Banyan VINES und Sicherheit

Das **VI**rtual **NE**working **S**ystem der Firma Banyan (**VINES**) ist ständigen Anpassungen an die Trends des Networking unterworfen, welche dessen Sicherheit entsprechend der gewählten Wege negativ oder positiv beeinflußt. Unter dem Oberbegiff Sicherheit von VINES sollen hauptsächlich Verfügbarkeit, Datenintegrität und Vertraulichkeit zusammengefaßt sein. Diese Eigenschaften betrachten wir nur bezüglich der Netzressourcen des VINES, wie z. B. Netzwerkdienste, StreetTalk-Listen und User-Accounts. Die Sicherheit der lokalen Ressourcen eines Netzwerk-Clients (PC, Mac oder UNIX) ist maximal so groß, wie es das auf ihm laufende Betriebssystem (DOS, OS/2, Windows 95, Windows NT, MacOS oder UNIX) zuläßt und wird deshalb in diesem Artikel nicht behandelt.

Kein Netzwerkbetriebssystem ist sicher, wenn die Netzwerkverantwortlichen und die Benutzer die Sicherheitsmöglichkeiten nicht sinnvoll verwenden. Deshalb ist der Gegenstand dieses Artikels – neben der Auflistung der Sicherheitsmechanismen des VINES – deren sinnvolle Nutzung und Ergänzung. Die Sicherheitsmechanismen wollen wir in folgende Gruppen unterteilen: Server/Backup, Account, Filedienst, Druckdienst, Maildienst und SMTP-Gateway.

Zur Sicherheit der VINES-Server/Backups sollte folgendes gewährleistet sein:

- Zutritt (Datennetzanschluß, Stromanschluss, Klimatisierung, Server-Hardware, Server-Console) auf kleine kompetente und verfügbare Personenkreise beschränken,
- Server-Console durch geeignetes Paßwort schützen,
- Remote-Console nur nutzen, wenn sicher ist, daß kein anderer sie parallel nutzt und keine laufenden Prozesse gestört werden (z. B. Backup),
- regelmäßige (z. B. tägliche) Sicherung der Daten der Server,
- Protokollierung der Backups nach Servername mit Datenträgerkennung, Erstellungsdatum, Art des Backups, Erfolg des Lesetests und verantwortliche Person (Verwaltung mehrerer Generationen von Sicherheitskopien),
- technische Daten des Backupgerätes, VINES-Version und Patch-Geschichte jedes Servers müssen bekannt sein (Kompatibilitätsproblem),
- Backups und Protokolle räumlich getrennt von Servern sicher vor unbefugtem Zugriff und physischer Zerstörung aufbewahren,
- Betreiben der VINES-Server über eine unabhängige Stromversorgung,
- Verwendung möglichst ausfallsicherer Hardwarekomponenten,
- Schutz der Server vor Verschmutzung, Feuchtigkeit und Überhitzung,
- sichere Verwahrung der Serverkeys und Softwareoptionen,
- regelmäßige Überprüfung der Serverressourcenauslastung (EVS-Service, MNET) und
- Beschränkung der Server Access Möglichkeiten (PC Dial-In, serielle Server to Server Verbindungen, Server to Server IP, Intranet Connect, User Login Locations, Access to UNIX).

Vertraulichkeit der Accounts

Die Vertraulichkeit der Accounts ist neben der Server/Backup-Sicherheit die wesentliche Basis für die Funktion aller anderen Sicherheitsmechanismen des VINES. Zur Sicherheit der Accounts von Nutzergruppen und/oder individuellen Nutzern bietet VINES folgende Möglichkeiten (MGROUP, MUSER):

- Paßwort [Mindestlänge und Lebensdauer kann vorgegeben werden; neues Paßwort muß sich von den letzten 10 Paßwörtern des Nutzers unterscheiden; Paßwortübertragung erfolgt immer verschlüsselt; nach drei vergeblichen Loginversuchen muß Client erneut gebootet werden; leider kann Nutzer nicht gezwungen werden, Sonderzeichen und/oder Ziffern zu verwenden; Ändern des eigenen Paßworts kann verhindert werden (eventuell für Nutzer, die zu „primitiven“ Paßwörtern neigen)]
- maximale Anzahl paralleler Sitzungen jedes Accounts festlegbar
- Client-Arten einschränkbar (DOS, OS/2, Mac)
- Login-Standorte einschränkbar (Server; Serverinterface; Netzkartenadresse des Clients)
- Login-Zeiten für jeden Tag der Woche separat festlegbar
- Editieren des eigenen Nutzerprofiles kann und sollte für die meisten Nutzer verhindert werden
- hierarchischer Profileaufbau möglich und empfehlenswert (USE)
- Lebensdauer eines Accounts kann auf ein konkretes Datum beschränkt werden (z. Z. Problem bei Datum ab 1.1.2000, da Jahrhunderte nicht abgefragt werden)
- Account kann zeitweilig (z. B. längere Zeit abwesende Nutzer) oder ständig (z. B. Sample Profile) disabled sein
  [Die bisher aufgelisteten Sicherheitsfestlegungen für Accounts können nur die Administratoren der entsprechenden Gruppe (enthalten in der Liste „AdminList@... “ der Gruppe) setzen.]
- Beschränkung der PC Dial-In (OPERATE) und Banyan Intranet Connect Zugänge auf kleine Nutzerkreise (vergleichbare Beschränkung der IP-Clients ist

z. Z. nicht realisiert - notfalls muß Login-Standort eingeschränkt werden)
- Vertretung ohne Accountfreigabe für andere Personen möglich (automatische Mailweiterleitung, gemeinsame Datenbestände auf Netzwerkplatten, ...).

Nutzerverhalten zur Wahrung der Vertraulichkeit seiner Accounts:

- Ungenutzte Accounts sind häufig leicht zu knacken, da der Hacker viel Zeit dazu hat, ohne in große Gefahr zu geraten, aufzufallen. Außerdem ist mit hoher Wahrscheinlichkeit ein recht einfaches Anfangspaßwort vergeben worden. Deshalb sollten nur die Nutzer einen Account bekommen, die diesen sofort nutzen wollen.
- Festlegung eines hinreichend langen (mindestens sechs Zeichen), hinreichend komplizierten (Sonderzeichen, Ziffern, Groß-/Kleinschreibung, ...) und mit dem Nutzer schwer in Zusammenhang zu bringenden Paßworts durch den Nutzer selbst,
- sichere Aufbewahrung des Paßworts (besser nur im Gedächtnis),
- Verwendung des Paßworts möglichst nicht im Beisein anderer Personen und nur in sicheren Bereichen,
- Sicherstellung, daß keine Pseudo-Login-Routinen im Netzwerk existieren (Vorsicht beim Einloggen über einen fremden Client),
- Änderung des Paßworts, sobald der Verdacht besteht, daß ein Unberechtigter in Besitz des Paßworts gelangt ist (Login hat nicht funktioniert, obwohl man sich sicher ist, alles richtig eingegeben zu haben; Zeit des letzten Logins ist falsch; Daten, die nur dieser Account ändern kann, sind unerwartet geändert; man ist beim Einloggen eventuell beobachtet worden; Login nicht mehr möglich – sofort Administrator informieren; Lebensdauer des Paßworts ist abgelaufen; ...),
- Sicherung der Vertretbarkeit durch geeignete Daten-, Software- und Dienstzugriffsrechte sowie Mailumleitung (Vertretbarkeit muß unabhängig von persönlichen Accounts sichergestellt sein),
- auch die Administratoren sollten die Paßwörter ihrer Nutzer nicht kennen – Nutzer zwingen, sein Paßwort beim ersten Login zu ändern!

Sicherheit von Netzdiensten

Die Sicherheit der Netzdienste ist maximal so hoch wie die Vertraulichkeit der zugriffsberechtigten Accounts und die Sicherheit zugehöriger Server und Backups. Deshalb sollten nur die für die Realisierung der Arbeitsaufgaben notwendigen Rechte gefordert und bereitgestellt werden (je mehr Nutzer eine bestimmte Netzressource nutzen dürfen, je geringer ist deren Sicherheit).

Sicherheit von VINES-Filediensten (SETARL; ATTRIB; SETATTR):

- Jedem Verzeichnis und jedem File ist eine spezifische Access Right List (ARL) zugeordnet.
  - Zu beachten sind unterschiedliche Rechtarten und Vererbungsregeln aus „VINES-Sicht“ (DOS, Windows, OS/2) und Mac-Sicht.
  - Weiterhin ist eine Rangfolge zu beachten, falls ein Account in mehreren Berechtigtengruppen der ARL eines Verzeichnissen oder einer Datei auftritt (*Owner* > *Username* > *Group* > *StreetTalk-Liste*= *Gruppenmaske* > *Organisationsmaske* > *World*).
  - Die ARLs eines Filedienstes sind schwer auf einem konsistenten und sicheren Stand zu halten.
    . Usernamen sollten nur in Ausnahmefällen explizit auftreten (außer als Owner),
    . Masken sollten vermieden werden (auch in StreetTalk-Listen, die in ARLs auftreten),
    . *World* sollte maximal Leserecht haben (meistens aber keinerlei Rechte),
    . das Recht, Rechte zu ändern, sollte nur in begründeten Ausnahmefällen vom Filediensverantwortlichen (Owner) delegiert werden.
- Jedem File sind neben den normalen DOS-Attributen 2 VINES-Attribute zuordenbar (Sharing und Execute Only Attribut) die parallele Nutzung und Lizenzschutz von Softwareinstallationen unterstützen.
- Die Speicherkontingentierung der Nutzer ist nur über Drittherstellersoftware möglich.
- Nur reine Bootsektorviren sind nicht verbreitbar.

Sicherheit von Druckdiensten (MSERVICE; SETPRINT; PCPRINT)

Standardmäßig wird bei der Definition eines neuen Druckdienstes die Nutzung nicht eingeschränkt (*@*@*), was aus Sicherheitssicht sehr problematisch ist – absichtliches Blockieren von Druckdiensten, Drucken von vertraulichen Daten auf falschem Drucker. Günstig ist, wenn an Stelle der World-Maske ein spezieller Listenname eingetragen wird. In dieser StreetTalk-Liste werden die Nutzungsberechtigten des Druckdienstes eingetragen.

Zur Unterstützung der Administratoren können weitere Operator (Nutzer) für Druckdienste festgelegt werden, die dadurch einige Managementaufgaben realisieren können.

PC-Print-Drucker sollten nur von einem kleinen Nutzerkreis (besser speziellem User mit maximaler Loginplatzbeschränkung) startbar sein, da jeder VINES-Nutzer, der einen Drucker an seinem PC hat, in wenigen Minuten jeden beliebigen ungeschützten PC-Print-Druckdienst auf seinen Drucker ausdrucken lassen könnte und so unbefugt an vertrauliche Daten gelangen würde. Startberechtigte Nutzer werden über das Feld „PCPRINT ST namen:“ bei der Destinationdefinition festgelegt.

Sicherheit von VINES-Maildiensten (SETMAIL; MMAIL; MAIL)

Problematisches:

- Das „unberechtigte“ Anlegen von Mailboxen kann nicht verhindert werden.
- Für Maildienste mit mehr als etwa 250 Mailboxen ist es mit normalen VINES-Mitteln nicht mehr möglich, eine Maildienststatistik zu generieren – ermöglicht Mißbrauch der Mailboxen als Datenspeicher (z. B. falls Plattenkontingent des entsprechenden Nutzers ausgeschöpft ist).
- Es gibt kein Tool, mit dem man sich die Mailboxsettings aller Nutzer geschlossen anzeigen lassen kann (Verhindern von an *@*@* adressierter Mail).
- Es gibt kein Tool, das ab einem gewissen Füllstand der Mailbox den entsprechenden Nutzer automatisch warnt.
- Es besteht die Gefahr der Virenverbreitung durch Mailverkehr.
- Mail, die aus dem Internet kommt oder in dieses geht, kann mit der im Internet üblichen Software leicht mitgelesen (protokolliert) und eventuell sogar gefälscht werden.

Unproblematisches:

- Man kommt nur über den entsprechenden Nutzer-Account an den Inhalt der Mailbox des Nutzers.
- Mailboxen werden in der Regel nur auf Servern gehalten – neuere Entwicklungen, wie Beyond Mail 3.0 lassen auch lokal gespeicherte Mailboxen zu (Sicherheit wird reduziert).
- Ein Maildienstadministrator ist nicht in der Lage, an fremde Mailinhalte zu kommen – nur einige Headerinformationen, die die Adressierung betreffen sind ihm zugänglich.

Sicherheit des iSMTP-Gateways:

Die Nutzer und die Administratoren der Gruppe, zu welcher der DOS-UNIX-Bridge-Filedienst des Gatewayservers gehört, können Mailinformationen während der Verarbeitung der entsprechenden Mails durch das Gateway lesen und modifizieren – Sicherheit ist vergleichbar mit der Mailsoftware des Internet. In der genannten StreetTalk-Gruppe sollte nur ein Nutzer existieren, der zugleich zu den Admins der Gruppe gehört.

Literaturverweise:

- Managing VINES Security (CD: Banyan Documentation StreetTalk for Windows NT 7.5 and VINES 7.x)
- Monitoring and Optimizing a VINES Network
- VINES Command Reference
- Managing VINES Services
- Managing VINES Workstations
- Operating a VINES Server
- Intelligent Messaging Mail Administrator’s Guide
- Banyan Intranet Connect

Michael Sommerfeld