

White Paper

asbLANtools[®]

Sicherheitsdokumentation von Microsoft Windows Netzwerken™



Dieses Dokument dient ausschließlich zu Informationszwecken. Die getroffenen Aussagen zu den Produkten stellen keine Garantien dar.

© 1995 – 2009 **asb Systemhaus**
Alle Rechte vorbehalten.

Die verwendeten Microsoft Warenzeichen sind eingetragene Warenzeichen der Microsoft Corporation. Andere aufgeführte Logos und Produkt-/Firmennamen sind Eigentum der jeweils aufgeführten Hersteller.

asb Systemhaus GmbH

Motzstraße 1
D-99094 Erfurt
Germany

Tel: +49 (361) 66 4 77-0

Fax: +49 (361) 66 4 77-21

E-Mail: info@asb-systemhaus.de

Internet: www.asb-systemhaus.de

asbLANtools® und asb Marken-
zeichen sind registrierte Waren-
zeichen der asb Systemhaus GmbH.

Dokumentationsstand: 01.06.2009

Inhaltsverzeichnis

1. Vorwort.....	4
2. Windows Sicherheit, ACL Objektlisten.....	5
2.1 Generelles, Windows Systemunterschiede.....	5
2.2 Zugriff auf Objekte.....	6
2.3 Identifikation eines Objektes	7
2.3 Sicherheitskennungen eines Objektes.....	7
2.3.1 Besitzerkennung.....	7
2.3.2 Gruppen-Kennung.....	8
2.3.3 Zugriffskontrollliste	8
2.3.4 Überwachungsliste.....	8
2.4 Zugriffskontrolllisten - ACL	9
2.4.1 Genereller Aufbau:	9
2.4.2 Zugriffskontrolleinträge - ACE	9
2.5 Vererbung.....	11
2.5.1 Wie wird vererbt?	11
2.6 Überprüfung von Berechtigungen.....	12
2.6.1 Objektzugriff anfordern	12
2.6.2 Effektive Rechte	13
2.7 Rangfolge von Berechtigungen.....	14
3. Allgemeine Produktbeschreibung.....	16
3.1 Konzept der Software	16
3.1.1 Warum Analyse und Dokumentation und nicht aktive Administration?	16
3.1.2 Konventionelle Dokumentation von zugewiesenen Rechten.....	16
3.1.3 Datenschutz, Datensicherheit und aktuelle Rechtssprechung.....	17
3.1.4 Zielstellung der Software asbLANtools®.....	17
3.1.5 Authentische Analysen	18
3.1.6 Die Arbeitsweise mit asbLANtools	18
3.1.7 Informationsbestandteile in der Version 2.8	19
3.2 asbLANtools anwenden.....	20
3.3 Versionspezifikation	22
3.4 Produktnutzen	22
3.4.1 .. für den Anwender	22
3.4.2 .. für das Unternehmen.....	23
4. Technische Produktbeschreibung asbLANtools	25
4.1 Komponenten.....	25
4.2 Arbeitsweise	28
4.2.1 Datenerfassung	28
4.2.2 Datenauswertung.....	29
4.2.3 Versionsmanagement.....	29
4.2.3 Reporting	29
4.2.4 Datenbanksystem und Schnittstellen.....	29
5. Lizenzierung.....	30
6. Übersicht Technische Spezifikation	30

1. Vorwort

Das vorliegende Dokument gibt einen Einblick in die Arbeitsweise und Anwendungsmöglichkeiten der Software **asbLANtools® in der Version 2.8.**

Bei weitergehenden Fragen, technischen Details, Fragen der Evaluierung, Lizenzierung oder Optionsvergleich zu anderen Produkten wenden Sie sich bitte direkt an den Vertrieb unter:

asb Systemhaus GmbH
Motzstraße 1
D- 99094 Erfurt
Tel. +49(361) 66477-51
Fax: +49(361) 66477-21
E-Mail: vertrieb@asb-systemhaus.de

2. Windows Sicherheit, ACL Objektlisten

2.1 Generelles, Windows Systemunterschiede

Die Anwendung der asbLANtools unterscheidet sich mit dem Einsatz der unterschiedlichen Windows Versionen. Ebenso können Unterschiede durch einzelne Servicepacks in den MS internen Sicherheitsfunktionen Auswirkungen auf die Auswertung durch asbLANtools finden. Wesentliche Änderungen im Security-Kernel wurden so beispielsweise durch MS zwischen für Windows NT von SP4 nach SP6 sowie Windows 2000 mit SP2 und SP4 (Vorbereitung 2003) vorgenommen.

Folgende Grundkonfigurationen sind bei Anwendung von asbLANtools zu betrachten:

- Windows NT4 Domäne
- Windows 2000 bzw. 2003 Mixed Mode Domäne
- Windows 2000 bzw. 2003 Native Mode Domäne
- Multidomänen-Netzwerk
- Gemischte Domänenumgebungen

asbLANtools sind grundsätzlich in diesen Umgebungen verwendbar und erfassen die im DB-Modell von asbLANtools vorgesehene Informationen. Im konkreten Applikationsfall können jedoch Besonderheiten auftreten, wie 2003-AD in einer W2k Umgebung, die individuell berücksichtigt werden müssen.

Stabilitätsbetrachtung zu asbLANtools

asbLANtools ist ein technologisch aufwendiges und kompliziertes System, das der MS NT/2000 Welt Rechnung trägt. Trotz aller Bemühungen kann es zu nicht bekannten, neuen Problemen kommen, welche z.B. durch zukünftige Ausgaben von MS Servicepacks oder anderen Anbietern von Software entstehen hervorgerufen werden, oder noch unbekannte "Konstellationen" entstehen.

Bekannte Probleme in W2k Netzen (mixed und native Mode) werden durch eine unsaubere Migration von NT nach W2K hervorgerufen.

asbLANtools und Windows 2000 arbeiten intern mit einem eindeutigen SID / UUID / GUID Bezug.

Durch die "unsaubere" Migration können beispielsweise Probleme in den Namenskonventionen von Konten (Accounts) auftreten. Diese haben Ihre eigentliche Ursache in der unsauberen Implementierung / Behandlung sensitiver / nichtsensitiver Objekte in MS Windows 2000. MS Zugriffstechnologien (in NT und ADSI erkennen dies selbst nicht). Erst durch LDAP können diese Probleme in einer zukünftigen asbLANtools Version beseitigt werden (LDAP wird in asbLANtools nur ab Windows 2000 unterstützt).

Doppelte (namensgleiche) Accounts, sind durch den Administrator in Windows 2000 zu entfernen. asbLANtools meldet diese, kann jedoch die Informationen dieser Accounts nicht eindeutig zuordnen und auswerten.

(Als doppelte Accounts werden Accounts mit unterschiedlicher UUID aber gleichen Namenszeichnung bezeichnet/ gefunden (Sensitivitätsproblem)
Beispiel Maschine "test" und "TEST", oder Gruppe "fibu" und "Fibu",..).



Der saubere Weg der Migration ist immer die Neuinstallation der Domäne.

Migrationsprobleme können auch durch einen frühzeitigen Einsatz von asbLANtools erkannt und beseitigt werden, indem zu migrierende Systeme vorab analysiert und dann gesäubert werden.

Insbesondere werden von asbLANtools unter W2K die

- Geschachtelte Gruppen
- Universal Groups
- Organisation Units

erfasst und behandelt und mittels asbLANtools Viewer visualisiert.

Zum Verständnis der Software asbLANtools ist erforderlich, einen "Ausflug" in die Grundlagen der Sicherheit von Informationen von Windows NT/ 2000 zu machen. Nur mit dem Verständnis dieser Grundlagen werden Sie auch asbLANtools richtig und nutzbringend anwenden können.

Die Aussagen zu Zugriffsrechten in NTFS sind nicht weniger komplex als Betrachtungen zu "politischen Aussagen" im täglichen Leben. Insbesondere der Begriff der Effektiven Rechte bedarf einiger besonderer Betrachtungen.

Als effektive Rechte wird das jeweils "resultierende" Zugriffsrecht eines Benutzers zum Zeitpunkt X am Standort Y über den Weg Z auf das Objekt A bezeichnet.

Ein effektives Recht wird somit nur als Näherung durch Gruppenmitgliedschaft eines Benutzers und der ACL Berechtigungslisten auf ein Objekt beschrieben.

In den Unterlagen zu Windows 2000 /2003 (Onlinehelp) findet man dazu den Hinweis, dass effektive Rechte zu keinem Zeitpunkt eineindeutig sind.

Dieser Umstand kann nur dadurch gemildert werden, dass zu den betrachteten Objekten möglichst alle Informationen transparent vorliegen.

Das ist die eigentliche Zielstellung von asbLANtools, die Wertung der Informationen ist oftmals kompliziert und bedarf der nachfolgenden Kenntnisse unabdingbar.

2.2 Zugriff auf Objekte

Das Betriebssystem behandelt alle Komponenten als Objekte. Zu diesen Objekten zählen u.a.

Dateien, Geräte, Drucker, Dienste, Prozesse, Threads, Mailslots, Pipes, Ereignisse, Mutexe, Semaphoren, Timer, Arbeitsstationen, Desktops, Freigaben und Registry-Schlüssel. Spezielle Objekte wie Verzeichnisse können andere Objekte enthalten und werden damit als Container bezeichnet. Container haben also über Objekte hinausgehende Eigenschaften.

Der Zugriff auf Objekte unter Windows NT/2000™ wird durch Systemschnittstellen des Betriebssystems angefordert. Nach der Anmeldung eines Benutzers läuft

für diesen ein Prozess auf dem System. Dieses Prozess-Objekt wurde durch die Anmeldung im Kontext des Benutzers erzeugt. Es besitzt alle Rechte des Benutzers.

Möchte der Benutzer nun eine Datei öffnen, so ruft dieses Prozess-Objekt eine Systemfunktion (hier z.B. OpenFile) auf. Das System überprüft nun, ob die Anforderung "Datei zum Lesen öffnen" im Kontext dieses Benutzers (Prozesses) gewährt werden kann oder nicht. Möchte der Benutzer eine neue Datei (ein Objekt) anlegen, so überprüft das System, ob der Kontext dieses Benutzers es erlaubt, im ausgewählten Verzeichnis (Container) ein neues Objekt anzulegen.

Abstrakt kann ein solcher Vorgang als Zugriffsanforderung eines Objektes auf ein anderes Objekt beschrieben werden, wobei der geforderte Zugriff genau angegeben wird (z.B. Lesezugriff auf eine Datei, Anlegen eines neuen Verzeichnisses). Der Schutz von Objekten bildet den Kern der Zugriffssteuerung unter Windows NT™. Im Systemkern gibt es genau eine Funktion der Zugriffssteuerung, welche beim ersten Zugriff auf Objekte die angeforderten Rechte überprüft. Diese Zentralisierung gewährt eine einheitliche und sichere Funktion des Betriebssystems.

2.3 Identifikation eines Objektes

Um zu kontrollieren, wer ein Objekt manipulieren darf, muss das Sicherheitssystem die Identität des Benutzers kennen. Um dieses zu garantieren, wird jeder Benutzer zu einer Anmeldung mit Namen und Kennwort gezwungen. Die nach der Anmeldung erzeugte Sitzung enthält so genannte Zugriffsschlüssel (Access-Tokens), also eine Art Schlüsselbund, mit denen sich Zugang zu den verschiedensten Objekten verschafft werden kann.

Jeder Schlüssel und auch jedes Schloss enthält eine Sicherheits-Kennung (Security Identifier; SID), durch welche eindeutig Benutzer, Benutzergruppen und andere Zugriffskonten identifiziert werden können. Diese Informationen werden als Kontext des Benutzers bezeichnet.

In einem Netzwerk muss es somit mindestens eine Stelle geben, welche Anmeldungen von Nutzern überprüfen kann. Macht das jede Arbeitsstation für sich, so entspricht dies dem Arbeitsgruppenmodell. In einer Windows Domäne werden Anmeldungen zentral durch die Domain-Controller überprüft. Die Delegation der lokalen Überprüfung an die Domäne wird durch die Mitgliedschaft des Computers in der Domäne oder durch Vertrauensstellungen zwischen Domänen möglich. In Windows 2000 werden diese NTLM-Mechanismen durch die Verwendung von Kerberos erweitert.

Nach einer erfolgreichen Anmeldung gibt es immer einen interaktiven "Sitzungs-Prozess, welcher über den Kontext des Benutzers verfügt. Der Access-Token enthält alle Benutzerrechte (z.B. "darf Besitz von Objekten übernehmen"), alle Kennungen (SID) von Gruppen, in denen der Benutzer Mitglied ist etc.

2.3 Sicherheitskennungen eines Objektes

Vergleichbar mit dem Schlüsselbund des Benutzers ist jedes Objekt mit verschiedenen "Schlössern" ausgestattet. Hat ein Benutzer einen passenden Schlüssel, so wird ihm der Zugriff auf bestimmte Funktionen und Eigenschaften des Objektes gewährt.

Diese Sicherheitsbeschreibung oder besser Sicherheits-Kennungen (Security Descriptor, SD) enthält folgende Komponenten:

2.3.1 Besitzerkennung

Die Besitzererkennung enthält den SID des Eigentümers des Objektes. Der Eigentümer ist mit dem Erzeugen des Objektes festgelegt. Dem Besitzer eines Objektes werden immer automatisch Rechte zur Veränderung der Zugriffsrechte eingeräumt (WRITE_DAC und READ_CONTROL). Er entscheidet somit allein, wer auf seine Daten zugreifen kann.



Besitzerrechte werden "lebenslang" beibehalten. Der Eigentümer ist somit jederzeit in der Lage die Zugriffsrechte seines "Besitzes" zu bestimmen (ändern)

Gibt er dieses Recht weiter (P = Berechtigungen verändern), so kann er als Eigentümer grundsätzlich immer noch die Rechte verändern.

Ein Besitzer eines Objektes kann anderen das Recht (O = Besitz aneignen) gewähren, sich dieses Objekt anzueignen.

Nur ein Benutzer mit dem Inbesitznahme-Privileg (SeTakeOwnership Privileg) kann sich ohne Willen des Eigentümers fremde Objekte aneignen. Besitzrechte können nicht weitergegeben werden, so dass damit immer Enteignungen nachweisbar bleiben.

2.3.2 Gruppen-Kennung

Die Gruppen-Kennung wird nur vom POSIX-Subsystem verwendet und spielt für den normalen Betrieb eine untergeordnete Rolle.

2.3.3 Zugriffskontrollliste

Die Sicherheitskennungen eines Objektes kann eine Zugriffskontrollliste (DACL) enthalten, welche explizit Rechte zum Zugriff auf dieses Objekt definiert. Auf Objekte ohne eine Zugriffskontrollliste haben alle Benutzer volle Zugriffsrechte - das Objekt ist somit nicht geschützt.

Versucht ein Benutzer, auf ein Objekt zuzugreifen, so wird sein Kontext gegen die Kennungen der Überwachungsliste geprüft. Die Arbeitsweise dieser Zugriffskontrolllisten wird im Punkt 0 genauer dargestellt.

2.3.4 Überwachungsliste

Im Weiteren können die Sicherheitskennungen (SD) eines Objektes eine Überwachungsliste (SACL) enthalten. Um den Vergleich zu vervollständigen - die Überwachungsliste ist die Alarmanlage für Objekte.

Versucht ein Benutzer, auf ein Objekt zuzugreifen, so wird sein Kontext gegen die Kennungen der Überwachungsliste geprüft. Gibt es eine Übereinstimmung, und entsprechen die geforderten Zugriffsrechte in Teilen den zu überwachenden Rechten, wird dieser Zugriffsversuch protokolliert.

Die Mechanismen der Überprüfungen sind bei DACL und SACL gleich. Eine Überprüfung liefert immer einen logischen Wert, welcher bei der DACL den Zugriff gewährt und bei der SACL die Protokollierung steuert.

Die Überwachung ist nicht das Thema dieses Kapitels und bleibt hier unberücksichtigt. Die folgenden Abschnitte können sinngemäß auch auf die SACL angewendet werden.

2.4 Zugriffskontrolllisten - ACL

2.4.1 Genereller Aufbau:

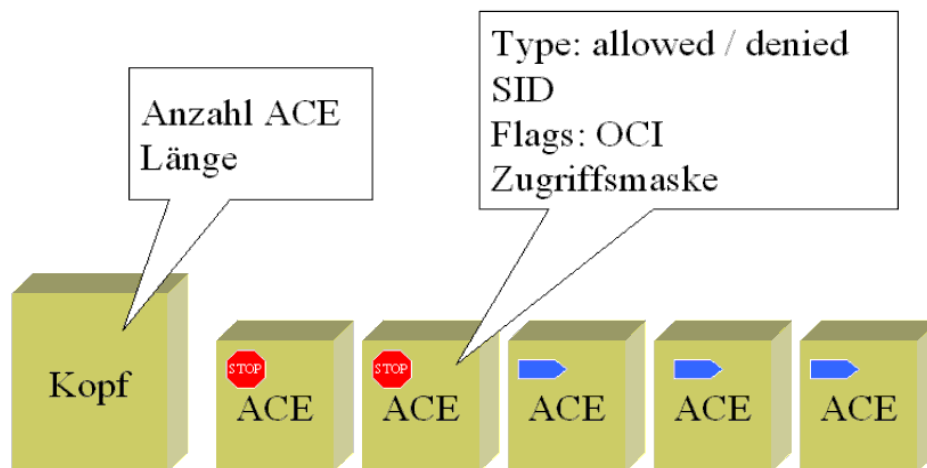


Abbildung 0.1: Der Aufbau einer Zugriffskontrollliste (ACL)

Jede Liste besitzt einen Kopf und Einträge.

Eine Liste ohne Header wird „NULL-DACL“ genannt. Eine NULL-ACL gewährleistet „volle“ Zugriffsrechte für alle Benutzer, während eine „Empty-DACL“ (Alle Zugriffsprüfungen werden negativ beschiedet) jegliche Zugriffe verbietet. Ein Anwender kann leider mit Boardmitteln nicht entscheiden, welcher Zustand vorliegt, wenn er feststellt, dass zu einem ACL-Eintrag keine Berechtigungen eingestellt sind.

Zugriffslisten können in 2 Speicherformaten gespeichert werden. Das absolute Format enthält absolute Adressen auf die Komponenten, das relative Format nur Offsets. Das relative Format eignet sich gut zur Speicherung im Dateisystem oder anderen Medien. Für die Funktionsweise spielen die Speicherformate keine Rolle und bleiben weiterhin unberücksichtigt.

Jeder Eintrag der Zugriffskontrollliste - Zugriffskontrolleintrag (ACE) - definiert gewährte oder untersagte Rechte für bestimmte Benutzerkennungen (SID). Versucht ein Benutzer, auf ein Objekt zuzugreifen, so wird sein Kontext gegen die Kennungen der Überwachungsliste geprüft. Werden alle geforderten Rechte gewährt und nicht untersagt, so erhält der Benutzer den Zugriff auf dieses Objekt.

2.4.2 Zugriffskontrolleinträge - ACE

Jeder Eintrag besitzt eine Position, Flags, einen Typ, eine Kennung (SID) und eine Zugriffsmaske. Durch die Reihenfolge in der Liste wird die Position der ACE bestimmt. Diese Ordnung bestimmt die Sequenz der Überprüfung und ist somit wichtig.

Die Flags des ACE enthalten die Vererbungsinformationen. ACEs, welche nur als Vorlage für neue Objekte dienen, müssen bei der Überprüfung der Zugriffsrechte nicht berücksichtigt werden. Die Vererbung wird genauer im Abschnitt 0 beschrieben.

Der Typ unterscheidet zwischen AccessAllowed oder AccessDenied. Ein AccessAllowed-ACE gewährt Rechte, der AccessDenied-ACE untersagt Rechte.

Der SID des ACE legt fest, für wen die Rechte dieses Eintrages gewährt oder verboten werden. Der SID wird gegen den Benutzer-Kontext geprüft, d.h. ob dieser SID im Access-Token des Prozesses vorhanden ist (Hier stehen, wie oben bereits genannt, alle SID der Gruppen, in denen der Benutzer Mitglied ist, etc.). Über den SID des ACE wird somit entschieden, ob dieser ACE für die Überprüfung der Zugriffsrechte verwendet wird oder nicht.

Die Zugriffsmaske (AccessMask) legt gewährte und untersagte Rechte fest. Sie ist ein 32-Bit Wort und wie folgt aufgebaut:

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
G	G	G	G	Reserved				A	Standard Access Rights				Object-Specific Access Rights																		
R	W	E	A					S																							

GR	-->	Generic_Read
GW	-->	Generic_Write
GE	-->	Generic_Execute
GA	-->	Generic_ALL
AS	-->	Right to access SACL

Abbildung 0.2: Der Aufbau der Access Maske

Generische Rechte

Generische Rechte sind allgemein definierte Rechte. GENERIC_ALL steht für Vollzugriff.

Generische Rechte gewähren außer GENERIC_ALL keine Rechte, sondern sind eine Vorlage für die Vererbung von Rechten auf neu angelegte Objekte und somit nur in Containern von Bedeutung. Während der Vererbung müssen damit die generischen Rechte auf Standardrechte und spezifische Rechte umgerechnet werden.

Standardrechte

Standardrechte sind Rechte, die auf alle Objekte zutreffen:

Delete, Write_DACL, Read_Control, Write_Owner, ...

Spezifische Rechte

Spezifische Rechte gelten für spezielle Objekte. Die Interpretation ist stark vom Objekt abhängig.

Beispiel:

0x0001 erlaubt:

- in Dateien Daten zu lesen
- Verzeichnisse auszulisten

0x0002 erlaubt:

- in Dateien zu schreiben
- in Verzeichnissen neue Dateien anzulegen

Die im NTFS bekannte Anzeige der Rechte als RWXDPO stellt die Informationen der AccessMask nur komprimiert - aber praktisch ausreichend dar. Mit der Festlegung von etwa 20 einzelnen atomaren Rechten wäre jeder Administrator überfordert. Das ist noch nicht alles! Für Container-Objekte lassen sich zusätzlich noch die Vorlagen-Rechte für neue Container und neue Objekte angeben.

2.5 Vererbung

Stellen Sie sich vor, sie müssten für jede neue Datei die Zugriffsrechte komplett eingeben!

Die praktisch beste Lösung bietet das Konzept der Vererbung der Rechte des Containers auf neue Objekte. Eine einfache Kopie der DACL könnte zwischen Eltern-Container und neuem Container verwendet werden. Eine Kopie der DACL von einem Container auf ein Objekt ist nicht möglich, wenn das Objekt eine andere Rechtestruktur hat.

Der Container muss somit Vorlagen für neue Container und Objekte bereitstellen. Jeder ACE der Zugriffsliste kann als Vorlage für Container (C = CONTAINER_INHERIT) und/oder Vorlage für Objekte (O = OBJECT_INHERIT) gekennzeichnet werden. Soll ein solcher ACE nicht für die Berechnung der Zugriffsrechte verwendet werden, so kann dieser als Vorlage (I = INHERIT_ONLY) gekennzeichnet werden. Die genannten Flags können in einer beliebigen Kombination auftreten: C, CI, CO, OI, COI.

Es existieren grundsätzliche Unterschiede in der Behandlung von ACE Einträgen in Windows NT /2000. Ebenso wird die Vererbung von Berechtigungen in Windows NT/2000 und 2003 unterschiedlich behandelt.

Windows NT:

Die Generierung der ACEs obliegt in Windows NT dem erzeugenden Programm. Die ACL eines Verzeichnisses kann einen unterschiedlichen Aufbau haben, abhängig, ob das Verzeichnis mit MKDIR, mit dem Dateimanager oder dem Windows Explorer erstellt wurde.

Windows 2000/2003:

Die Generierung der ACEs obliegt dem Systemkernel Funktionen.

Diese kontrollieren primäre Anforderungen und Regeln.

Für die Festlegung der Rechte für einen SID können 1 bis 3 ACE erzeugt werden. Diese Vielfalt der Darstellung der verkürzten Notation RWXDPO ist über MS Boardwerkzeuge (Dateimanager, Explorer, CACLS,..) nur eingeschränkt und ungenau möglich. Eine korrekte Anzeige und Dokumentation ist derzeit nur mit zusätzlichen Werkzeugen wie asbLANtools möglich.

2.5.1 Wie wird vererbt?

Folgende Abbildung zeigt die ACE eines Elterncontainers. Für die Vererbung der Rechte auf ein neues Objekt werden nur die ACE benötigt, welche als OBJECT_INHERIT gekennzeichnet sind. Diese ACE werden in die Zugriffsliste des neuen Objektes übernommen. Generische Rechte werden durch das Generic Mapping bei der Objekterstellung in Standard- und spezifische Rechte umgewandelt und alle Vererbungsflags gelöscht.

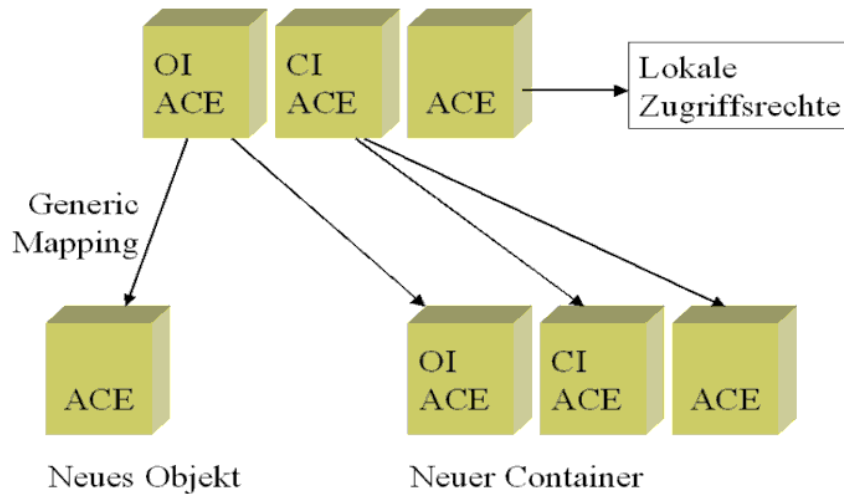


Abbildung 0.3: Die Vererbung von Rechten

Für neue Container werden alle Vorlagen (INHERIT_ONLY) kopiert. Zusätzlich wird, wie bei der Vererbung, auf Objekte der CONTAINER_INHERIT ACE über das Generic Mapping in einen einfachen ACE umgerechnet.

Vorlagen-ACE ohne INHERIT_ONLY Flag werden über das Generic Mapping umgerechnet, behalten aber die generischen Rechte und die Vererbungsinformationen.

Mit Windows 2000 stellt das Betriebssystem Schnittstellen bereit, welche die vielen Möglichkeiten durch einheitliche Algorithmen reduziert. Das gilt nicht nur für die Vererbung, sondern auch für die Reihenfolge der ACE, für welche es Richtlinien aber keine Kontrollen durch das Betriebssystem gibt.

2.6 Überprüfung von Berechtigungen

2.6.1 Objektzugriff anfordern

Dieser Algorithmus wird eingesetzt, um auf der Basis der Access-Token des Aufrufers zu bestimmen, ob eine bestimmte Zugriffsanforderung gestattet werden kann. Jede öffnende Funktion der Win32-API, die auf sichtbare Objekte angewendet wird, hat einen Parameter, der die gewünschte Zugriffsart angibt. Um festzustellen, ob der Aufrufer Zugriff hat, werden folgende Schritte ausgeführt:

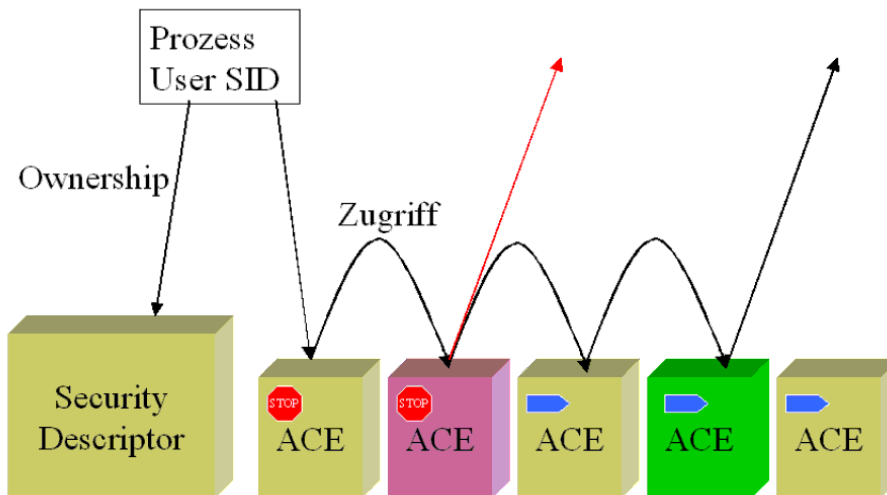


Abbildung 0.4: Die Überprüfung von Rechten

Wenn das Objekt keine DACL hat, ist es ungeschützt und das Sicherheitssystem gewährt den gewünschten Zugriff.

Wenn der Aufrufer das Inbesitznahme-Privileg (SeTakeOwnership Privileg) hat, gewährt das Sicherheitssystem den Write-Owner Zugriff, bevor es die DACL prüft, wenn dies der einzige geforderte Zugriff war.

Wenn der Aufrufer der Besitzer des Objektes ist, werden die Zugriffsrechte Read_Control und Write_DACL gewährt. Wenn dies die einzigen angeforderten Zugriffsrechte sind, wird der Zugriff ohne Prüfung der DACL gewährt.

Die ACE der DACL werden der Reihenfolge nach geprüft. Wenn die SID im ACE mit einem Access-Token des Aufrufers übereinstimmt, wird der ACE verarbeitet.

Im Falle eines AccessAllowed-ACE wird die Maske des ACE zu einer akkumulierten Zugriffsmaske hinzugefügt (OR). Wurden alle geforderten Zugriffsrechte erreicht, wird der Zugriff gewährt und die weitere Verarbeitung der DACL abgebrochen.

Ist bei einem AccessDenied-ACE ein angefordertes Recht in der Maske des ACE enthalten, so wird der Zugriff verweigert und die weitere Verarbeitung der DACL abgebrochen.

2.6.2 Effektive Rechte

Die Win32-API Funktion GetEffectiveRightsFromAcl arbeitet wie folgt:

Der Algorithmus baut eine AccessAllowed und eine AccessDenied Maske auf, indem er alle ACE wie folgt prüft:

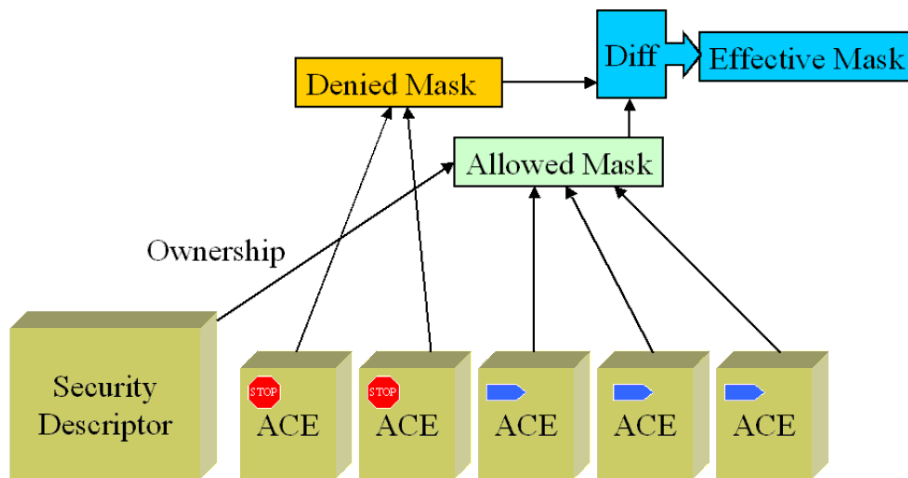


Abbildung 0.5: Die effektiven Rechte

Wenn das Objekt keine DACL hat, ist es nicht geschützt und das Sicherheitssystem gewährt alle Zugriffsrechte.

Wenn der Aufrufer das Inbesitznahme Privileg (SeTakeOwnership Privileg) hat, gewährt das Sicherheitssystem den Write-Owner Zugriff, bevor es die DACL prüft.

Wenn der Aufrufer der Besitzer des Objektes ist, werden die Zugriffsrechte Read_Control und Write_DACL gewährt.

Enthält ein AccessDenied-ACE eine SID, die mit einem der Access-Tokens des Aufrufers übereinstimmt, wird die Maske des ACE zur AccessDenied Maske hinzugefügt.

Enthält ein AccessAllowed-ACE einen SID, der mit einem der Access-Tokens des Aufrufers übereinstimmt, wird die Maske des ACE zur AccessAllowed Maske hinzugefügt.

Wenn alle Einträge in der DACL geprüft wurden, wird die berechnete Access-Maske ($\text{AccessAllowed} \& \sim \text{AccessDenied}$) als maximal erlaubter Zugriff zurückgegeben.

2.7 Rangfolge von Berechtigungen

Aufgrund der oben beschriebenen Algorithmen zur Überprüfung der Rechte (Punkt 0) ist leicht ersichtlich, dass die Reihenfolge der ACE in der Zugriffskontrollliste eine entscheidende Rolle spielt.

Leicht lässt sich dieser Einfluss in der folgenden Abbildung darstellen:

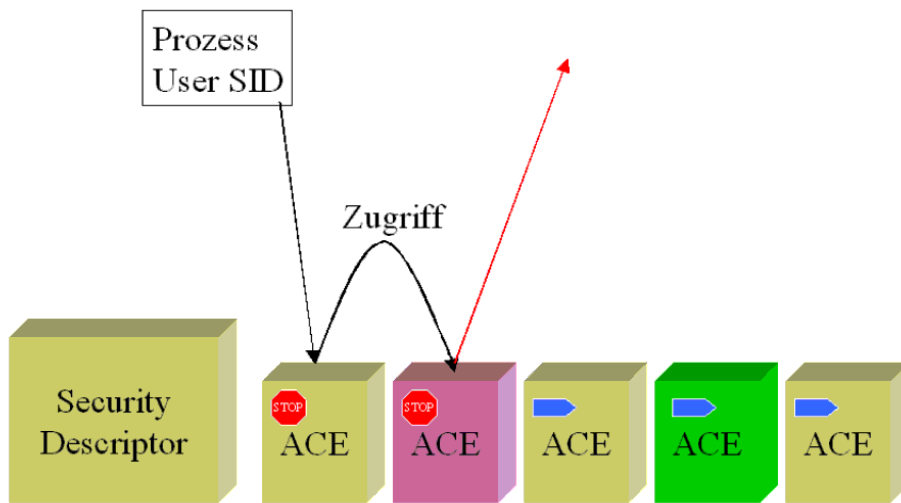


Abbildung 0.6: ACE Liste in korrekter Reihenfolge

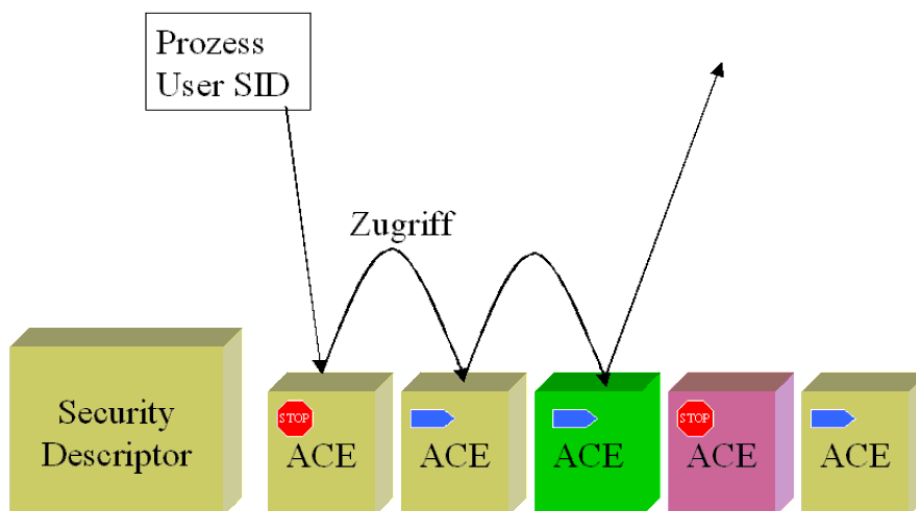


Abbildung 0.7: ACE Liste mit fehlerhafter Reihenfolge

Für Objekt A (Abbildung 0.6) wird der Zugriff mit dem ersten ACE abgelehnt, da der Benutzer als Kennung eingetragen ist. Bei Objekt B (Abbildung 0.7) wird mit dem ersten ACE das geforderte Recht erreicht und auf eine weitere Prüfung der Zugriffskontrollliste verzichtet.

Die "Interpretation" und Änderung der ACE Eintragungen in einer ACL Liste ist ab Windows 2000 nicht mehr von der jeweiligen Applikation abhängig. Zur Nutzung der Software asbLANtools ist die Kenntnis der in diesem Kapitel dargestellten Zusammenhänge erforderlich. Ohne ein tieferes Verständnis der Zusammenhänge ist eine umfassende Analyse der Sicherheit nicht gegeben.

3. Allgemeine Produktbeschreibung

3.1 Konzept der Software

3.1.1 Warum Analyse und Dokumentation und nicht aktive Administration?

Das Besondere der **asbLANtools®** ist die Funktionalität einer ausschließlichen Analyse und Dokumentation von Sicherheitseinstellungen. *Das hat entscheidende, gebaltvolle Gründe.* Das Produkt läßt aus Sicherheitsgründen bewußt keine direkte Administration im Netzwerk zu (*nur über Zusatzprodukte*). Das hauptsächliche Problem der „Sicherheitsverwaltung“ von Netzwerken ist nicht die Veränderung von Einstellungen, sondern die Dokumentation und Analyse sowie deren Strukturierung. Laut namhaften Untersuchungen entsteht die Mehrzahl der Datenverluste nicht durch Viren, defekte Hardware oder extern erzeugte Netzwerkeinbrüche sondern durch Defizite im internen Management der Netzwerkressourcen. Daher ist es Sinn und Zweck des Produktes **asbLANtools®**, eine ausschließliche Analyse und Dokumentation der wichtigen Benutzer – und Zugriffsrechte in der Domäne vorzunehmen.

Die asbLANtools® visualisieren den aktuellen Zustand der Netzwerk - Domänen. Das ist unabdingbare Voraussetzung, um gezielt an den existierenden Schwachstellen ansetzen zu können. Bestehende Sicherheitsrisiken in der Vergabe von Zugriffsrechten werden transparent und können im Anschluß durch geplante und vorausschauende Administration mit den entsprechenden Mitteln nachhaltig beseitigt werden. Gelöschte Benutzereintragungen und deren verbleibende Objekteinträge (NTFS, Dienste, Zugriffs -Token,..) können sicher analysiert werden.

asbLANtools® leistet also nicht nur einen grundlegenden Beitrag zur Erhöhung der Netzwerksicherheit, sondern die Software selbst ist auch ausnahmslos als Dokumentationsinstrument völlig gefahrlos für bestehende Strukturen im Netzwerk einsetzbar.

asbLANtools Analysedaten sollten sicher aufbewahrt werden, weil diese mögliche Schwachstellen eines Netzwerk in komprimierter Form offenbaren.

3.1.2 Konventionelle Dokumentation von zugewiesenen Rechten

Windows Betriebssysteme (hier Windows NT™, Windows 2000™, Windows XP™, Windows 2003™ und Windows VISTA™) stellen von Haus aus keine Werkzeuge für die Dokumentation von Benutzern, Gruppen, Freigaben, Zugriffsrechten usw. zur Verfügung. Die Standardwerkzeuge von Windows sind bei der Analyse und Dokumentation bestehender Netzwerkstrukturen im Allgemeinen nicht ausreichend. Insbesondere die Anforderungen größerer und sensiblerer Unternehmensaufgaben sowie geltende, sich ständig verschärfende Gesetze und die Rechtssprechung erfordern die Dokumentation, den authentischen Nachweis in lebenden Netzwerken und deren Sicherheitseinstellungen.

Die stetig steigende Vernetzung als Voraussetzung von besserer DV - Kommunikation erfordert eine firmeninterne sensible Überwachung von Sicher-

heitseinstellungen. Das Zeitalter der alleinigen Sicherheitsanforderung von Viren-scanner und Firewall für Unternehmen als „Securitylösung“ ist längst vorbei.

3.1.3 Datenschutz, Datensicherheit und aktuelle Rechtssprechung

Die IT – Verantwortlichen und Administratoren haften für die Einhaltung der spezifischen betriebsinternen Vorgaben und Richtlinien.

Dies muß im Zweifel bewiesen werden

Jedem soviel Zugriffsrechte wie nötig – nicht wie möglich.

Elektronische Nachweispflicht: Dokumentationserstellung und Auswertung der erstellten Reports und Berichte.

Compliance

Unternehmen dulden keine Unregelmäßigkeiten. Verstöße müssen geahndet werden

Einsetzung von IT- Sicherheitsbeauftragten

Prüfung durch Verbände und Wirtschafts– und Steuerprüfgesellschaften.

3.1.4 Zielstellung der Software asbLANtools®

asbLANtools® ist ein Werkzeug für die Administration und Revision von Unternehmen.

Zielstellung ist die Analyse und Dokumentation sowie Unterstützung der Administratoren bei Verwaltungsaufgaben. Es wurden bewußt keine „aktiven“ Administrationsfunktionen (z.B. eine Benutzerverwaltung) integriert, um den Charakter der Software nicht zu verfälschen.

Es ist einfach mit den verschiedensten Bordmitteln und Werkzeugen einen Benutzer anzulegen und dessen Eigenschaften zu verändern , jedoch relativ schwierig die „Spuren“ des Benutzers oder dessen Berechtigungen im Netzwerk zu verfolgen oder eindeutig zu bestimmen.

Die Lösung einer der Grundaufgaben eines Administrators oder Revisors „Welche Rechte hat ein Benutzer im Netzwerk“ sind erfordert zumeist zeit-aufwändige Arbeitsprozesse. Ebenso kann die Momentaufnahme einer Berechtigung im sich stetig veränderndem Netzwerk am Ende der Analyse bereits wieder einen anderen Zustand aufweisen.

Mit **asbLANtools®** werden dem Administrator Möglichkeiten geboten auch Aussagen für die Vergangenheit des Netzwerkes zu tätigen, und Unterschiede zwischen zwei oder mehr Datenbeständen miteinander zu vergleichen.

Die „Information auf den Punkt zu bringen“ ist umso aufwändiger, je größer das Netzwerk ist. Mit der Active Directory -Verwaltung ist es relativ einfach die Eigenschaften eines Benutzers fast überall im Netzwerk schnell auf den Bildschirm zu holen und zu verändern, aber die Analyse, Zugriff

und Dokumentation der „Security -Descriptoren und dessen Inhalt“ ist in großen Datenmassiven recht zu zeitaufwändig, insbesondere bei weltweit verteilten Netzwerken (WAN und ständig zu „dünnen „ Leitungen). sind diese Prozesse zeitaufwändig.

asbLANtools® bietet die Möglichkeit, diese Daten-Informationen automatisch über Agenten /Dienste sozusagen VorOrt zu scannen und diese Daten für zentrale Auswertungen in leistungsstarken Datenbanken bereitzustellen.

3.1.5 Authentische Analysen

Mit **asbLANtools®** vom Netzwerk erfaßte Daten werden mit authentischen Identifikatoren abgespeichert. Insbesondere bilden die SID (Security Identifier) und GUID (Global Identifier) für die Verifikation und Identifikation von Daten, Komponenten und Benutzern im Netzwerk die Grundlage für eine eindeutige, nachweisbare Aussagen. Grundsätzlich ist es möglich, ein gelöscht Konto unter gleichem „Bezeichner sprich Namen“ wieder anzulegen, aber über

asbLANtools® werden die Kontodifferenzen SID und GUID gespeichert und ausgewertet.

asbLANtools® ist eines der wenigen weltweit verfügbaren Systeme mit dieser Eigenschaft.

3.1.6 Die Arbeitsweise mit asbLANtools

asbLANtools® ist vorrangig für den Einsatz in großen Netzwerken konzipiert. Gedacht. Je größer das Netzwerk, desto größer der Nutzen für den Anwender (Administrator, Revisor). Die Software **asbLANtools®** arbeitet als OFFLINE System, d.h. alle für eine Auswertung notwendigen Daten müssen zuvor erfaßt (gescannt) werden.

Diese Arbeitsweise ist zunächst gewöhnungsbedürftig, bietet aber den Vorteil, daß zur Auswertung/ Analyse selbst nur die Geschwindigkeit der „Datenbank“ ausschlaggebend ist und die Netzwerklasten verringert werden.

In der vorliegenden **Version 2.8** kann je eine „Momentaufnahme“ des Netzwerkes in einer Datenbank abgelegt werden. Es können beliebig viele Datenbanken angelegt werden. Die „Momentaufnahmen“ = „ein Datenbestand“ können miteinander auf Unterschiede verglichen werden.

Über einen leistungsstarken **Viewer** können Details zu jeweils einem Datenbestand analysiert und dokumentiert werden. Die Dokumentation erfolgt über die leistungsstarke Reportsoftware Seagate Crystal Reports® (jetzt BusinessObjects®).

Die Struktur der Datenbank ist für den Kunden Anwender offen gelegt. Die Einzigartigkeit der **asbLANtools®** besteht in der „Abbildung“ einer oder

mehrerer Windows Domänen in einem relationalen Datenbankmodell. Dies bringt sehr große Vorteile in der Geschwindigkeit von Auswerteprozessen. Abfragen an die Datenbank können mit verknüpften Abfragen auf Basis der SID schnell und einfach realisiert werden.

Ebenso bietet das SID basierte Datenbankmodell den Vorteil eindeutiger Aussagen, d.h. ein Benutzer „Müller“ und ein später neu angelegter Benutzer gleichen Namens werden als unterschiedliche Accounts geführt. Dies hat auch Auswirkungen auf die SID-basierenden Objektberechtigungen (Files, Prozesstokens, Systemrechte etc). Es werden eindeutige und damit richtige Aussagen getätigt. Anders ist dies, wenn wie - in anderen Produkten - Aussagen auf Basis der Account-Namenstabelle getroffen werden.

asbLANtools® bietet auch - auf Grund der offengelegten Strukturen - die Möglichkeit der Integration in andere firmeninterne Lösungen (Hardwareverwaltung, Benutzerabrechnungssysteme, etc.) . Mittels einfacher Reportwerkzeuge können eigene Abfragen an die Datenbank gestellt werden oder ausgelieferte die über 75 vorinstallierten Reportvorlagen an die Bedürfnisse des Anwenders angepaßt werden.

Datenbanken:

asbLANtools® benötigen für die Darstellung und Verarbeitung der Informationen ein leistungsfähige Datenbanken.

In der Version 2.8 sind folgende Datenbanken einsetzbar:

- MS SQL Server 2000
- MS SQL Server 2005
- MS DataEngine des SQL Servers

Der Einsatz von MS Access wird nur in kleinen Netzwerken oder zum Softwaretest empfohlen, da hier Beschränkungen in der Auswertung bestehen.

3.1.7 Informationsbestandteile in der Version 2.8

In der vorliegenden Version 2.8 werden die nachfolgenden Bestandteile eines Windows Netzwerkes ausgewertet:

- Domänen - Informationen
- Maschinen
- Benutzerkonten
- Benutzergruppen
- Spezielle und generische Benutzerkonten für Computer
- Benutzerrechte
- Freigaben
- Informationen zu NTFS- Objekten
- Zugriffsrechte im NTFS (inklusive aller ACL /ACE Details, bitgenau)
- Drucker
- Systemdienste
- Policies (generische Berechtigungen)

Informationen können von den folgenden Plattformen erfaßt werden von:

- Domänencontrollern
- Alleinstehenden Servern (NT, 2000, 2003)
- Windows NT™ ,2000, 2003, XP , VISTA Workstations

In jedem Fall muß das zu untersuchende System Mitglied einer Domäne sein.

Arbeitsplattform:

Windows NT Server

Windows XP

Windows 2000 Server

Windows 2003 Server

- => jeweils aktuelle, bzw. für **asbLANtools** freigegebene Service-Packs (siehe Release Notes/ Readme)

Anmerkung:

Um Daten von einem Server oder einer Workstation zu scannen , muß auf der jeweiligen Maschine keine asbLANtools- Software installiert werden.

3.2 asbLANtools anwenden

Die Software ist für den branchenunabhängigen Einsatz in mittleren und großen Windows - Netzwerken konzipiert. Das Kundenspektrum reicht von Netzwerken mit 100 Benutzern bis hin zu Netzwerkkomplexen mit 100.000 Benutzern. Vorrangig wird asbLANtools® in Unternehmen mit sensiblen Sicherheitsanforderungen (Banken ,Versicherungen) aber auch in Unternehmen aus Industrie und Verwaltung sowie bei großen Versorgungsdienstleistern eingesetzt.

Die optimale Form (Einsatzkonzept) ist abhängig von der Unternehmensgröße sowie der Unternehmensstruktur und muß individuell ermittelt werden. So besteht die Möglichkeit alle DatenScans nur über das Modul Administrator, oder über einen oder mehreren ScanAgenten zu erfassen. Ebenso können mehrere Datenbanken auch an mehreren Standorten mit unterschiedlichem Informationsgehalt angewendet werden. Als untere Richtgrö-

ße für den asbLANtools® werden Netzwerke mit ca. 100 Benutzern angesehen. Die Dokumentation von Windows-Domänen ist sowohl für die Administration als auch für die Revision von großer Bedeutung. Für einen erfolgreichen Einsatz sollte ein Einsatzkonzept als Bestandteil des DV und Sicherheitskonzeptes auch Notfallkonzept erarbeitet werden. asbLANtools® bietet über separate Module die Möglichkeit komplette Berechtigungsdaten (Benutzer und Gruppen,..) sowie Filesystem - Berechtigungen rückzuspeichern. Diese Möglichkeit der Extraktion- bzw. Separation wird auch gern kann für Migrationsaufgaben verwendet.

3.3 Versionsspezifikation

asbLANtools® liegt in verschiedenen Spezifikationen vor. Die Software wird ständig weiterentwickelt. Die Versionsstände werden durch eine interne Release - Kennzeichnung markiert.

Dies ist auch die Voraussetzung für den Kundensupport.

*Aktuelle Version 2.8.0,
Release-Stand: 2.8.0.7, 06/2009*

3.4 Produktnutzen

3.4.1 .. für den Anwender

- *Nutzen der Dokumentation*

Die vollständige und übersichtliche Dokumentation des Ist - Zustandes von Windows Domänen ermöglicht zunächst eine **umfassende Informationsbeschaffung über die Struktur der Domänen**. Schwachstellen in der Rechtevergabe können somit identifiziert und nachfolgend behoben werden. Das ist eine Voraussetzung zur **Gewährleistung von Sicherheitsanforderungen und des Datenschutzes**, denn existierende Schwachstellen in der Vergabe von Zugriffsrechten werden transparent, auf NTFS - Ebene möglich. Windows Netzwerke lassen sich somit nachhaltig vor unerlaubten Zugriffen und Datenmißbrauch schützen. Die mühelose Aufbereitung relevanter Daten für andere Unternehmensbereiche sowie die bessere Wahrnehmung der Dokumentation für Security - Audits **erleichtert den Arbeitsalltag der Administration** und der Revisoren erheblich.

- *Intelligente Erfassungstechnologie*

Die Verlagerung des Sammelvorganges (DatenScan) in netzwerkschwache Zeiten und die vom Netzwerk losgelöste Auswertung ermöglicht eine **effiziente Informationsbeschaffung und Auswertung** sowie **geringe Netzwerkbelastung**. Dadurch sind beträchtliche Arbeitszeiteinsparungen möglich.

- *Performance*

Die einfache und zügige Installation sowie die Windows -konforme Benutzeroberfläche schaffen eine **hohe Bedienungsfreundlichkeit und Funktionalität**.

Die Performance der **asbLANtools®** Prozesse hängt von einer Reihe Faktoren ab, welche in einem konkreten Einsatzkonzept für größere Unternehmen unabdingbare Voraussetzung für den effektiven Einsatz dieses Produktes sind.

Einflußfaktoren sind:

- Größe des Netzwerkes (Benutzer und Gruppen Anzahl)
- Strukturierung des Netzes (WAN Komponenten, Replikation, Last)

- Antwortzeiten
- Datenbankserver, Leistungsfähigkeit
- Filesystem, Zustand bzw. „vorrangig“ lokale Datenerfassung

3.4.2 .. für das Unternehmen

Im Zeitalter der Informations- und Kommunikationstechnologie und des damit verbundenen verstärkten Wettbewerbs in vielen Märkten hängt der Erfolg von Unternehmen zunehmend von der optimalen Versorgung mit den relevanten Informationen ab. Informationen sind zu einer wichtigen Ressource geworden. Der kontrollierte Datenzugriff sowie der Schutz von Unternehmensdaten jeglicher Art werden somit zum entscheidenden Erfolgs-, Kosten - und auch Bestandsfaktor.

Voraussetzung für einen optimalen Informationsfluß und die Befriedigung des ständig wachsenden Informationsbedarfes in Unternehmen sind leistungsfähige Netzwerke mit eindeutig geregelten Informationszugehörigkeiten und klar definierten Kommunikationswegen sowie Vorgaben und Einstellungen. Für Windows 2000/ 2003 -Netzwerke schafft **asbLANtools®** die notwendigen Voraussetzungen, um über die Struktur der Rechtevergabe und verwendeten Einstellungen für Informationszugriffe eines Benutzers den notwendigen Überblick zu behalten.

- *Nutzen der Dokumentation*

Die vollständige und übersichtliche Dokumentation des Ist - Zustandes von Windows - Domänen bewirkt eine Transparenz administrativer Vorgänge und somit eine Qualitätsverbesserung der Aufgabenerfüllung. Infolge der mit dem Produkt

asbLANtools® möglichen nachhaltigen Dokumentation verbessert sich der Informationsfluß zwischen den Unternehmensbereichen. Damit ist insgesamt eine **Steigerung der Effizienz von administrativen Steuerungs- und Kontrollfunktionen** verbunden. Diese leistet einen erheblichen Beitrag zur **Erhöhung der Netzwerksicherheit**.

- *intelligente Erfassungstechnologie*

Die Erfassungs- und Auswertungsprozesse mit den **asbLANtools®** laufen unabhängig voneinander ab. Das ermöglicht eine getrennte und effektive sowie sichere Beschaffung der auszuwertenden Informationen sowie eine Trennung der personellen Zuständigkeit für die Prozesse. **Einsparungspotentiale in den Personalkosten** werden somit möglich. Die Verlagerung der Prozesse in netzwerkschwache Zeiten (Nacht- und Wochenendbetrieb) **verringert die Kosten beim Einsatz** der Software. Die Trennung von Erfassung und Auswertung bietet zudem die Möglichkeit, das die Auswertung selbst nur mit dem Zugriff auf die Datenbank verbunden ist. – **Der Zugriff mit administrativen Berechtigungen auf das Netzwerk ist somit für eine Analyse selbst nicht erforderlich**.

- **Günstiges Preis-/Leistungsverhältnis**

Die Lizenzierung erfolgt auf Basis der Netzwerkgröße (Accounts im Netzwerk)

- **Datenschutz**

„Jedem Benutzer seine Berechtigung“, **nicht mehr und nicht weniger !!**
Der oftmals alleinige Einsatz von Firewall und Virenschanner „.. als Werkzeuge für den Datenschutz reichen heute nicht mehr aus. Entsprechend bestätigter Studien (IDC) entstehen 70% aller Schäden durch Mitarbeiter oder firmeninterne Datenzugriffe. Hier helfen nur stetige, sichere und übersichtliche Methoden der Verwaltung der Zugriffsberechtigungen. **asbLANtools®** bietet genau für diese Aufgabe eine effektive Lösungsplattform.

Mit weitergehenden Lösungen von asb Systemhaus können die „Überwachungsaufgaben von Zugriffsberechtigungen automatisiert werden. (Dies setzt jedoch die Analyse voraus). So bieten die Produkte asbTREErights und asbDISKman Möglichkeiten Veränderungen an Berechtigungsstrukturen durch Benutzer realtime zu registrieren und rückgängig zu machen, so daß diese auch als Eigentümer angelegte „Daten“ nur noch bearbeiten können.

Anmerkung: In Windows / NTFS ist jeder Bearbeiter der eine Datei erzeugt auch dessen „lebenslanger Eigentümer“. Ein Eigentümer hat immer das Recht (analog einem First-Level Administrator) die Berechtigungen zu ändern.

Genau hier liegen jedoch verschiedene Sicherheitsrisiken versteckt. Die Produkte asbTREErights und asbDISKman bieten Möglichkeiten den Eigentümer sofort zu „enteignen“ und vorgegebene Berechtigungen jederzeit einzuhalten.

.. für die Migration von Netzwerken

Die Migration von Netzwerken ist eine zeitaufwändige Angelegenheit. Insbesondere die Neustrukturierung von Berechtigungsstrukturen, die sich zunehmend mehr oder minder „spontan“ entwickeln, bedarf besonderer Aufmerksamkeit. Neben der Migration von NT4/Windows 2000 nach Windows 2003 sind auch unternehmensspezifische Migrationen mitunter erforderlich. asbLANtools® kann hier helfen, viel Zeit zu sparen. Sie können Benutzerkonten manuell bearbeiten und dann auf das neue Zielsystem speichern. Mit der zukünftigen asbLANtools® Version sollen auch Umgebungen simuliert werden können..

.. für die überwachungssensiblen Umgebungen

Mit **asbLANtools®** werden alle Veränderungen an Benutzerkonten, Gruppen und Zugriffsrechten aufgezeichnet und können mit anderen (älteren Datenbeständen) verglichen werden. Hier sind alle Abweichungen sichtbar. Die Unterschiede können auch auf Basis von Skript - Lösungen automatisiert ausgegeben werden.

Die gekennzeichneten Unterschiede sind authentisch. Ein gelöscht und wieder erzeugtes Konto wird beispielsweise erkannt.

.. für den Administrator

Oftmals ist es für den Administrator schwierig Übersicht über das Datenmassiv des Unternehmens zu halten und punktgenaue Informationen abzufragen bzw. schnell zu suchen. Einmal in eine Datenbank importierte Informationen können mit höchster Effizienz abgefragt und auf diese sodann zugegriffen werden.

.. für den Einsatz durch die Revision

Die Aufgaben der Revision bestehen sowohl in der vollständigen, als auch stochastischen Prüfung von Konten und Daten. asbLANtools® unterstützt Revisoren bei der Arbeit, indem in aller Ruhe und ohne Gefahren der Verwendung administrativer Kontenzugänge Auswertungen auch „offline“ durchgeführt werden können.

Einmal geprüfte Systeme können später mit dem DifferenzViewer erneut auf Veränderungen geprüft werden. Damit kann sehr viel Arbeitszeit eingespart und die Genauigkeit von Aussagen wesentlich erhöht werden.

.. für den Einsatz in Kleinunternehmen

Für kleine Unternehmen kann der Einsatz von asbLANtools® bereits bei ? Benutzern von Vorteil sein. Die kompakte Einsatzumgebung bietet durch eine effiziente Datenerfassung schnell und übersichtlich auch hier Hilfestellung. Insbesondere günstige Einstiegspakete können hier Anwendung finden.

.. für den Einsatz in Großunternehmen

asbLANtools® wird bereits bei mehreren Unternehmen mit 100.000 und mehr Accounts eingesetzt. Nur leistungsfähige Systeme bieten hier die notwendige Effektivität und Übersicht. Bei 100.000 Konten und beispielsweise 20.000 Gruppen müssen somit bis zu $2 \cdot 10^9$ (2 Milliarden) Sicherheitseinträge für die Domäne geprüft werden. In der Praxis liegt dieser Wert bei ca. 20% , hier 400 Millionen.

Dies kann nur ein System auf Basis eines relationalen Datenbankmodells, wie es die asbLANtools® besitzen leisten.

4. Technische Produktbeschreibung asbLANtools

4.1 Komponenten

Das Analyse- und Dokumentations - Werkzeug asbLANtools® besteht aus mehreren Modulen:

asbLANtools® Startmenü-System

- Administrator für Verwaltung / DatenScan
- Viewer für visuelle Auswertung mit Reporting Modul für Dokumentation
- DifferenzViewer für Bestandsvergleich
- ScanService für automatisierte Datenerfassung
- Importservice für automatischen Datenbankimport
- Batchprozessor für produktiven DatenScan über CMD Interface
- Offene Datenbankschnittstelle für Integration von Fremdanwendungen bzw. eigene Auswertungen
- *Modul asbCACLS zum Setzen und Rückspeichern von Berechtigungen im Netzwerk;*
- *Programm asbSuperACL zur Onlineauswertung effektiver Berechtigungen im Filesystem.*

Alle Komponenten können separat oder gemeinsam auf einem oder mehreren Servern im Netzwerk installiert werden. Ebenso können gleichzeitig mehrere Datenbanken eingesetzt werden, auch unterschiedlichen Typs.

Der **asbLANtools® Administrator** stellt das hauptsächliche Modul für die Konfiguration der Datenerfassung dar. Gleiches gilt für den **asbLANtools® Viewer** zur Auswertung. Mit dem Administrator wird die Konfiguration aller Einstellungen für die Online - Erfassung von Daten sowie dessen Ausführung gesteuert.

Über Services können später die Aufträge zur Datenerfassung in der produktiven **asbLANtools®** Umgebung automatisiert werden. Administrator – und „Produktionsumgebung“ sind ab Version 2.6.6 vollständig voneinander getrennt.

Die folgende Abbildung zeigt die Benutzeroberfläche des **asbLANtools® Administrators**.

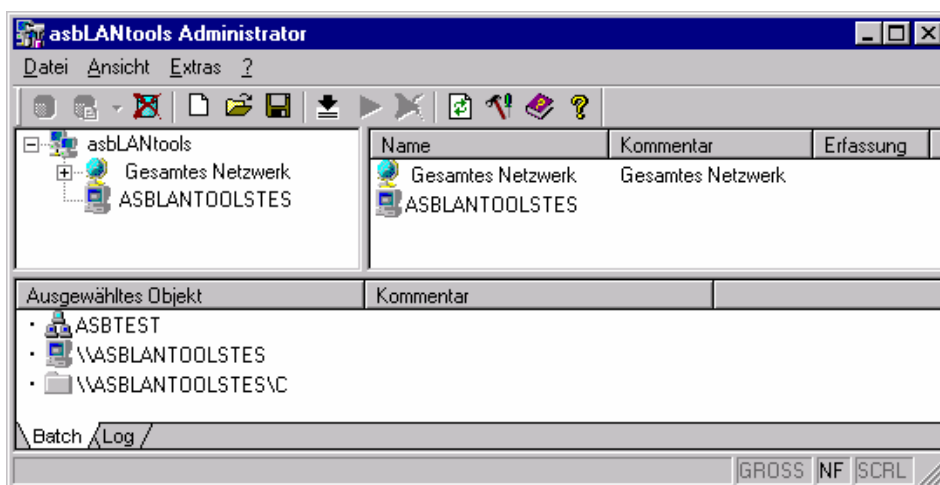


Abb.1: Der asbLANtools® Administrator ???

Die hauptsächliche Auswertung der Sicherheitsinformationen erfolgt visuell über den Windows -konformen **asbLANtools® Viewer**. Ein farbiger Leitfaden führt den Administrator zu den Abweichungen in der Rechtestruktur. Selektierte Objekte können über die Crystal Report Schnittstelle dokumentiert bzw. die Reports ausgedruckt werden.

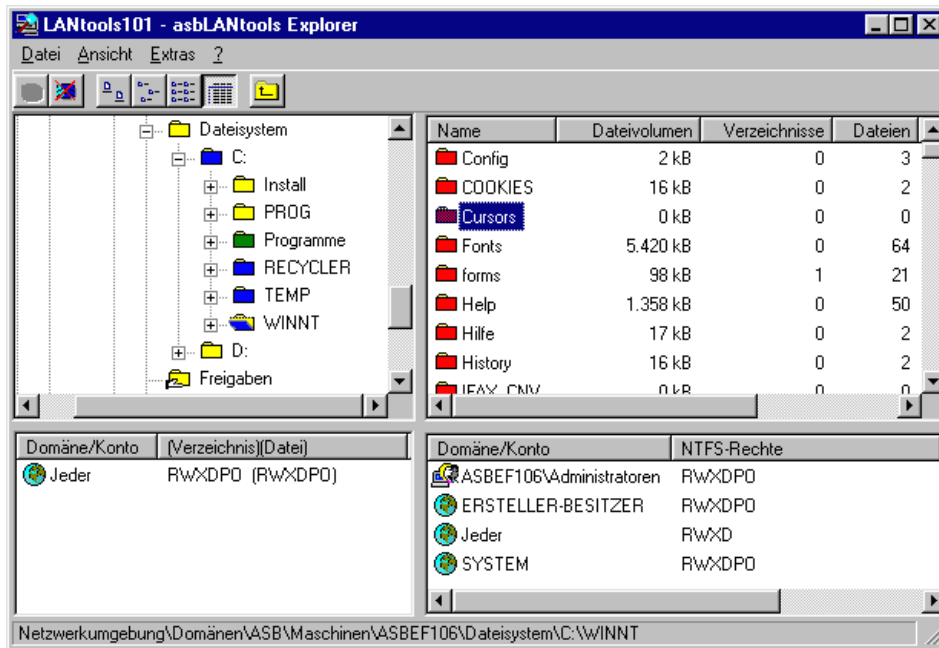


Abb.2: Die Ergebnisanzeige des asbLANtools® Viewers

4.2 Arbeitsweise

asbLANtools® ist für die Offline - Auswertung konzipiert, d.h. die Arbeitsweise erfolgt generell in zwei Prozessschritten:

- Datenerfassung
- Datenauswertung

Die nachfolgende Übersicht zeigt die Ablaufstrukturierung mit asbLANtools®.

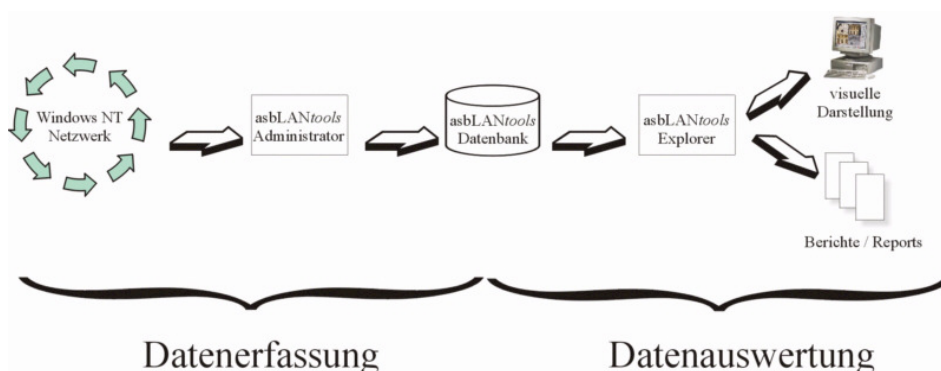


Abb.3: Datenerfassung und Datenauswertung

Für die Datenerfassung ist in Netzwerken keine Installation von asbLANtools® Software auf den zu analysierenden Systemen notwendig. In größeren Netzwerken sollten generell eine oder mehrere asbLANtools® - Arbeitsrechner installiert werden, je nach Anforderung, Größenordnung und Strukturierung des Unternehmens.

Zur Unterstützung des produktiven Einsatzes sowie der Unterstützung von verteilten Umgebungen (über WAN-Strecken,..) besteht die Möglichkeit der dezentralen Auftragsbearbeitung und automatischen Zusammenführung der Auswertedaten. Hier kommen speziell entwickelte Services zum Einsatz.

4.2.1 Datenerfassung

Im Rahmen der Datenerfassung werden Informationen über Windows Domänen, Windows - Maschinen innerhalb dieser Domänen sowie Informationen über die Dateisysteme dieser Maschinen erfaßt. Alle Funktionen können zentral gesteuert werden. In größeren Netzwerken ist eine dezentrale Erfassung möglich, bei der alle Informationen in einer zentralen Datenbank abgelegt werden. Diese Datenbank sollte vorzugsweise ein Microsoft SQL Server sein.

4.2.2 Datenauswertung

Für die Auswertung erfaßter Daten gibt es in **asbLANtools®** sowie im Umfeld vielfältige Möglichkeiten:

- Visuelle Auswertung über **asbLANtools® Viewer**;
- **Selektives Reporting** über Crystal Reports (über Modul Viewer);
- Auswertung über **offene Datenbankschnittstelle** für kundenindividuelle Auswertungen , z.B. einfache Abfragen über MS Access.

Modul DifferenzViewer für den Vergleich von Datenbeständen; Ausgabe und Editing über CSV/Textfiles (vorteilhaft für Migrations- Anforderungen).

4.2.3 Versionsmanagement

Mit **asbLANtools®** kann ab der Version 2.8.x je Datenbank ein „Versionsstand“ gespeichert und ausgewertet werden.

Ein Versionsstand dokumentiert bei vollständigem DatenScan immer die vollständige Rechte- Struktur einer oder mehrerer Domänen.

Über das Modul DifferenzViewer können zwei oder mehr Datenbestände gleichzeitig auf Unterschiede verglichen werden. Damit lassen sich z.B. Unterschiede zu „freigegebenen bzw. einmal geprüften Umgebungen“ auf laufende Änderungen prüfen. Der DifferenzViewer ermöglicht somit der Revision auf früher vorgenommene Prüfungen zurückzugreifen und damit bisher entstehenden Prüfungsaufwand wesentlich zu reduzieren..

4.2.3 Reporting

Über das Modul **asbLANtools® Viewer** besteht die Möglichkeit des Reporting (Crystal Reports Ausgaben). Es können sowohl Gesamt- als auch selektierte Einzeldaten ausgegeben werden.

Verfügbar sind ca. 75 unterschiedliche Reports. Eine Erweiterung mit kunden-spezifischen Reports oder mit nachträgliche Erweiterungen des Herstellers sind jederzeit ohne Installationsaufwand möglich (Copy). Ebenso können Reports und Abfragen zu Auswertungen individuell angepaßt werden, wodurch individuelle Anforderungen berücksichtigt werden können.

4.2.4 Datenbanksystem und Schnittstellen

Als besonderen Vorteil bieten die **asbLANtools®** eine offene Datenbank - Schnittstelle sowie eine relational verknüpfte Tabellenstruktur. Der Vorteil dieses Systems wird besonders bei großen Netzwerkumgebungen durch hohe Leistungsfähigkeit deutlich. Ebenso können über diese Schnittstelle, die vollständig beschrieben ist , third-party Softwaresysteme zur Auswertung eingesetzt werden.

5. Lizenzierung

Das Lizenzmodell richtet sich nach der Anzahl der Accounts in einer Domäne.

(Summe der Benutzer- und Maschinenkonten).

Es können mehrere Domänen gleichzeitig lizenziert werden.

Für Großkunden (Servicevertrag) werden Firmenlizenzen ausgestellt.

Ebenso bestehen vorteilhafte Lizenzierungsmöglichkeiten für Händler und Schulungsunternehmen.

Für die Evaluierung / Test besteht die Möglichkeit des Bezuges einer Evaluierungslizenz, die einen begrenzten Datenauszug generiert.

6. Übersicht Technische Spezifikation

Merkmal	Beschreibung
Version	2.8.0
Analysierte Betriebssystemumgebungen	Windows NT 4, Windows NT, 2000, 2003, XP, VISTA
Betriebssystem für asbLANtools® Services	Windows 2000 Server SP4, XP SP2, 2003 SP1
Unterstützte Datenbanken	MS SQL Server 2000, 2005, (Oracle 8.1.7, ff .eingeschränkte Unterstützung)
Datenbanktechnologie	ADO /DAO und OLEDB
Windows Domänen-Typ	NT4, W2k: native mode & mixed mode sowie AD Unterstützung
Datenmodell	Relationales SID basierendes Modell mit offener Schnittstelle
Reporting	Crystal Reports Ausgaben
Administration	Analyse und Dokumentation keine aktive Veränderung von Daten
Backup	Rückspeicherung von Security Daten über erstellte Skripte möglich.
Datenvolumen : Vollständiger Scan	ca. 0,3 % des Datenvolumens (Filesystem), im Wesentlichen abhängig von dem Umfang und Optionen des gescannten Filesystems (Optionen zur Datenreduktion vorhanden)
Ausgabeformat /Zwischendatei	TXT- bzw. CSV- Format, Kompaktierung sowie optional Kryptierung

Zeitaufwand für DatenScan	Stark abhängig vom Zustand des Netzwerkes realer Scan-Durchsatz: Filesystem: 10,.. 1.000 GB Datenvolumen/Stunde; Domäne: 1.000 Benutzeraccounts / Minute Maschineninformation: ca. 10,..20 Sek.
Zeitaufwand für Datenbankimport	Generell Minimal im Verhältnis zu DatenScan MS SQL: Fast-Page-Import Modus Oracle: Einsatz Oracle Loader möglich
Anforderung DifferenzViewer	Maximale CPU- und Speicheranforderung sowie schnelle Datenbank - Verbindung
Typischer asbLANtools® Rechner für 1000,.. 20.000 Benutzer	Server mit schnellem Plattensystem, 50 GB, 2 GB RAM, CPU 2 GHz; MS SQL oder Oracle DB
Automatisierung	Sowohl DatenScan als auch Bereitstellung (Import in eine Standard-DB) können über Services und Auftragssteuerung (Scheduling) automatisiert werden.
Lizenzierung	Nach Anzahl der Accounts im Netzwerk / Domäne