computer authentication που βασίζεται στην τεχνολογία του public key. Τα βασικά πλεονεκτήματα του IPSec είναι ότι μπορεί να χρησιμοποιηθεί για φτιάξει ένα VPN αυτόματα ανάλογα με την πολιτική ασφαλείας της επιχείρησης και ότι μπορεί να δημιουργήσει VPN βασισμένη στις μηχανές και όχι στους χρήστες. Το IPSec παρέχεται στις RAS στα Windows 2000 και στα Windows NT 4.0.

Στο σημείο αυτό θα πρέπει να παρατηρήσουμε τα εξής :

- PPTP μπορεί να δημιουργήσει ένα VPN από μόνο του. Το PPTP καλύπτει τις ανάγκες των περισσότερων επιχειρήσεων για ασφάλεια και μπορεί να προσφέρει μια φτηνή και λιγότερο πολύπλοκη διαχείριση του περιβάλλοντος
- Το L2TP μαζί με το IPSec δημιουργούν μαζί ένα ασφαλή VPN. Τα VPN και L2TP καλύπτουν τις ανάγκες των επιχειρήσεων για advanced απαιτήσεις ασφάλειας αν και μία ακριβή και πολύπλοκη λύση.

4 Τελευταία νέα για τη Microsoft

4.1 Η Microsoft και τα προϊόντα της Modulo προστάτευσαν τις εκλογές

Στις πρόσφατες εκλογές που έγιναν στην Βραζιλία όπου πάνω από 60 εκατομμύρια πολίτες ψήφισαν ηλεκτρονικά για πρόεδρο, την Γερουσία και για πάνω από 2000 τοπικά γραφεία, η Microsoft με τα Windows NT 4.0 και η Modulo με τα He@tseeker Pro και CFW98 προϊόντα δημιούργησαν ένα ασφαλές περιβάλλον που εξασφάλιζε την αξιοπιστία των εκλογών.

Συγκεκριμένα τα Windows NT 4.0 Server και Workstation παρείχαν όλα εκείνα τα στοιχεία που χρειαζόταν για να υποστηρίξουν ένα δίκτυο τέτοιου μεγέθους και με μεγάλη πολυπλοκότητα. Σε αυτό το εγχείρημα βοήθησαν και τα προϊόντα της Modulo.

Το δίκτυο συνεχώς παρακολουθούσε τον ευατό του για τυχόν επιθέσεις.. Έλεγχε κάθε αίτηση για πρόσβαση στα στοιχεία ή στους πόρους του συστήματος και ενημέρωνε τους υπεύθυνους των εκλογών σε κάθε ένδειξη εισβολής. Αυτό επιτυγχάνονταν από ένα ολοκληρωμένο σύστημα παρακολούθησης όπου καταγράφονταν κάθε πρόσβαση στους υπολογιστές, στα αρχεία, ή στα προγράμματα.

4.2 Το RSA Data Security συνέδριο

Η Microsoft είναι ο βασικός χορηγός του RSA Data Security συνεδρίου, το πιο σημαντικό συνέδριο της χρονιάς για την ασφάλεια και την κρυπτογραφία των δεδομένων. Με περισσότερες από 120 τοποθετήσεις για τους τελευταίους αλγόριθμους απόκρυψης μέχρι την εθνική πολιτική για την γρυπτογραφία, το συνέδριο είναι ιδανικό για τις επιχειρήσεις και τους τεχνολόγους.

Ο ρόλος της Microsoft στο συνέδριο είναι να παρέχει Internet και e-mail σύνδεση με τους σύνεδρους. Το δίκτυο θα τρέχει μέσα από τα Windows 2000 beta 2 κι έτσι δίνεται μία καθώς πρέπει ευκαιρία να αξιολογηθεί το καινούργιο αυτό μέλος της οικογένειας των Windows NT.

4.3 Ο ιός “Remote Explorer”

Ο ιός αυτός που πρόσφατα ανακαλύφθηκε έχει απασχολήσει την Microsoft. Αφού μελέτησε τον ιό κατέληξε στα εξής συμπεράσματα:

- Ο ιός ακολουθεί το παραδοσιακό σενάριο. Τρέχει κάτω από τα προνόμια του χρήστη, εγκαθιστά τον εαυτό του σε εκτελέσιμα αρχεία και απλώνονται όταν αυτοί μεταφέρονται σε άλλους υπολογιστές και καταστρέφουν τα αρχεία.
- Δεν εκμεταλλεύεται τα αδύνατα σημεία του λειτουργικού συστήματος των Windows NT.

Αυτό που είναι ασυνήθιστο με τον ιό είναι ότι όταν ένα αρχείο που έχει προσβληθεί τρέχει από έναν τοπικό διαχειριστή τότε χρησιμοποιεί τα προνόμια του διαχειριστή και εγκαθιστά τον εαυτό του δαν υπηρεσία. Στη συνέχεια όταν ο ιός μεταφερθεί σε άλλο υπολογιστή επαναλαμβάνει την ίδια διαδικασία.

Υπάρχουν δύο ειδών προσβολές:

- Infected executables: Αν ένα αρχείο που έχει προσβληθεί τρέξει από ένα διαχειριστικό χρήστη , θα προσπαθήσει να προσβάλει το τοπικό σύστημα με

το να εγκαταστήσει μία υπηρεσία των Windows NT που ονομάζεται "Remote Explorer".

- Virus-Installed System Service: Μόλις ένα προσβεβλημένο αρχείο τρέχει σε ένα σύστημα από ένα χρήστη με τοπικά διαχειριστικά δικαιώματα, θα εγκαθιστήσει μία υπηρεσία που ονομάζεται "Remote Explorer". Όταν γίνει υπηρεσία του συστήματος μπορεί να τρέξει ακόμα και όταν ο χρήστης κάνει log off από τη κονσόλα. Όταν τρέχει, θα προσπαθήσει προσβάλει και άλλα αρχεία στο σύστημα και να καταστρέφει δεδομένα. Η υπηρεσία θα περιμένει ένα χρήστη με δικτυακά διαχειριστικά δικαιώματα να κάνει log on στο σύστημα. Μόλις συμβεί αυτό θα προσπαθήσει να συνδεθεί με άλλα συστήματα στο δίκτυο τα domain administrative πιστοποιητικά του χρήστη για εγκαταστήσει τον εαυτό του σε απομακρυσμένα συστήματα.

Για να ελέγξει κάποιος χρήστης αν έχει προσβληθεί θα πρέπει από το Control Panel/ Services να δει αν έχει εγκατασταθεί ο "Remote Explorer".

Summary

The Microsoft Security advisor site is where the organization posts bulletins about any secyrity issues relating to Microsoft products. Anyone can find whitepapers on security, the latest news about Microsoft and information on its products and features and about the technology they use.

Βιβλιογραφια

Η εργασία στηρίχτηκε αποκλειστικά σε πηγές από το διαδίκτυο

hhtp://www.microsoft.com../misc/privacy_security.htm
hhtp://www.microsoft.com../security/bulletins/ms98-001.asp
hhtp://www.microsoft.com../security/bulletins/ms98-002.asp
hhtp://www.microsoft.com../security/bulletins/ms98-003.asp
hhtp://www.microsoft.com../security/bulletins/ms98-004.asp
hhtp://www.microsoft.com../security/bulletins/ms98-005.asp
hhtp://www.microsoft.com../security/bulletins/ms98-006.asp
hhtp://www.microsoft.com../security/bulletins/ms98-007.asp
hhtp://www.microsoft.com../security/bulletins/ms98-008.asp
hhtp://www.microsoft.com../security/bulletins/ms98-009.asp
hhtp://www.microsoft.com../security/bulletins/ms98-010.asp
hhtp://www.microsoft.com../security/bulletins/ms98-011.asp
hhtp://www.microsoft.com../security/bulletins/ms98-013.asp
hhtp://www.microsoft.com../security/bulletins/ms98-015.asp
hhtp://www.microsoft.com../security/bulletins/ms98-016.asp
hhtp://www.microsoft.com../security/bulletins/ms98-017.asp
hhtp://www.microsoft.com../security/bulletins/ms98-018.asp
hhtp://www.microsoft.com../security/bulletins/ms98-019.asp
hhtp://www.microsoft.com../security/bulletins/ms98-020.asp

hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=11
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=12
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=13
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=14
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=15
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=16
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=17
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=18
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=19
hhtp://www.microsoft.com../security/products/sna.asp?Parent=3&ID=50
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=21
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=22
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=23
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=24
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=25
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=26
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=27
hhtp://www.microsoft.com../security/..nticode/default.asp?Parent=4&ID=28