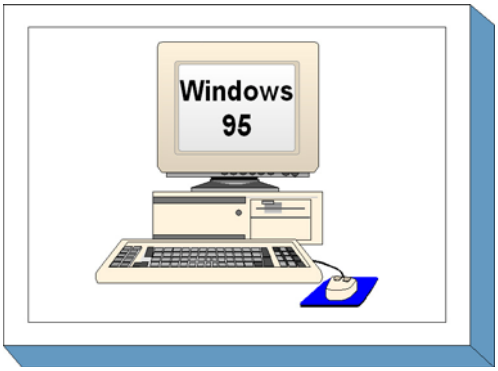
B 3.206 Client unter Windows 95



Beschreibung

Betrachtet wird ein handelsüblicher PC, der mit dem Betriebssystem Windows 95 oder einem der Nachfolgesysteme Windows 98, 98 SE oder ME betrieben wird. Die hier aufgeführten Maßnahmen gelten zunächst für Windows 95, sind jedoch weitgehend, eventuell mit leichten Anpassungen, auch auf die anderen hier genannten Systeme anwendbar. Der PC kann über Disketten-, CD-ROM-, DVD- oder andere Laufwerke für auswechselbare Datenträger sowie andere Peripheriegeräte verfügen. Falls der Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, WLAN, müssen diese entsprechend den Sicherheitsvorgaben der Institution abgesichert werden, wie dies in den entsprechenden Bausteinen beschrieben ist.

Für die weiteren Betrachtungen wird zugrunde gelegt, dass dieser PC auch von mehreren Benutzern betrieben werden kann. Dabei gelten jedoch folgende grundlegende Überlegungen:

Wesentliche Sicherheitseigenschaften von Windows 95 lassen sich erst in einem servergestütztem Netz realisieren. Wird ein Windows 95-Rechner als Einzelplatzrechner betrieben, so sollte von einem Mehr-Benutzer-Betrieb abgesehen werden, solange nicht unter Zuhilfenahme eines PC-Sicherheitsproduktes wichtige Funktionen wie z. B. Rechtekontrolle und Protokollierung realisiert werden können. Selbst bei Nutzung des Rechners durch nur einen Benutzer gelten dieselben Überlegungen, wenn die Benutzerumgebung durch einen Administrator mittels Systemrichtlinien eingeschränkt werden soll, da faktisch damit wieder ein Mehr-Benutzer-Betrieb entsteht.

Fazit: Ein nicht vernetzter Windows 95-Rechner sollte nur von einem Benutzer und uneingeschränkt genutzt werden können. Eine Einschränkung des Benutzers ist nur dann sinnvoll, wenn damit das Navigieren im System erleichtert wird oder wenn Fehlbedienungen damit ausgeschlossen werden sollen. Wird dennoch ein Mehr-Benutzer-Betrieb realisiert, so ist dieser unter Sicherheitsgesichtspunkten nur in Kombination mit einem PC-Sicherheitsprodukt sinnvoll.

Gefährdungslage

Für den IT-Grundschutz eines PC mit Windows 95 werden folgende Gefährdungen angenommen:

Höhere Gewalt:

- G 1.2 Ausfall des IT-Systems
- G 1.4 Feuer
- G 1.5 Wasser
- G 1.8 Staub, Verschmutzung

Organisatorische Mängel:

- G 2.1 Fehlende oder unzureichende Regelungen
- G 2.7 Unerlaubte Ausübung von Rechten
- G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz
- G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern
- G 2.22 Fehlende Auswertung von Protokolldaten
- G 2.35 Fehlende Protokollierung unter Windows 95
- G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal
- G 3.8 Fehlerhafte Nutzung des IT-Systems
- G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten
- G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel
- G 3.22 Fehlerhafte Änderung der Registrierung

Technisches Versagen:
- G 4.23 Automatische CD-ROM-Erkennung
- G 4.24 Dateinamenkonvertierung bei Datensicherungen unter Windows 95

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.4 Diebstahl
- G 5.9 Unberechtigte IT-Nutzung
- G 5.21 Trojanische Pferde
- G 5.23 Computer-Viren
- G 5.43 Makro-Viren
- G 5.60 Umgehen der Systemrichtlinien

Maßnahmenempfehlungen

Um den betrachteten IT-Verbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz.

Für Clients unter Windows 95 sind eine Reihe von Maßnahmen umzusetzen, beginnend mit der Planung und Konzeption über den Betrieb bis hin zur Notfallvorsorge. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im folgenden aufgeführt.

Planung und Konzeption

Zunächst muss festgelegt werden, unter welchen Bedingungen die Clients unter Windows 95 eingesetzt werden sollen. In Abhängigkeit davon sind zusätzliche Maßnahmen erforderlich.

Wenn mit einem Rechner unter Windows 95 mehrere Benutzer arbeiten sollen, so muss durch Einrichten von Zugriffsrechten dafür gesorgt werden, dass diese Benutzer gegeneinander geschützt sind. Bei Nutzung des Systems als Client lässt sich dieser Schutz durch die Zugangs- und Zugriffskontrolle des Servers für die dort gespeicherten Daten erreichen. Ein Schutz von lokal auf dem Windows 95 Rechner gespeicherten Daten kann dagegen nur durch Installation zusätzlicher Sicherheitssoftware erzielt werden, und auch dieser Schutz ist nur höchst mangelhaft, wenn auf eine Verschlüsselung verzichtet wird.

Sollen an dem Windows 95-Rechner mehrere Benutzer arbeiten, so ist eine Administration des Rechners und eine Benutzertrennung unumgänglich. In diesem Fall sind die folgenden Maßnahmen für den Mehrbenutzerbetrieb **zusätzlich** umzusetzen:
- M 2.63 *Einrichten der Zugriffsrechte*
- M 2.103 *Einrichten von Benutzerprofilen unter Windows 95*
- M 3.18 *Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung*

Soll die Benutzerumgebung benutzerspezifisch mit bestimmten Einschränkungen versehen werden, so sind weiterhin die folgenden Maßnahmen zu ergreifen (die Maßnahme M 2.65 wirkt nur in Verbindung mit M 4.41):

- M 2.65 *Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System*
- M 2.104 *Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95*
- M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*

Notfallvorsorge

Nur eine regelmäßige Datensicherung gewährleistet, dass auch im Fehlerfall und bei einem Angriff auf die Sicherheit wichtige Daten weiter verfügbar bleiben. Diese Sicherung wird bei einem Client unter Windows 95 in der Regel darin bestehen, dass wichtige Dateien auf dem Server gehalten oder zumindest regelmäßig dorthin übertragen werden. Zusätzlich bieten Rettungsdisketten bei einer Reihe lokaler Fehler eine Hilfe, den Rechner ohne Datenverlust wieder funktionsfähig zu machen.

Nachfolgend wird das Maßnahmenbündel für den Bereich "Client unter Windows 95" vorgestellt.

Planung und Konzeption

- M 2.63 (A) Einrichten der Zugriffsrechte
- M 2.103 (A) Einrichten von Benutzerprofilen unter Windows 95
- M 2.104 (Z) Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95
- M 4.41 (Z) Einsatz angemessener Sicherheitsprodukte für IT-Systeme
- M 4.74 (A) Vernetzte Windows 95 Rechner

Umsetzung

- M 4.57 (A) Deaktivieren der automatischen CD-ROM-Erkennung

Betrieb

- M 2.65 (Z) Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System
- M 3.18 (A) Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung
- M 4.56 (B) Sicheres Löschen unter Windows-Betriebssystemen

Notfallvorsorge

- M 6.45 (A) Datensicherung unter Windows 95
- M 6.46 (A) Erstellung von Rettungsdisketten für Windows 95

G 1.2 Ausfall des IT-Systems

Ausfall zentraler Komponenten

Der Ausfall einer Komponente eines IT-Systems kann zu einem Ausfall des gesamten IT-Betriebs führen. Insbesondere zentrale Komponenten eines IT-Systems sind geeignet, solche Ausfälle herbeizuführen, z. B. LAN-Server, Datenfernübertragungseinrichtung. Auch der Ausfall von Komponenten der technischen Infrastruktur, beispielsweise Klima- oder Stromversorgungseinrichtungen, kann zu einem Ausfall des IT-Systems beitragen.

Technisches Versagen/ menschliche Fehlhandlungen

Technisches Versagen (z. B. G 4.1 *Ausfall der Stromversorgung*) muss nicht zwingend als Ursache für den Ausfall eines IT-Systems angenommen werden. Ausfälle lassen sich auch oft auf menschliches Fehlverhalten (z. B. G 3.2 *Fahrlässige Zerstörung von Gerät oder Daten*) oder vorsätzliche Handlungen (z. B. G 5.4 *Diebstahl*, G 5.102 *Sabotage*) zurückführen. Auch durch höhere Gewalt (z. B. Feuer, Blitzschlag, Chemieunfall) können Schäden eintreten, allerdings sind diese Schäden meist um ein Vielfaches höher.

Werden auf einem IT-System zeitkritische IT-Anwendungen betrieben, sind die Folgeschäden nach Systemausfall entsprechend hoch, wenn es keine Ausweichmöglichkeiten gibt.

Beispiele:

- Durch Spannungsspitzen in der Stromversorgung wird das Netzteil eines wichtigen IT-Systems zerstört. Da es sich um ein älteres Modell handelt, steht nicht unmittelbar Ersatz bereit. Die Reparatur nimmt einen Tag in Anspruch, in dieser Zeit ist der gesamte IT-Betrieb nicht verfügbar.
- Es wird eine Firmware in ein IT-System eingespielt, die nicht für diesen Systemtyp vorgesehen ist. Das IT-System startet daraufhin nicht mehr fehlerfrei und muss vom Hersteller wieder betriebsbereit gemacht werden.
- Bei einem Internet Service Provider führte ein Stromversorgungsfehler in einem Speichersystem dazu, dass dieses abgeschaltet wurde. Obwohl der eigentliche Fehler schnell behoben werden konnte, ließen sich die betroffenen IT-Systeme anschließend nicht wieder hochfahren, da Inkonsistenzen im Dateisystem auftraten. Bis alle Folgeprobleme behoben waren, waren mehrere der vom ISP betriebenen Webserver tagelang nicht erreichbar.

Ausfall einer Archivkomponente

- In elektronischen Archiven kann der Zeitpunkt der erstmaligen Archivierung als Entstehungszeitpunkt von Dokumenten missinterpretiert werden, wenn keine anderweitigen Beweisverfahren, z. B. Zeitstempeldienste, zur Beglaubigung eingesetzt werden. Dies gilt vor allem für Geschäftsprozesse, in die die elektronische Archivierung von massenhaft anfallenden Belegdaten transparent eingebunden ist. Im vorliegenden Fall konnte aufgrund des Ausfalls einer Archivkomponente ein Teil von Belegdaten erst um einen Tag verzögert archiviert werden. Durch die Verwendung von WORM-Medien wurde die Reihenfolge der physikalischen Archivierung der Geschäftsbelege trotzdem nachweisbar dokumentiert, es wurde jedoch kein Nachweis für die ansonsten nicht auftretende Verzögerung durch die ausgefallene Archivkomponente geführt. Dadurch entstand bei einer späteren Prüfung der Eindruck einer nachträglichen Manipulation.

G 1.4 Feuer

Neben direkten durch das Feuer verursachten Schäden an einem Gebäude oder dessen Einrichtung lassen sich Folgeschäden aufzeigen, die insbesondere für die Informationstechnik in ihrer Schadenswirkung ein katastrophales Ausmaß erreichen können. Löschwasserschäden treten beispielsweise nicht nur an der Brandstelle auf. Sie können auch in tiefer liegenden Gebäudeteilen entstehen. Bei der Verbrennung von PVC entstehen Chlorgase, die zusammen mit der Luftfeuchtigkeit und dem Löschwasser Salzsäure bilden. Werden die Salzsäuredämpfe über die Klimaanlage verteilt, können auf diese Weise Schäden an empfindlichen elektronischen Geräten entstehen, die in einem vom Brandort weit entfernten Teil des Gebäudes stehen. Aber auch "normaler" Brandrauch kann auf diesem Weg beschädigend auf die IT-Einrichtung einwirken.

Ein Brand entsteht nicht nur durch den fahrlässigen Umgang mit Feuer (z. B. Adventskranz, Schweiß- und Lötarbeiten), sondern auch durch unsachgemäße Benutzung elektrischer Einrichtungen (z. B. unbeaufsichtigte Kaffeemaschine, Überlastung von Mehrfachsteckdosen). Technische Defekte an elektrischen Geräten können ebenfalls zu einem Brand führen.

Die Ausbreitung eines Brandes kann unter anderem begünstigt werden durch:

- Aufhalten von Brandabschnittstüren durch Keile,
- Unsachgemäße Lagerung brennbarer Materialien,
- Nichtbeachtung der einschlägigen Normen und Vorschriften,
- Fehlen von Brandmeldeeinrichtungen,
- Fehlen von Handfeuerlöschern bzw. automatische Löscheinrichtungen,
- mangelhaft vorbeugenden Brandschutz (z. B. Fehlen von Brandabschottungen auf Kabeltrassen).

Beispiele:

- Anfang der 90er Jahre erlitt im Frankfurter Raum ein Großrechenzentrum einen katastrophalen Brandschaden, der zu einem kompletten Ausfall führte.
- Immer wieder kommt es vor, dass elektrische Kleingeräte wie z. B. Kaffeemaschinen oder Halogenlampen unsachgemäß installiert sind oder betrieben werden und dadurch Brände verursachen.

G 1.5 Wasser

Der unkontrollierte Eintritt von Wasser in Gebäuden oder Räumen kann beispielsweise bedingt sein durch:

- Regen, Hochwasser, Überschwemmung,
- Störungen in der Wasser-Versorgung oder Abwasser-Entsorgung,
- Defekte der Heizungsanlage,
- Defekte an Klimaanlagen mit Wasseranschluss,
- Defekte in Sprinkleranlagen,
- Löschwasser bei der Brandbekämpfung und
- Wassersabotage z. B. durch Öffnen der Wasserhähne und Verstopfen der Abflüsse.

Unabhängig davon, auf welche Weise Wasser in Gebäude oder Räume gelangt, besteht die Gefahr, dass Versorgungseinrichtungen oder IT-Komponenten beschädigt oder außer Betrieb gesetzt werden (Kurzschluss, mechanische Beschädigung, Rost etc.). Wenn zentrale Einrichtungen der Gebäudeversorgung (Hauptverteiler für Strom, Telefon, Daten) in Kellerräumen ohne selbsttätige Entwässerung untergebracht sind, kann eindringendes Wasser sehr hohe Schäden verursachen.

Beispiele:

- Viele Gewerbebetriebe, auch große Unternehmen, tragen der Hochwassergefährdung nicht hinreichend Rechnung. So wurde ein Unternehmen bereits mehrere Male durch Hochwasserschäden am Rechenzentrum "überrascht". Das Rechenzentrum schwamm im wahrsten Sinne des Wortes innerhalb von 14 Monaten zum zweiten Mal davon. Der entstandene Schaden belief sich auf mehrere hunderttausend Euro und ist nicht von einer Versicherung gedeckt.
- In einem Serverraum verlief eine Wasserleitung unterhalb der Decke, die mit Gipskarton verkleidet war. Als eine Verbindung undicht wurde, wurde dies nicht rechtzeitig erkannt. Das austretende Wasser sammelte sich zunächst an der tiefsten Stelle der Verkleidung, bevor es dort austrat und im darunter angebrachten Stromverteiler einen Kurzschluss verursachte. Dies führte dazu, dass bis zur endgültigen Reparatur sowohl die Wasser- als auch die Stromversorgung des betroffenen Gebäudeteils abgeschaltet werden musste.

G 1.8 Staub, Verschmutzung

Staub stört Elektronik

Trotz zunehmender Elektronik in der IT kommt sie noch nicht ohne mechanisch arbeitende Komponenten aus. Zu nennen sind Disketten, Fest- und Wechselplatten, Diskettenlaufwerke, Drucker, Scanner etc, aber auch Lüfter von Prozessoren und Netzteile. Mit steigenden Anforderungen an die Qualität und die Schnelligkeit müssen diese Geräte immer präziser arbeiten. Bereits geringfügige Verunreinigungen können zu einer Störung eines Gerätes führen. Staub und Verschmutzungen können beispielsweise durch

- Arbeiten an Wänden, Doppelböden oder anderen Gebäudeteilen,
- Umrüstungsarbeiten an der Hardware bzw.
- Entpackungsaktionen von Geräten (z. B. aufwirbelndes Styropor)

in größerem Maße entstehen, die entsprechende Ausfälle der Hardware verursachen können.

Vorhandene Sicherheitsschaltungen in den Geräten führen meist zu einem rechtzeitigen Abschalten. Das hält zwar den Schaden, die Instandsetzungskosten und die Ausfallzeiten klein, führt aber dazu, dass das betroffene Gerät nicht verfügbar ist.

Beispiele:

- Bei der Aufstellung eines Servers in einem Medienraum, zusammen mit einem Kopierer und einem Normalpapier-Faxgerät, traten nacheinander die Lähmung des Prozessor-Lüfters und des Netzteil-Lüfters aufgrund der hohen Staubbelastung des Raumes auf. Der Ausfall des Prozessor-Lüfters führte zu sporadischen Server-Abstürzen. Der Ausfall des Netzteil-Lüfters führte schließlich zu einer Überhitzung des Netzteils mit der Folge eines Kurzschlusses, was schließlich einen Totalausfall des Servers nach sich zog.
- Um eine Wandtafel in einem Büro aufzuhängen, wurden von der Haustechnik Löcher in die Wand gebohrt. Der Mitarbeiter hatte hierzu sein Büro für kurze Zeit verlassen. Nach Rückkehr an seinen Arbeitsplatz stellte er fest, dass sein PC nicht mehr funktionierte. Ursache hierfür war Bohrstaub, der durch die Lüftungsschlitze in das PC-Netzteil eingedrungen war.

G 2.1 Fehlende oder unzureichende Regelungen

Die Bedeutung übergreifender organisatorischer Regelungen und Vorgaben für das Ziel IT-Sicherheit nimmt mit dem Umfang der Informationsverarbeitung, aber auch mit dem Schutzbedarf der zu verarbeitenden Informationen zu.

Von der Frage der Zuständigkeiten angefangen bis hin zur Verteilung von Kontrollaufgaben kann das Spektrum der Regelungen sehr umfangreich sein. Auswirkungen von fehlenden oder unzureichenden Regelungen werden beispielhaft in den Gefährdungen G 2.2 ff. beschrieben.

Vielfach werden nach Veränderungen technischer, organisatorischer oder personeller Art, die wesentlichen Einfluss auf die IT-Sicherheit haben, bestehende Regelungen nicht angepasst. Veraltete Regelungen können dem störungsfreien IT-Betrieb entgegen stehen. Probleme können auch dadurch entstehen, dass Regelungen unverständlich oder zusammenhanglos formuliert sind und dadurch missverstanden werden.

Dass Regelungsdefizite schadensfördernde Auswirkungen haben können, machen folgende **Beispiele** deutlich:

- Durch eine mangelhafte Betriebsmittelverwaltung kann der termingerechte Arbeitsablauf in einem Rechenzentrum schon durch eine unterbliebene Druckerpapierbestellung stark beeinträchtigt werden.
- Neben einer Beschaffung von Handfeuerlöschern muss auch deren Wartung geregelt sein, um sicherzustellen, dass diese im Brandfall auch funktionstüchtig sind.
- Bei einem Wasserschaden wird festgestellt, dass dieser auch den darunter liegenden Serverraum in Mitleidenschaft zieht. Durch eine unzureichende Schlüsselverwaltung kann der Wasserschaden im Serverraum allerdings nicht unmittelbar behoben werden, weil keiner informiert ist, wo sich der Schlüssel zum Serverraum gerade befindet. Dadurch steigt der Schaden erheblich.

G 2.7 Unerlaubte Ausübung von Rechten

Rechte wie Zutritts-, Zugangs- und Zugriffsberechtigungen werden als organisatorische Maßnahmen eingesetzt, um eine sichere und ordnungsgemäße IT-Nutzung zu gewährleisten. Werden solche Rechte an die falsche Person vergeben oder wird ein Recht unautorisiert ausgeübt, können sich eine Vielzahl von Gefährdungen ergeben, die die Vertraulichkeit und Integrität von Daten oder die Verfügbarkeit von Rechnerleistung beeinträchtigen.

Beispiele:

- Der Arbeitsvorbereiter, der keine Zutrittsberechtigung zum Datenträgerarchiv besitzt, entnimmt in Abwesenheit des Archivverwalters Magnetbänder, um Sicherungskopien einspielen zu können. Durch die unkontrollierte Entnahme wird das Bestandsverzeichnis des Datenträgerarchivs nicht aktualisiert, die Bänder sind für diesen Zeitraum nicht auffindbar.
- Ein Mitarbeiter ist erkrankt. Ein Zimmerkollege weiß aufgrund von Beobachtungen, wo dieser sein Passwort auf einem Merkzettel aufbewahrt und verschafft sich Zugang zum Rechner des anderen Mitarbeiters. Da er erst kürzlich durch ein Telefonat mitbekommen hat, dass der Kollege noch eine fachliche Stellungnahme abzugeben hatte, nimmt er hier unberechtigterweise diese Aufgabe im Namen seines Kollegen wahr, obwohl er zu der Thematik nicht auf dem aktuellen Sachstand ist. Eine daraus folgende Erstellung einer Ausschreibungsunterlage in der Verwaltungsabteilung fordert im Pflichtenheft daher eine längst veraltete Hardwarekomponente, weil die dortigen Mitarbeiter der fachlichen Stellungnahme des erfahrenen Kollegen uneingeschränkt vertraut haben.

G 2.9 Mangelhafte Anpassung an Veränderungen beim IT-Einsatz

Die speziell für den Einsatz von Informationstechnik geschaffenen organisatorischen Regelungen, aber auch das gesamte Umfeld einer Behörde bzw. eines Unternehmens unterliegen ständigen Veränderungen. Sei es nur, dass Mitarbeiter ausscheiden oder hinzukommen, Mitarbeiter das Büro wechseln, neue Hardware oder Software beschafft wird, der Zulieferbetrieb für die Betriebsmittel Konkurs anmeldet. Dass sich bei einer ungenügenden Berücksichtigung der vorzunehmenden organisatorischen Anpassungen Gefährdungen ergeben, zeigen folgende Beispiele:

- Vor Urlaubsantritt vergisst ein Mitarbeiter, der Urlaubsvertretung Zugriffsrechte auf alle von dieser benötigten Dateien und Verzeichnisse zu übertragen. Hierdurch können sich Verzögerungen im IT-Betrieb ergeben.
- Durch bauliche Änderungen im Gebäude werden bestehende Fluchtwege verändert. Durch mangelhafte Unterrichtung der Mitarbeiter ist die Räumung des Gebäudes nicht in der erforderlichen Zeit möglich.
- Durch eine Umstellung eines IT-Verfahrens werden größere Mengen an Druckerpapier benötigt. Durch fehlende Unterrichtung der Beschaffungsstelle kommt es zu Engpässen im IT-Betrieb.
- Beim Empfang elektronischer Dokumente werden diese nicht automatisch auf Makro-Viren überprüft, da dieses Problem noch nicht bekannt ist oder kein Virenprüfprogramm vorhanden ist.
- Bei der Übermittlung elektronischer Dokumente wird nicht darauf geachtet, diese in einem für die Empfängerseite lesbaren Format abzuspeichern.

G 2.21 Mangelhafte Organisation des Wechsels zwischen den Benutzern

Arbeiten mehrere Benutzer zeitlich versetzt an einem Einzelplatz-IT-System, so findet zwangsläufig ein Wechsel zwischen den Benutzern statt. Ist dieser nicht ausreichend organisiert und geregelt, wird er unter Umständen nicht sicherheitsgerecht durchgeführt. Hierdurch können Missbrauchsmöglichkeiten entstehen, wenn z. B.

- laufende Anwendungen nicht korrekt abgeschlossen werden,
- aktuelle Daten nicht gespeichert werden,
- Restdaten im Hauptspeicher oder in temporären Dateien verbleiben,
- der vorhergehende Benutzer sich nicht am IT-System abmeldet und
- der neue Benutzer sich nicht ordnungsgemäß am IT-System anmeldet.

G 2.22 Fehlende Auswertung von Protokolldaten

Die meisten IT-Systeme und Anwendungen bieten Funktionalitäten an, um die Nutzung der Operationen, ihre Reihenfolge und ihre Auswirkungen zu protokollieren.

Im Lebenszyklus eines IT-Systems kommen verschiedene Protokollierungskonzepte zum Einsatz. Während der Entwicklungsphase werden ausführliche Protokolle erstellt, um im Fehlerfall die Protokolldaten für eine detaillierte Problemanalyse heranziehen zu können und die Fehlerbehebung zu erleichtern.

In der Einführungsphase werden Protokolle genutzt, um unter anderem die Performance des IT-Systems in der Produktivumgebung zu optimieren oder um die Wirksamkeit des Sicherheitskonzepts erstmals in der Praxis zu überprüfen.

In der Produktivphase werden Protokolle hauptsächlich auf die Sicherstellung des ordnungsgemäßen Betriebs bezogen. Protokolldaten dienen dann dem Zweck, nachträglich feststellen zu können, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein Angriffsversuch unternommen wurde. Protokolldaten werden für die Fehleranalyse im Schadensfall und zur Ursachenermittlung bzw. zur Integritätsprüfung genutzt. Die Protokollierung kann auch der Täterermittlung und damit auch der Abschreckung von potenziellen Tätern dienen. Durch regelmäßige Auswertung der Protokolldaten können vorsätzliche Angriffe auf ein IT-System unter Umständen frühzeitig erkannt werden. Findet die Auswertung der Protokolldaten nicht oder nur unzureichend statt, können diese nicht für Präventivmaßnahmen genutzt werden.

Bei einigen IT-Systemen oder Anwendungen fehlen ausreichende Protokollierungsmöglichkeiten. Häufig ist es mit systemeigenen Mitteln nicht oder nur schwer möglich, bei der Protokollierung nach der Art der Ereignisse zu differenzieren. Teilweise ist überhaupt keine Protokollierung vorgesehen.

Beispiele:

- Ein nicht autorisierter Benutzer versucht, Zugriff auf einen Datenbank-Server zu erlangen, indem er zu bekannten Benutzernamen die entsprechenden Passwörter rät. Die erfolglosen Authentisierungsversuche werden im System protokolliert. Aufgrund fehlender Auswertung der Protokolldateien werden die Angriffsversuche nicht erkannt. Der unautorisierte Benutzer kann unerkannt den Angriffsversuch gegebenenfalls bis zum Erfolg fortsetzen.
- Auf einem nicht vernetzten Windows 95-Rechner gibt es keine Möglichkeit, die Aktivitäten eines oder mehrerer Benutzer benutzerspezifisch zu protokollieren. Es ist daher nicht festzustellen, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein solcher Versuch unternommen wurde.

G 2.35 Fehlende Protokollierung unter Windows 95

Auf einem nicht vernetzten Windows 95-Rechner gibt es keine Möglichkeit, die Aktivitäten eines oder mehrerer Benutzer benutzerspezifisch zu protokollieren. Es ist daher nicht festzustellen, ob Sicherheitsverletzungen im IT-System stattgefunden haben oder ob ein solcher Versuch unternommen wurde.

Hinweis:

Der Inhalt dieser Gefährdung wurde in G 2.22 *Fehlende Auswertung von Protokolldaten* integriert und ist mit der Version 1999 entfallen.

G 2.36 Ungeeignete Einschränkung der Benutzerumgebung

Die meisten Betriebssysteme bieten die Möglichkeit, die Benutzerumgebung individuell für jeden Benutzer einzuschränken. Wo dies nicht der Fall ist, können hierfür im Allgemeinen spezielle Sicherheitsprodukte eingesetzt werden. Dabei bestehen prinzipiell zwei Möglichkeiten:

1. Bestimmte Funktionalitäten werden erlaubt, alle anderen sind verboten.
2. Bestimmte Funktionalitäten werden verboten, alle anderen sind erlaubt.

In beiden Fällen besteht die Möglichkeit, den Benutzer derart einzuschränken, dass dieser wesentliche Funktionen nicht mehr ausführen kann oder dass sogar ein sinnvolles und effizientes Arbeiten mit dem IT-System nicht mehr möglich ist.

Überlaufen von Partitionen

Eine weitere Form, die Benutzerumgebung einzuschränken, besteht in der Begrenzung des nutzbaren Speicherplatzes. Reicht der zur Verfügung stehende Speicherplatz nicht mehr aus, so können keine weiteren Informationen gespeichert werden. Je nach Art und Aufteilung des betroffenen IT-Systems können hiervon eine Vielzahl von Benutzern und Anwendungen betroffen sein. Wenn dabei auf eine Trennung zwischen Daten- und Systempartition verzichtet wurde, kann das gesamte IT-System ausfallen, weil beispielsweise kein Speicherplatz für Auslagerungen des Arbeitsspeichers ("Swap") mehr vorhanden ist.

Beispiele:

falsche Sparsamkeit

- In einer Firma hatte der Administrator den Benutzern durch enge Quotas nur sehr wenig Speicherplatz auf dem Mailserver zur Verfügung gestellt, um die Benutzer zu disziplinieren. Diese sollten angehalten werden, die Mails nicht in den Eingangspostfächern, sondern in den jeweiligen Arbeitsverzeichnissen zu speichern. Dadurch liefen die E-Mail-Postfächer allerdings schon nach wenigen Mails über und die Benutzer konnten keine weiteren E-Mails empfangen.
- In einer Behörde war festgelegt worden, dass bestimmte sicherheitsrelevante Informationen wie Anmeldeversuche ein Jahr lang protokolliert werden sollten. Da für die Protokoll-Daten aber zu wenig Platz auf dem Server vorhanden war, wurden diese immer automatisch nach einer Woche gelöscht. Als auffiel, dass geschäftsrelevante Daten manipuliert worden waren, konnte zwar eine Sicherheitslücke entdeckt werden, es ließ sich aber nicht mehr nachvollziehen, wie und durch wen diese ausgenutzt worden war.

G 3.2 Fahrlässige Zerstörung von Gerät oder Daten

Durch Fahrlässigkeit, aber auch durch ungeschulten Umgang kann es zu Zerstörungen an Geräten und Daten kommen, die den Betrieb des IT-Systems empfindlich stören können. Dies ist auch durch die unsachgemäße Verwendung von IT-Anwendungen möglich, wodurch fehlerhafte Ergebnisse entstehen oder Daten unabsichtlich verändert oder zerstört werden. Durch unachtsames Benutzen eines einzigen Löschbefehls können ganze Dateistrukturen gelöscht werden.

Beispiele:

- Benutzer, die aufgrund von Fehlermeldungen den Rechner ausschalten, statt ordnungsgemäß alle laufenden Anwendungen zu beenden bzw. einen Sachkundigen zu Rate zu ziehen, können hierdurch schwerwiegende Integritätsfehler in Datenbeständen hervorrufen.
- Durch umgestoßene Kaffeetassen oder beim Blumengießen eindringende Feuchtigkeit können in einem IT-System Kurzschlüsse hervorrufen werden.
- In einem z/OS-System verfügte ein Systemprogrammierer über die Berechtigung, das Programm *ICKDSF* zum Formatieren von Festplatten aufzurufen. Als er zur Ausübung seiner Tätigkeit dringend eine Festplatte benötigte, wählte er aus dem vorhandenen Pool eine freie Festplatte aus, gab jedoch aufgrund eines Tippfehlers eine falsche Adresse an. Den im System-Log anstehenden Reply las er nur flüchtig und beantwortete ihn sofort. Die Formatierung einer bereits belegten Festplatte wurde dadurch freigegeben und wichtige Produktionsdaten zerstört.
- Ein Benutzer, der es sich zur Gewohnheit gemacht hat, unter Unix den Löschbefehl *rm* grundsätzlich ohne den Parameter für die Sicherheitsabfragen (*-i*) durchzuführen oder gar mit *-f* die Sicherheitsabfragen grundsätzlich ausschaltet, riskiert in hohem Maße das versehentliche Löschen von Dateien. Ähnliches gilt auch für den Befehl *del* *.* unter MS-DOS.

G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen

Aufgrund von Nachlässigkeit und fehlenden Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten IT-Sicherheitsmaßnahmen nicht oder nicht im vollen Umfang durchführen. Es können Schäden entstehen, die sonst verhindert oder zumindest vermindert worden wären. Je nach der Funktion der Person und der Bedeutung der missachteten Maßnahme können sogar gravierende Schäden eintreten.

Vielfach werden IT-Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewusstsein heraus nicht beachtet. Ein typisches Indiz dafür ist, dass wiederkehrende Fehlermeldungen nach einer gewissen Gewöhnungszeit ignoriert werden.

Beispiele:

- Der verschlossene Schreibtisch bietet zur Aufbewahrung von Disketten oder anderen Informationsträgern keinen hinreichenden Schutz gegen unbefugten Zugriff, wenn der Schlüssel im gleichen Büro aufbewahrt wird, z. B. auf dem Schrank oder im Zettelkasten.
- Geheimzuhaltende Passwörter werden schriftlich fixiert in der Nähe eines Terminals oder PCs aufbewahrt.
- Obwohl die schadensmindernde Eigenschaft von Datensicherungen hinreichend bekannt ist, treten immer wieder Schäden auf, wenn Daten unvorhergesehen gelöscht werden und aufgrund fehlender Datensicherung die Wiederherstellung unmöglich ist. Dies zeigen insbesondere die dem BSI gemeldeten Schäden, die z. B. aufgrund von Computer-Viren entstehen.
- Der Zutritt zu einem Rechenzentrum sollte ausschließlich durch die mit einem Zutrittskontrollsystem (z. B. Magnetstreifenleser, Chipkartenleser oder biometrische Verfahren) gesicherte Tür erfolgen. Die Fluchttür wird jedoch, obwohl sie nur im Notfall geöffnet werden darf, als zusätzlicher Ein- und Ausgang genutzt.
- In einem z/OS-System liefen täglich Batch-Jobs für die RACF-Datenbank-Sicherungen. Die korrekte Ausführung dieser Abläufe sollte täglich von den zuständigen Administratoren geprüft werden. Da die Sicherungen jedoch über mehrere Monate ohne Probleme durchgeführt wurden, kontrollierte niemand mehr den Ablauf. Erst nachdem die RACF-Datenbanken des Produktionssystems defekt waren und die Sicherungen zurückgespielt werden sollten, wurde festgestellt, dass die Batch-Jobs seit mehreren Tagen nicht mehr gelaufen waren. Dies führte dazu, dass keine aktuellen Sicherungen vorhanden waren und die Änderungen der letzten Tage von Hand nachgetragen werden mussten. Neben einem erheblichen zusätzlichen Administrationsaufwand ergab sich dadurch ein Unsicherheitsfaktor, da nicht alle Definitionen sicher rekonstruiert werden konnten.

G 3.6 Gefährdung durch Reinigungs- oder Fremdpersonal

Es ist bereits nicht immer ganz einfach, eigene Mitarbeiter ausreichend zum richtigen Umgang mit IT zu schulen. Bei Betriebsfremden kann grundsätzlich nicht vorausgesetzt werden, dass sie mit der IT entsprechend den Vorgaben der besuchten Institution umgehen, vor allem, da sie diese in den seltensten Fällen kennen.

Die Gefährdung durch Besucher, Reinigungs- und Fremdpersonal erstreckt sich von der unsachgemäßen Behandlung der technischen Einrichtungen, über den Versuch des "Spielens" an IT-Systemen gegebenenfalls bis zum Diebstahl von IT-Komponenten.

Beispiele:

- Besucher können, wenn sie unbegleitet sind, Zugriff auf Unterlagen, Datenträger oder Geräte haben, diese beschädigen oder unbefugt in Kenntnis von schützenswerten Infornationen gelangen.
- Durch Reinigungspersonal kann versehentlich eine Steckverbindung gelöst werden, Wasser kann in Geräte gelangen, Unterlagen können verlegt oder sogar mit dem Abfall entfernt werden.
- In einem Rechenzentrum sollten in den Maschinenräumen Malerarbeiten durchgeführt werden. Der Maler stieß mit der Leiter versehentlich an den zentralen Notausschalter der Stromversorgung und löste diesen aus. Die gesamte Stromversorgung der z/OS-Systeme in diesem Rechenzentrum war sofort unterbrochen. Durch den Stromausfall waren mehrere Platten (DASD - Direct Access Storage Device) nicht sofort verfügbar. Der hinzugezogene Techniker benötigte mehrere Stunden, bis die Produktion wieder anlaufen konnte.

G 3.8 Fehlerhafte Nutzung des IT-Systems

Eine fehlerhafte Nutzung des IT-Systems beeinträchtigt die Sicherheit eines IT-Systems, wenn dadurch IT-Sicherheitsmaßnahmen missachtet oder umgangen werden.

Beispielsweise können zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Terminals zu IT-Sicherheitsvorfällen führen.

Gleichermaßen können durch fehlerhafte Bedienung von IT-Systemen oder IT-Anwendungen Daten versehentlich gelöscht oder verändert werden.

G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind. Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu Sicherheitslücken, falls über die notwendigen Rechte hinaus weitere vergeben werden.

Beispiel:

Durch eine fehlerhafte Administration der Zugriffsrechte hat ein Sachbearbeiter die Möglichkeit, auf die Protokolldaten zuzugreifen. Durch gezieltes Löschen einzelner Einträge ist es ihm daher möglich, seine Manipulationsversuche am Rechner zu verschleiern, da sie in der Protokolldatei nicht mehr erscheinen.

G 3.17 Kein ordnungsgemäßer PC-Benutzerwechsel

Arbeiten mehrere Benutzer an einem PC, so kann es aufgrund von Nachlässigkeit oder Bequemlichkeit dazu kommen, dass sich bei einem Wechsel der vorhergehende Benutzer nicht abmeldet und der neue sich nicht ordnungsgemäß anmeldet. Dies wird von den Betroffenen meist damit begründet, dass die Zeit, die das IT-System zum Neustarten benötigt, sehr lang ist und als nicht akzeptabel empfunden wird.

Dieses Fehlverhalten führt jedoch dazu, dass die Protokollierung von An- und Abmeldevorgängen und damit ein Teil der Beweissicherung unwirksam wird. Es lässt sich anhand der Protokolle nicht mehr zuverlässig feststellen, wer den Rechner zu einem bestimmten Zeitpunkt genutzt hat.

Beispiele:

- Ein PC wird abwechselnd von drei Benutzern eingesetzt, um Reisekostenabrechnungen durchzuführen. Nachdem der erste Benutzer den Anmeldevorgang durchgeführt hat, erfolgt kein ordnungsgemäßer PC-Benutzerwechsel mehr, weil die damit verbundenen Ab- und Anmeldevorgänge aus Bequemlichkeit nicht durchgeführt werden.
- Aufgrund von Unregelmäßigkeiten wird geprüft, wer welchen Vorgang am Rechner bearbeitet hat. Da nach Protokollierung nur ein Benutzer am PC gearbeitet hat, kann der Verursacher im Nachhinein nicht mehr festgestellt werden bzw. der einzige angemeldete Benutzer muss die Konsequenzen tragen.

G 3.22 Fehlerhafte Änderung der Registrierung

Windows-Betriebssysteme ab Windows 95 bieten die Möglichkeit, die Benutzerumgebung eines PC fest bzw. benutzerindividuell einzuschränken. Dies geschieht in der Regel unter Verwendung des Systemrichtlinieneditors (unter Windows 95 *POLEDIT.EXE*) oder des Registrierungseditors (unter Windows 95 *REGEDIT.EXE*). Unter Windows NT/2000/XP werden die Registrierungseditoren *regedt32.exe*, *regedit.exe* sowie das kommandozeilenorientierte Werkzeug *reg.exe* eingesetzt, um die Registrierung zu bearbeiten.

Die Benutzung dieser Programme sollte mit Bedacht und jede Änderung der Registrierung mit äußerster Sorgfalt ausschließlich durch geschultes Personal erfolgen, weil sehr schnell ein Systemzustand eingestellt werden kann, der ein Arbeiten mit dem PC nicht mehr erlaubt. Im ungünstigsten Fall ist dann das Betriebssystem neu zu installieren oder bestimmte Hardware-Komponenten erneut zu initialisieren (durch Laden der entsprechenden Treiber).

Unter Windows NT/2000/XP sind Registrierungseinträge durch Zugriffsrechte geschützt. Die Sicherheitseinstellungen für Registrierungsschlüssel können unter Windows NT/2000 nur mit dem Registrierungseditor *regedt32.exe* festgelegt werden. Unter Windows XP kann dazu sowohl *regedt32.exe* als auch *regedit.exe* verwendet werden. Durch falsche Konfiguration der Zugriffsrechte kann ein Benutzer die Registrierung wissentlich oder unwissentlich auf unerlaubte Weise modifizieren. Unsachgemäße Änderungen können dabei zu Systemschäden führen, so dass die Sicherheit und/oder die Arbeitsfähigkeit des Arbeits-PCs bzw. im Extremfall des gesamten Netzes gefährdet ist.

G 4.23 Automatische CD-ROM-Erkennung

Bei Windows-Betriebssystemen wie unter Windows 95 oder Windows NT können CD-ROMs, aber auch andere auswechselbare Datenträger automatisch erkannt und bearbeitet werden. Bei eingeschalteter CD-ROM-Erkennung werden CD-ROMs automatisch erkannt und die Datei *AUTORUN.INF* automatisch ausgeführt, wenn diese sich im Wurzelverzeichnis der CD-ROM befindet. Diese Datei kann beliebige auf der CD-ROM gespeicherte Programme (z. B. mit Schadfunktion) automatisch ausführen.

Ob diese Option eingeschaltet ist, erkennt man zum Beispiel unter Windows 95 daran, dass der Explorer vor dem CD-ROM-Laufwerksbuchstaben den Namen der CD-ROM automatisch einblendet. Ein Nebeneffekt hierbei ist, dass Energiespar-Funktionen in der Regel nicht mehr aktiviert werden.

G 4.24 Dateinamenkonvertierung bei Datensicherungen unter Windows 95

Werden zur Datensicherung unter Windows 95 Programme benutzt, die lange Dateinamen nicht unterstützen, so sind alle langen Dateinamen vor der Datensicherung mit dem zum Lieferumfang von Windows 95 gehörenden Programm LFNBK.EXE und der Option /B in die 8.3er-Konvention zu konvertieren. Anschließend ist das Datensicherungsprogramm aufzurufen. Schließlich sind die ursprünglichen Dateinamen mit LFNBK.EXE /R wieder herzustellen.

Dieses Verfahren ist jedoch mit Vorsicht anzuwenden, da zum einen bei der Namenskonvertierung Informationen verloren gehen können, zum anderen sich Dateien nicht mehr herstellen lassen, sobald sich die Verzeichnisstruktur nach der Datensicherung auf diesem PC geändert hat. Dies kann dann einen Datenverlust zur Folge haben.

G 5.2 Manipulation an Informationen oder Software

Informationen oder Software können auf vielfältige Weise manipuliert werden: durch falsches Erfassen von Daten, Änderungen von Zugriffsrechten, inhaltliche Änderung von Abrechnungsdaten oder von Schriftverkehr, Änderungen in der Betriebssystem-Software und vieles mehr. Grundsätzlich betrifft dies nicht nur digitale Informationen, sondern beispielsweise auch Dokumente in Papierform. Ein Täter kann allerdings nur die Informationen und Software-Komponenten manipulieren, auf die er Zugriff hat. Je mehr Zugriffsrechte eine Person auf Dateien und Verzeichnisse von IT-Systemen besitzt bzw. je mehr Zugriffsmöglichkeiten auf Informationen sie hat, desto schwerwiegendere Manipulationen kann sie vornehmen. Falls die Manipulationen nicht frühzeitig erkannt werden, kann der reibungslose Ablauf von Geschäftsprozessen und Fachaufgaben dadurch empfindlich gestört werden.

unterschiedliche Motive

Manipulationen an Informationen oder Software können unter anderem aus Rachegefühlen, um einen Schaden mutwillig zu erzeugen, zur Verschaffung persönlicher Vorteile oder zur Bereicherung vorgenommen werden.

Beispiele:

- In einem Schweizer Finanzunternehmen wurde durch einen Mitarbeiter die Einsatzsoftware für bestimmte Finanzdienstleistungen manipuliert. Damit war es ihm möglich, sich illegal größere Geldbeträge zu verschaffen.
- Sehr häufig werden Kundendatenbanken von Mitarbeitern beim Verlassen der Firma kopiert, um die Kundendaten für andere Zwecke gewinnbringend einsetzen zu können. Solche illegal beschafften Daten von Privatkunden sind beispielsweise benutzt worden, um Vertragsabschlüsse vorzutäuschen. Mitarbeiter, die im Unfrieden eine Behörde oder ein Unternehmen verlassen, könnten auch Informationen oder IT-Systeme mutwillig zerstören oder den Zugriff auf wichtige Informationen oder IT-Systeme verhindern.
- Archivierte Dokumente stellen meist besonders schützenswerte Informationen dar. Die Manipulation solcher Dokumente ist besonders schwerwiegend, da sie unter Umständen erst nach Jahren bemerkt wird und eine Überprüfung dann oft nicht mehr möglich ist.
- Eine Mitarbeiterin hat sich über die Höhergruppierung ihrer Zimmergenossin in der Buchhaltung dermaßen geärgert, dass sie sich während einer kurzen Abwesenheit der Kollegin unerlaubt Zugang zu deren Rechner verschafft hat. Hier hat sie durch einige Zahlenänderungen in der Monatsbilanz enormen negativen Einfluss auf das veröffentlichte Jahresergebnis des Unternehmens genommen.

G 5.4 Diebstahl

Durch den Diebstahl von IT-Geräten, Zubehör, Software oder Daten entstehen einerseits Kosten für die Wiederbeschaffung sowie für die Wiederherstellung eines arbeitsfähigen Zustandes, andererseits Verluste aufgrund mangelnder Verfügbarkeit. Darüber hinaus können Schäden durch einen Vertraulichkeitsverlust und daraus resultierenden Konsequenzen entstehen.

Von Diebstählen sind neben teuren IT-Systemen auch mobile IT-Systeme, die unauffällig und leicht zu transportieren sind, häufig betroffen.

Beispiele:

- Im Frühjahr 2000 verschwand ein Notebook aus dem amerikanischen Außenministerium. In einer offiziellen Stellungnahme wurde nicht ausgeschlossen, dass das Gerät vertrauliche Informationen enthalten könnte. Ebenso wenig war bekannt, ob das Gerät kryptographisch oder durch andere Maßnahmen gegen unbefugten Zugriff gesichert war. Bei Sicherheitsuntersuchungen war bereits vor ungenügenden Sicherheitskontrollen gewarnt worden.
- In einem deutschen Bundesamt wurde mehrfach durch die gleichen ungesicherten Fenster eingebrochen. Neben anderen Wertsachen verschwanden auch mobile IT-Systeme. Ob Akten kopiert oder manipuliert wurden, konnte nicht festgestellt werden.

G 5.9 Unberechtigte IT-Nutzung

Ohne Mechanismen zur Identifikation und Authentisierung von Benutzern ist die Kontrolle über unberechtigte IT-Nutzung praktisch nicht möglich. Selbst bei IT-Systemen mit einer Identifikations- und Authentisierungsfunktion in Form von Benutzer-ID- und Passwort-Prüfung ist eine unberechtigte Nutzung denkbar, wenn Passwort und zugehörige Benutzer-ID ausgespäht werden.

Um das geheim gehaltene Passwort zu erraten, können Unbefugte innerhalb der Login-Funktion ein mögliches Passwort eingeben. Die Reaktion des IT-Systems gibt anschließend Aufschluss darüber, ob das Passwort korrekt war oder nicht. Auf diese Weise können Passwörter durch Ausprobieren erraten werden.

Viel Erfolg versprechender ist jedoch die Attacke, ein sinnvolles Wort als Passwort anzunehmen und alle Benutzereinträge durchzuprobieren. Bei entsprechend großer Benutzeranzahl wird damit oft eine gültige Kombination gefunden.

Falls die Identifikations- und Authentisierungsfunktion missbräuchlich nutzbar ist, so können sogar automatisch Versuche gestartet werden, indem ein Programm erstellt wird, das systematisch alle möglichen Passwörter testet.

Beispiel:

- 1988 nutzte ein Internet-Wurm eine Schwachstelle der betroffenen Unix-Betriebssysteme aus, um gültige Passwörter zu finden, obwohl die gültigen Passwörter verschlüsselt gespeichert waren. Dazu probierte ein Programm sämtliche Eintragungen eines Wörterbuches aus, indem es sie mit der zur Verfügung stehenden Chiffrierfunktion verschlüsselte und mit den abgespeicherten verschlüsselten Passwörtern verglich. Sobald eine Übereinstimmung gefunden war, war auch ein gültiges Passwort erkannt.

G 5.21 Trojanische Pferde

Anwenderprogramme, Command Tables und Scriptsprachen

Ein Trojanisches Pferd, oft auch (eigentlich fälschlicherweise) kurz *Trojaner* genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Der Benutzer kann daher auf die Ausführung dieser Funktion keinen Einfluss nehmen - insoweit besteht eine gewisse Verwandtschaft mit Computer-Viren. Es ist jedoch keine Selbstreproduktion vorhanden. Als Träger für Trojanische Pferde lassen sich alle möglichen Anwenderprogramme benutzen. Aber auch Scriptsprachen, wie Batch-Dateien, ANSI-Steuersequenzen, *REXX Execs* und *ISPF Command Tables* bei z/OS-Betriebssystemen, Postscript und Ähnliches, die vom jeweiligen Betriebssystem oder Anwenderprogramm interpretiert werden, können für Trojanische Pferde missbraucht werden.

Die Schadwirkung eines Trojanischen Pferdes ist um so wirkungsvoller, je mehr Rechte sein Trägerprogramm besitzt.

Beispiele:

geänderte Login-Programme

- Ein geändertes Login-Programm kann ein Trojanisches Pferd enthalten, das Namen und Passwort des Benutzers über das Netz an den Angreifer übermittelt und dann an das eigentliche Login-Programm weitergibt. Solche Trojanischen Pferde sind z. B. bei Online-Diensten wie AOL oder T-Online aufgetreten.

Bildschirmschoner

- Auch Bildschirmschoner, besonders solche, die aus dem Internet herunter geladen werden, können eine versteckte Funktion enthalten, mit der die eingegebenen Passwörter des angemeldeten Benutzers protokolliert und an einen Angreifer übermittelt.

Back Orifice und NetBUS

- Bei dem Programm *Back Orifice* handelt es sich um eine Client-Server-Anwendung, die es dem Client erlaubt, einen Windows-PC über das Netz fernzuwarten. Insbesondere können Daten gelesen und geschrieben sowie Programme ausgeführt werden. Eine Gefährdung entsteht dadurch, dass dieses Programm in ein anderes Anwendungsprogramm integriert und somit als Trojanisches Pferd verwendet werden kann. Wird das Trojanische Pferd gestartet und besteht eine Netzverbindung, so kann ein Angreifer die Fernwartungsfunktion von *Back Orifice* für den Benutzer unbemerkt benutzen. In diesem Zusammenhang ist auch das Programm NetBUS zu erwähnen, das ähnliche Funktionen bietet.

manipulierte Programme und Bibliotheken

- Mit Hilfe von Root-Kits für verschiedene Unix-Varianten, die manipulierte Versionen von Systemprogrammen wie *ps, who, netstat* etc. enthalten, ist es möglich, längere Zeit unbemerkt Hintertüren (so genannte *Backdoors*) offen zu halten, die einen unbemerkten Einbruch in das System ermöglichen und dabei die Angriffsspuren verstecken. Häufig werden u. a. die Dateien */sbin/in.telnetd, /bin/login, /bin/ps, /bin/who, /bin/netstat* und die C-Libraries ausgetauscht.

aktuelles Verzeichnis im Suchpfad

- Eine weitere Gefahrenquelle bei Unix-Systemen ist der "." in der Umgebungsvariable *$PATH*. Wenn das jeweils aktuelle Arbeitsverzeichnis (.) als Pfad in der Variable *PATH* enthalten ist, werden zunächst die dort befindlichen Programme ausgeführt. So könnte beim Auflisten des Inhaltes eines

Verzeichnisses vom Superuser unbeabsichtigt ein darin enthaltenes modifiziertes "*ls*"-Programm mit root-Rechten ausgeführt werden.

- Eine Möglichkeit, sich im z/OS-Betriebssystem höhere Rechte zu erschleichen, bietet sich dann, wenn für den Angreifer ein *Update*-Zugriff auf Dateien existiert, die entweder beim Logon-Vorgang durchlaufen (z. B. eine *REXX EXEC*) oder während der Verarbeitung allgemein benutzt werden (z. B. *ISPF Command Tables*). Der Angreifer kann dann den vorhandenen Code durch eigene Programmteile ersetzen.

Einschleusen von Programmcode

G 5.23 Computer-Viren

Computer-Viren gehören zu den Programmen mit Schadensfunktionen. Als Schaden ist hier insbesondere der Verlust oder die Verfälschung von Daten oder Programmen sicherlich von größter Tragweite. Solche Funktionen von Programmen können sowohl unbeabsichtigt als auch bewusst gesteuert auftreten.

Die Definition eines Computer-Virus bezieht sich nicht unmittelbar auf eine möglicherweise programmierte Schadensfunktion:

Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. (Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.)

Die Eigenschaft der Reproduktion führte in Analogie zum biologischen Vorbild zu der Bezeichnung "Virus". Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig sind das Überschreiben oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems.

Computer-Viren können im Prinzip bei allen Betriebssystemen auftreten. Die größte Bedrohung ist jedoch im Bereich der IBM-kompatiblen Personalcomputer (PC) vorhanden. Bei den hier am meisten verbreiteten Betriebssystemen (MS-DOS, PC-DOS, DR DOS, NOVELL DOS etc.) werden derzeit weltweit rund 20.000 Viren (einschließlich Varianten) gezählt.

Spezielle Computer-Viren für die Betriebssysteme Windows 3.x, Windows NT, Windows 95, OS/2 und Unix spielen in der Praxis eine untergeordnete Rolle. Bei PC-typischer Hardware können jedoch die Festplatten dieser Rechner von DOS-Boot-Viren infiziert werden, wenn die Boot-Reihenfolge zuerst ein Booten von Diskette vorsieht.

Für Apple-Computer sind ca. 100 spezielle Computer-Viren bekannt, für die es auch entsprechende Suchprogramme gibt.

Arten von Computer-Viren

Es werden drei Grundtypen von Computer-Viren unterschieden:

- Boot-Viren
- Datei-Viren
- Makro-Viren

Es sind auch Misch- und Sonderformen dieser drei Typen bekannt. Weitere Unterteilungsmerkmale sind die Tarnmechanismen, mit denen die Viren oft gegen die Erkennung durch Benutzer und Suchprogramme geschützt sind.

Boot-Viren

Als "Booten" bezeichnet man das Laden des Betriebssystems. Hierbei werden u. a. Programmteile ausgeführt, die zwar eigenständig sind, sich aber in sonst

nicht zugänglichen und im Inhaltsverzeichnis der Disketten und Festplatten nicht sichtbaren Sektoren befinden. Boot-Viren überschreiben diese mit ihrem Programm. Der originale Inhalt wird an eine andere Stelle auf dem Datenträger verlagert und dann beim Start des Computers anschließend an den Virus-Code ausgeführt. Dadurch startet der Computer scheinbar wie gewohnt. Der Boot-Virus gelangt jedoch bereits vor dem Laden des Betriebssystems in den Arbeitsspeicher des Computers und verbleibt dort während der gesamten Betriebszeit. Er kann deshalb den Boot-Sektor jeder nicht schreibgeschützten Diskette infizieren, die während des Rechnerbetriebs benutzt wird. Boot-Viren können sich nur durch Booten oder einen Boot-Versuch mit einer infizierten Diskette auf andere Computer übertragen.

Datei-Viren

Die meisten Datei-Viren (auch File-Viren genannt) lagern sich an Programmdateien an. Dies geschieht jedoch so, dass beim Aufruf auch hier der Virus-Code zuerst ausgeführt wird und erst anschließend das originale Programm. Dadurch läuft das Programm anschließend scheinbar wie gewohnt und der Virus wird nicht so schnell entdeckt. Es sind jedoch auch primitivere, überschreibende Viren bekannt, die sich so an den Anfang des Wirtsprogramms setzen, so dass dieses nicht mehr fehlerfrei läuft. Datei-Viren verbreiten sich durch Aufruf eines infizierten Programms.

Bei den Mischformen von Boot- und Datei-Viren haben so genannte multipartite Viren eine größere Bedeutung erlangt. Sie können sich sowohl durch Aufruf eines infizierten Programms als auch durch Booten (oder einen Boot-Versuch) von einer infizierten Diskette verbreiten.

Makro-Viren

Auch Makro-Viren sind in Dateien enthalten, diese infizieren jedoch nicht die Anwendungsprogramme, sondern die damit erzeugten Dateien. Betroffen sind alle Anwendungsprogramme, bei denen in die erzeugten Dateien nicht nur einzelne Steuerzeichen, sondern auch Programme und andere Objekte eingebettet werden können. Davon sind insbesondere Microsoft Word- und Excel-Dateien betroffen. Bei diesen steht eine leistungsfähige Programmiersprache für Makros zur Verfügung, die auch von weniger geschulten Benutzern leicht zur Programmierung von Viren missbraucht werden kann (siehe auch G 5.43 *Makro-Viren*).

Makros sind Programme, mit deren Hilfe das Anwenderprogramm um zusätzliche Funktionen erweitert werden kann, die auf den Anwendungsfall zugeschnitten sind (z. B. Erzeugen einer Reinschrift aus dem Entwurf eines Textes). Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Microsoft Word, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert oder das Makro automatisch gestartet wird. Wird z. B. eine Word-Datei über einen WWW-Browser empfangen, der das Dokument automatisch mit Microsoft Word öffnet, kann hierdurch ein enthaltenes Makro aktiviert werden. Da Datendateien auch häufiger als herkömmliche Programmdateien über Datenträger und vernetzte IT-Systeme verteilt werden, ist die Gefährdung durch Makro-Viren inzwischen größer als durch Boot- und Datei-Viren.

Beispiele für Schadensfunktionen von Computer-Viren

- Der Boot-Virus Michelangelo überschreibt an jedem 6. März die ersten Spuren der Festplatte mit stochastischem Inhalt und macht sie dadurch unbrauchbar.
- Der multipartite Virus Onehalf verschlüsselt maximal die Hälfte des Inhalts der Festplatte. Wird der Virus entfernt, sind die verschlüsselten Daten nicht mehr verfügbar.
- Der Microsoft Word-Makro-Virus WAZZU fügt bei den befallenen Dokumenten an zufälligen Stellen das Wort "Wazzu" ein.
- Der Microsoft Word-Makro-Virus Melissa erschien am 26.3.1999 und verbreitete sich über das Wochenende weltweit. Er ist in einer Datei von Word 97 oder Word 2000 enthalten, die von einem befallenen Computer mittels Microsoft Outlook an bis zu 50 gespeicherte Einträge aus jedem Adressbuch verschickt wird. Dies hat bei einigen größeren Organisationen das Mail-System überlastet.
- W32.Mypics.Worm ist ein in Visual Basic geschriebener Computerwurm, der sich automatisch auf Windows 95/98 und Windows NT Rechnern verbreitet. Er enthält eine zerstörerische Schadenswirkung, die aktiv wird, sobald die Jahreszahl 2000 ist. Dann wird u. a. das BIOS des Rechners verändert, so dass der Rechner nicht mehr korrekt bootet.

G 5.43 Makro-Viren

Mit dem Austausch von Dateien (z. B. per Datenträger oder E-Mail) besteht die Gefahr, dass neben der eigentlichen Datei (Textdatei, Tabelle etc.) weitere, mit dem Dokument verbundene Makros bzw. eingebettete Editorkommandos übersandt werden. Diese Makros laufen erst mit dem jeweiligen Anwendungsprogramm (Winword, Excel etc.) bei der Bearbeitung des Dokuments ab, indem der Benutzer das Makro aktiviert bzw. das Makro automatisch gestartet wird. Wird ein Dokument über einen WWW-Browser empfangen, der das Dokument automatisch öffnet, kann hierdurch ein (Auto-) Makro aktiviert werden.

Da die Makrosprachen über einen sehr umfangreichen Befehlssatz verfügen, besteht auch die Gefahr, dass einem Dokument ein Makro beigefügt wird, das eine Schadfunktion enthält (z. B. einen Virus).

In der Praxis hat diese Gefährdung insbesondere bei den Dateien der Programme Word für Windows und Excel der Firma Microsoft weltweit beträchtlich zugenommen. Für den Benutzer ist dabei nicht transparent, dass Dateien für Word-Vorlagen (*.DOT), in denen Makros enthalten sein können, durch Umbenennen in *.DOC-Dateien scheinbar zu Datendateien werden, die keine Makros enthalten. Von Microsoft Word werden solche Dateien jedoch ohne Hinweis auf diese Tatsache in nahezu gleicher Weise verarbeitet (Ausnahme: Winword ab Version 7.0a).

Die Word-Makro-Viren haben inzwischen die Spitzenstellung bei gemeldeten Infektionen eingenommen. Hervorzuheben ist, dass Makro-Viren auf verschiedenen Betriebssystem-Plattformen auftreten können, nämlich auf allen, auf denen Winword läuft (Windows Versionen 3.1 und 3.11, Windows 95, Windows NT, Apple-Computer).

Beispiel:

- Der Winword-Makro-Virus "Winword.Nuclear" wurde im Internet über die Datei WW6ALERT.ZIP verbreitet. Der Makro-Virus bewirkt einerseits, dass an Ausdrucken der Text "STOP ALL FRENCH NUCLEAR TESTIN IN PACIFIC!" angehängt wird, andererseits aber auch den Versuch, Systemdateien zu löschen.

G 5.60 Umgehen der Systemrichtlinien

Besteht lokaler Zugang zu einem nicht vernetzten PC unter Windows 95, ist es möglich, die Passwortdatei (*name.PWL*), die zu einer bestimmten Benutzer-Kennung gehört, zu löschen. Der Zugang mit dieser Benutzer-Kennung ist dann ohne Kenntnis des Benutzer-Passwortes möglich. Dies ist insbesondere dann kritisch, wenn ein nicht vernetzter Windows 95-Rechner durch Systemrichtlinien für bestimmte Benutzer eingeschränkt ist, aber eine Administrator-Kennung (z. B. *ADMIN*) existiert, die alle Rechte besitzt. Durch löschen der *ADMIN.PWL* durch einen auf diesem PC eingeschränkten, aber dennoch berechtigten Benutzer kann dieser sich anschließend als Administrator anmelden. Die für den Benutzer eingestellten Einschränkungen bzw. Systemrichtlinien werden somit umgangen.

M 2.63 Einrichten der Zugriffsrechte

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Verantwortliche der einzelnen IT-Anwendungen, Administrator

Arbeiten mit einem IT-System mehrere Benutzer, so muss durch eine ordnungsgemäße Administration der Zugriffsrechte sichergestellt werden, dass die Benutzer das IT-System nur gemäß ihren Aufgaben nutzen können.

Vorausgesetzt sei, dass von den Fachverantwortlichen die Zugangs- und Zugriffsberechtigungen für die einzelnen Funktionen festgelegt wurden (siehe M 2.7 *Vergabe von Zugangsberechtigungen* und M 2.8 *Vergabe von Zugriffsrechten*). Anschließend werden die Benutzer des IT-Systems den einzelnen Funktionen zugeordnet. Die Ergebnisse sind schriftlich zu dokumentieren.

Der Administrator muss dann das IT-System so konfigurieren, dass diese Benutzer Zugang zum IT-System erhalten und mit den ihnen zugewiesenen Zugriffsrechten nur ihre Aufgaben wahrnehmen können. Bietet das IT-System keine Möglichkeit, Zugriffsrechte zuzuweisen (z. B. beim DOS-PC mit mehreren Benutzern), so ist ein Zusatzprodukt zu diesem Zweck einzusetzen (siehe z. B. M 4.41 *Einsatz angemessener Sicherheitsprodukte für IT-Systeme*).

Lässt das IT-System es zu, so sind die sinnvoll einsetzbaren Protokollfunktionen zur Beweissicherung durch den Administrator zu aktivieren. Dazu gehören erfolgreiche und erfolglose An- und Abmeldevorgänge, Fehlermeldungen des Systems, unerlaubte Zugriffsversuche.

Für den Vertretungsfall muss der Administrator vorab kontrollieren, ob der Vertreter vom Fachverantwortlichen autorisiert ist. Erst dann darf er die erforderlichen Zugriffsrechte im akuten Vertretungsfall einrichten.

Ergänzende Kontrollfragen:

- Werden die vom Administrator eingerichteten Zugriffsrechte sporadisch überprüft?
- Liegt eine Dokumentation vor, welche Rechtestruktur im IT-System realisiert ist?

M 2.65 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Revisor, Administrator, IT-Sicherheitsmanagement

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die Benutzer des IT-Systems sich regelmäßig nach Aufgabenerfüllung abmelden oder ob mehrere Benutzer unter einer Kennung arbeiten.

Sollte festgestellt werden, dass tatsächlich mehrere Benutzer unter einer Kennung arbeiten, sind sie auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hinzuweisen. Gleichzeitig sollte der Sinn dieser Maßnahme erläutert werden, die im Interesse des einzelnen Benutzers liegt.

Stellt sich heraus, dass die An- und Abmeldevorgänge zu zeitintensiv sind und trotz Aufforderung nicht akzeptiert werden, sollten alternative Maßnahmen diskutiert werden wie zum Beispiel:

- Das IT-System kann für bestimmte Zeitintervalle einem Benutzer zugeordnet werden, so dass in dieser Zeit andere Benutzer das IT-System nicht nutzen dürfen. Dies setzt voraus, dass der Arbeitsprozess dementsprechend zeitlich variabel ist.
- Es können zusätzliche IT-Systeme angeschafft werden, mit denen die quasiparallele Arbeit an einem IT-System vermieden werden kann. Zu beachten ist, dass zwar die Anschaffungskosten für die zusätzlichen IT-Systeme anfallen, aber andererseits die Anschaffungskosten für PC-Sicherheitsprodukte entfallen können.
- Sollten sich die Datenbestände der einzelnen Benutzer separieren lassen (beispielsweise Benutzer A bearbeitet die Daten A-L, Benutzer B die Daten M-Z), so können dafür unterschiedliche Zugriffsrechte eingeräumt werden. Will ein Benutzer dann mit seinen Daten arbeiten, muss er sich zuvor beim System anmelden, da seine Kollegen kein Zugriffsrecht auf diese Daten besitzen.

Ergänzende Kontrollfragen:

- Wie häufig wird der ordnungsgemäße Benutzerwechsel geprüft?
- Gibt es Akzeptanzprobleme bezüglich des Benutzerwechsels?
- Lassen sich die Datenbestände separieren?

M 2.103 Einrichten von Benutzerprofilen unter Windows 95

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Unter Windows 95 besteht die Möglichkeit, durch Einrichten von Benutzerprofilen eine Benutzertrennung durchzuführen. Diese Trennung dient jedoch (wenn nicht durch Systemrichtlinien eine Einschränkung erfolgt, siehe M 2.104 *Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95*) ausschließlich dazu, benutzerspezifische Einstellungen zu konservieren und damit für den jeweiligen Benutzer eine individuelle Arbeitsumgebung zu erhalten, die er nach seinen Bedürfnissen und Erfordernissen anpassen kann. Ein Windows 95-Anmeldepasswort wird erst nach Aktivieren der Benutzerprofile obligatorisch. Für dieses Passwort gelten im übrigen dieselben Überlegungen wie für WfW-Anmeldepasswörter (siehe M 4.46 *Nutzung des Anmeldepasswortes unter WfW und Windows 95*).

Die den Benutzer betreffenden Einstellungen werden in einem Verzeichnis *C:\WINDOWS\PROFILES\Benutzername* gespeichert.

Benutzerprofile sollten auf einem nicht vernetzten Windows 95-Rechner immer dann aktiviert werden, wenn unerfahrenen Benutzern das Navigieren unter Windows 95 erleichtert werden soll. Dies ist ebenfalls sinnvoll, wenn eine Benutzertrennung, wenn auch nicht unter Sicherheitsgesichtspunkten, so doch aus organisatorischen oder prinzipiellen Gründen gewünscht wird.

Dazu öffnet man die Programmgruppe *SYSTEMSTEUERUNG*, dann die Schaltfläche *KENNWÖRTER* und kann anschließend die Benutzerprofile aktivieren bzw. deaktivieren.

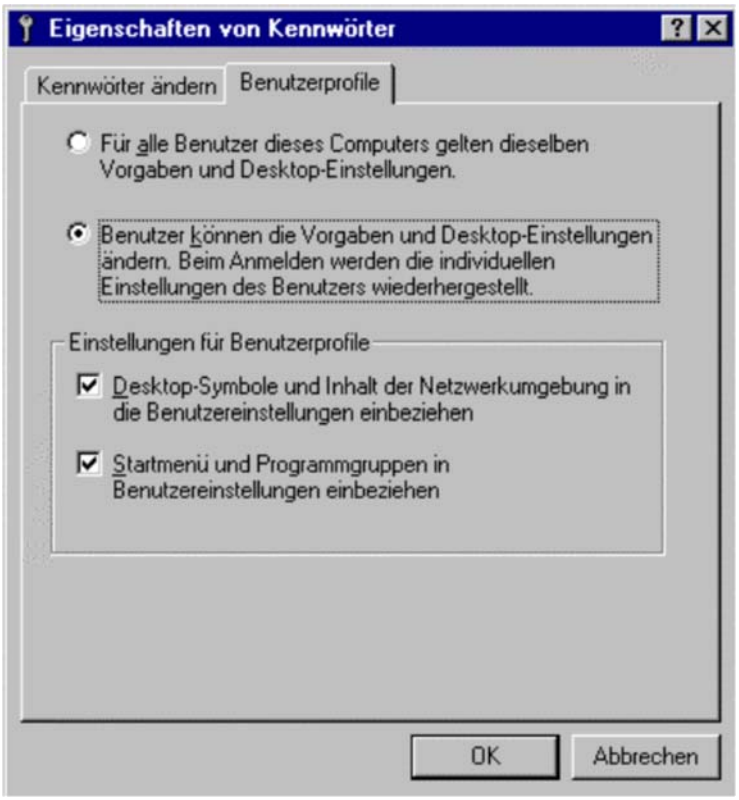


Abbildung: Maske Benutzerprofile

Hinweis: In Novell Netware- oder Windows NT-Netzen können verpflichtende Benutzerprofile angelegt werden, indem das entsprechende Profil in einem dem Benutzer zugeordneten Netzverzeichnis zugriffsgeschützt gespeichert wird. Dieses Profil hat den Namen *USER.MAN* und wird bei jeder Anmeldung am Server automatisch geladen (siehe M 4.51 *Benutzerprofile zur Einschränkung der Nutzungsmöglichkeiten von Windows NT*).

Ergänzende Kontrollfragen:

- Sollen an dem Windows 95 Rechner mehrere Benutzer arbeiten?
- Ist eine Benutzertrennung unter Sicherheitsgesichtspunkten oder aus organisatorischen bzw. prinzipiellen Gründen sinnvoll?

M 2.104 Systemrichtlinien zur Einschränkung der Nutzungsmöglichkeiten von Windows 95

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator

Soll unerfahrenen Benutzern das Navigieren unter Windows 95 erleichtert werden oder ist aus betrieblicher Sicht die Einschränkung bestimmter Ressourcen notwendig, so kann unter Windows 95 mit so genannten Systemrichtlinien die Benutzerumgebung benutzerspezifisch mit bestimmten Restriktionen versehen werden. Jedoch sollte berücksichtigt werden, dass Benutzer gegenüber dem IT-System möglicherweise eine abweisende Haltung einnehmen, wenn Einschränkungen nicht unmittelbar einsichtig sind. Eine Einschränkung sollte also nur dann erfolgen, wenn sie tatsächlich notwendig ist oder wenn sie vom Benutzer nicht bemerkt wird.

Sobald Systemrichtlinien aktiviert sind, wird beim Starten von Windows 95 überprüft, ob benutzerspezifische Einschränkungen für den aktuellen Benutzer eingerichtet wurden. Ist dies der Fall, werden diese geladen. Ist dies nicht der Fall, werden die Einschränkungen für den Standardbenutzer herangezogen. Im folgenden werden zunächst die prinzipiellen Einschränkungen beschrieben, die mit den **Systemrichtlinien** eingestellt werden können. Anschließend wird aufgezeigt, wie diese mittels des Systemrichtlinieneditors (*POLEDIT.EXE)* angelegt und aktiviert werden können.

Die wesentlichen mit Systemrichtlinien einzustellenden Restriktionen für einen nicht vernetzten Windows 95-Rechner sind:

- Der Zugriff auf die **Systemsteuerung** kann bezüglich der Optionen *ANZEIGE, NETZWERK, KENNWÖRTER, DRUCKEREINSTELLUNGEN* und *SYSTEM* eingeschränkt werden. Die jeweiligen Optionen können zum Teil vollständig deaktiviert oder auf einzelne Registerkarten beschränkt werden.

  Wesentlich bei diesen Optionen sind folgende Punkte:

  - Es können Vorgaben für Bildschirmfarben unter Ergonomiegesichtspunkten gemacht werden.
  - Es kann vorgesehen werden, eigene Kennwörter durch den Benutzer ändern zu lassen.
  - Druckerkonfiguration und Hardware-Einstellungen lassen sich fest vorgeben.

- Der Zugriff auf einzelne Funktionen der **Benutzeroberfläche** kann eingeschränkt werden. Beispielsweise können die Befehle *AUSFÜHREN, SUCHEN* und *BEENDEN* entfernt werden. Damit wird zum Beispiel verhindert, dass Benutzer nach sicherheitsrelevanten Dateien oder Programmen suchen und diese dann ggf. ausführen. Die Laufwerke lassen sich aus dem *ARBEITSPLATZ* und für den *EXPLORER* (dem früheren Dateimanager) ausblenden. Partitionen (Laufwerke) können dann ggf. nur noch

aus Anwendungen heraus gewechselt werden, da standardmäßig nur die Start-Partition (z. B. *C:*) zur Verfügung steht.

- Der **Programmstart** von ausführbaren Dateien kann eingeschränkt und die DOS-Eingabeaufforderung deaktiviert werden. Die für den einzelnen Benutzer erlaubten Anwendungen lassen sich explizit vorgeben (z. B. *WINWORD.EXE, EXCEL.EXE* und *EXPLORER.EXE*)

Zusätzlich kann für den Rechner gefordert werden, dass die Windows 95-Anmeldekennwörter sowohl aus Buchstaben als auch aus Sonderzeichen oder Zahlen bestehen müssen und welche Mindestlänge sie aufweisen sollen. Programme, die beim Systemstart ausgeführt werden sollen, lassen sich ebenfalls vorgeben.

Im folgenden wird in einzelnen Schritten gezeigt, wie Systemrichtlinien angelegt und aktiviert werden können und welche Restriktionen für einen nicht vernetzten Windows 95-Rechner Sicherheit bieten:

1. Anlegen einer Systemrichtliniendatei

Mit Hilfe des Systemrichtlinieneditors wird eine Systemrichtliniendatei erzeugt. Ihr Name ist zwar beliebig, jedoch wird an dieser Stelle der Einfachheit halber der Name *CONFIG.POL* gewählt. Dazu wird das Programm *POLEDIT.EXE* aufgerufen, eine neue Datei angelegt und diese unter dem Namen *CONFIG.POL* abgespeichert. Diese Datei enthält automatisch Einträge für den Standardbenutzer und den Standardcomputer, die im nächsten Schritt ggf. einzuschränken sind. Für den Administrator sind ebenfalls Einträge für den Computer und den Benutzer anzulegen (im Menü *BEARBEITEN* mit *BENUTZER HINZUFÜGEN* und *COMPUTER HINZUFÜGEN*), die im dritten Schritt zu spezifizieren sind.

Abbildung: Systemrichtlinien-Editor

2. Definition einer Richtlinie für den Standardbenutzer und Standardcomputer

Öffnet man mit dem Systemrichtlinieneditor die Einstellungen für den Standardbenutzer, so kann man menügeführt die entsprechenden sicherheitsrelevanten Einträge vornehmen.

Beispielsweise:

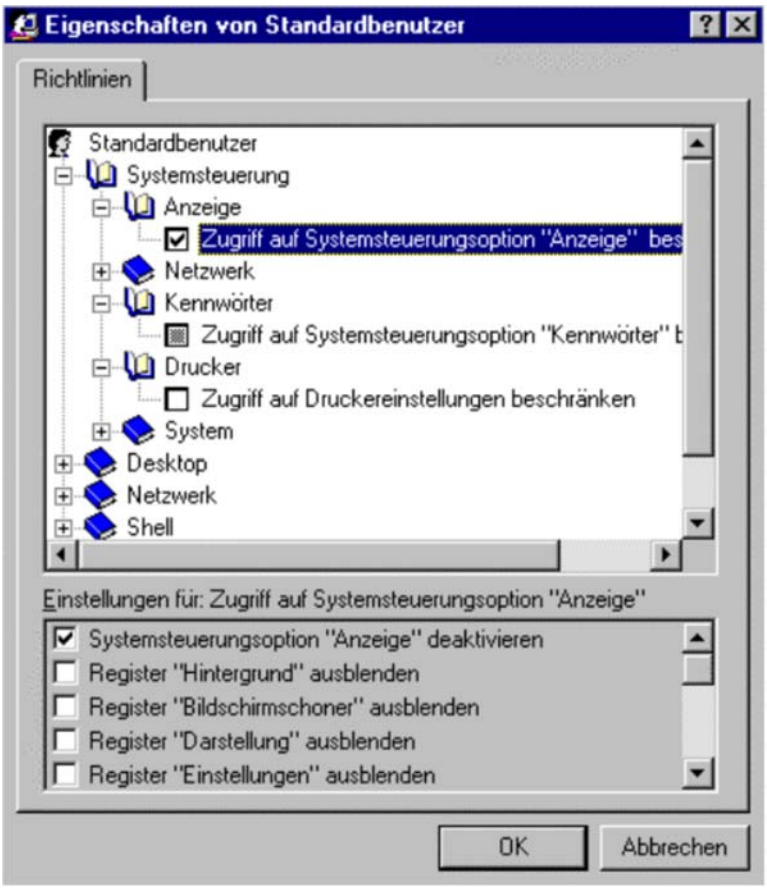


Abbildung: Maske Eigenschaften Standardbenutzer

Für einen **Standardbenutzer** sollten folgende Restriktionen eingestellt werden:

Systemsteuerung

- Der Zugriff auf die Registerkarte *BILDSCHIRMSCHONER* sollte dann deaktiviert werden, wenn der Benutzer die Bildschirmsperre nicht deaktivieren können soll. In diesem Fall ist ihm allerdings die Möglichkeit zu geben, das Bildschirmpasswort zu ändern. Dazu darf die *SYSTEMSTEUERUNG* (s. u.) nicht vollständig und bei der Option *KENNWÖRTER* die Registerkarte *KENNWORT ÄNDERN* nicht deaktiviert sein.
- Damit der Benutzer die Systemrichtlinien nicht deaktivieren kann, ist zwingend die Registerkarte *BENUTZERPROFILE* für die Systemsteuerungsoption *KENNWÖRTER* auszublenden.
- Die Einstellungen für die Hardware-Konfiguration sind vorzunehmen und der Zugriff auf die Register und Schaltflächen für die Systemsteuerungsoption *SYSTEM* maximal zu beschränken, damit fehlerhafte Konfigurationen durch den Benutzer vermieden werden, die die Verfügbarkeit oder Leistungsfähigkeit des Rechners einschränken können.

Shell-Zugriffsbeschränkungen

- Der Befehl *AUSFÜHREN* sollte deaktiviert werden, wenn verhindert werden soll, dass bestimmte Programme unter Angaben von Optionen gestartet werden können.
- Die *SYSTEM*- und *DRUCKERSTEUERUNG* kann vollständig deaktiviert werden, wenn man die Option *ORDNER UNTER "EINSTELLUNGEN" IM MENÜ "START" ENTFERNEN* aktiviert. Dies ist immer dann notwendig, wenn dem Benutzer jegliche Möglichkeit genommen werden soll, System- oder Druckereinstellungen zu ändern. Damit der Benutzer sein Bildschirmpasswort ändern kann, ist unter der Systemsteuerungsoption *ANZEIGE* die Registerkarte *BILDSCHIRMSCHONER* (siehe oben) freizugeben. Der Benutzer kann dann durch Klicken mit der rechten Maustaste auf den Desktop über *EIGENSCHAFTEN* auf die Bildschirmsperre zugreifen.
- Soll die Benutzung des *EXPLORERS* nicht erlaubt sein, so ist die Option *LAUFWERKE IM FENSTER "ARBEITSPLATZ" AUSBLENDEN* zu aktivieren, da der *EXPLORER* über den *ARBEITSPLATZ* gestartet werden kann, selbst wenn die Nutzung explizit verboten wurde.

System-Zugriffsbeschränkungen

- Die Option *PROGRAMME ZUM BEARBEITEN DER REGISTRIERUNG DEAKTIVIEREN* ist zu wählen.
  Hinweis: Diese Option betrifft nur den Registrierungseditor (*REGEDIT.EXE*). Mit dem Systemrichtlinien-Editor (*POLEDIT.EXE*) lässt sich die lokale Registrierung nach wie vor bearbeiten. Dieses Programm sollte daher von der Festplatte gelöscht werden.
- Es sollten nur zugelassene Anwendungen ausführbar sein.
  Es sind diejenigen Anwendungen, wie etwa *WINWORD.EXE*, *ACCESS.EXE*, *EXPLORER.EXE*, einzutragen, die der Benutzer ausführen können soll.
- Die MS-DOS-Eingabeaufforderung ist zu deaktivieren.
- Ggf. sind Single-Mode-Anwendungen für MS-DOS zu deaktivieren.
  Falls einige DOS-Anwendungen unter Windows 95 aufgerufen werden sollen, der Benutzer aber nicht auf die DOS-Ebene gelangen soll, ist die DOS-Eingabeaufforderung zu **aktivieren**, jedoch sind bei den zugelassenen Anwendungen für Windows nur diejenigen zu nennen, die benötigt werden. Die *COMMAND.COM* darf dann dort **nicht** genannt werden.

Für einen **Standardcomputer** sollten folgende Restriktionen eingestellt werden:

Netzwerk

- Unter *KENNWÖRTER* ist ein alphanumerisches Windows-Anmeldekennwort und eine Mindestlänge von sechs Zeichen zu fordern.
- Unter *UPDATE* ist *REMOTE-UPDATE* nicht zu deaktivieren, da sonst die Systemrichtlininen nicht geladen werden.

System

- Die *BENUTZERPROFILE* sind zu aktivieren.

3. Definition einer Richtlinie für den Administrator

In einer Richtlinie für den Administrator sollten keine der obigen Restriktionen gesetzt werden. Hierfür ist ein eigener Benutzer unter Windows 95 sowie ein Benutzer und Computer mittels Systemrichtlinien einzurichten, da sonst für ihn die über den Standardbenutzer eingestellten Einschränkungen gelten. Das dazugehörige Passwort darf nur dem Administrator und seinem Vertreter bekannt sein.

Diese Richtlinie ist ebenfalls in der Datei *CONFIG.POL* abzulegen.

4. Definition von Richtlinien für einzelne Benutzer basierend auf dem Standardbenutzer und Standardcomputer

Werden weitere Benutzer benötigt, deren Restriktionen sich von den unter 1. spezifizierten unterscheiden sollen, so sind analog zu 1. diese Richtlinien zusätzlich in der Datei *CONFIG.POL* einzurichten. Dazu kopiert man das Standardprofil, gibt diesem den Namen des betreffenden Benutzers und stellt die Restriktionen wie unter 1. für diesen Benutzer ein.

5. Aktivieren der Richtlinien

Beim Einrichten der Systemrichtlinien durch den Administrator ist besondere Vorsicht und Aufmerksamkeit geboten, da sehr leicht inkonsistente Systemzustände eingestellt werden können, die ein Arbeiten mit dem Rechner verhindern. Das Betriebssystem wäre neu zu installieren. Die Systemrichtlinien sollten also nur dann aktiviert werden, wenn die Richtlinien mit äußerster Sorgfalt definiert wurden.

Dazu öffnet der Administrator mit dem Systemrichtlinieneditor (*POLEDIT.EXE*) die lokale Registrierung und setzt dort für den *LOKALEN COMPUTER* unter der Option *NETZWERK-UPDATE* den Schalter *REMOTE-UPDATE*. Als Update-Modus muss *INTERAKTIV* gewählt werden. Der Pfad für die oben definierte *CONFIG.POL* ist ebenfalls anzugeben.

Die notwendigen Einstellungen können von besonders erfahrenen Administratoren auch mit dem Registrierungseditor (Programm *REGEDIT.EXE*) vorgenommen werden.

Darüber hinaus sind in der Programmgruppe *SYSTEMSTEUERUNG* mit der Schaltfläche *KENNWÖRTER* die Benutzerprofile zu aktivieren.

Ergänzende Kontrollfragen:

- Ist die Einschränkung der Benutzerumgebung aus betrieblicher Sicht notwendig?
- Ist die Einschränkung bestimmter Ressourcen notwendig?

M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Leiter IT, IT-Sicherheitsmanagement, Benutzer

Wird ein IT-System oder eine IT-Anwendung von mehreren Benutzern verwendet und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet. Ist es einem Dritten möglich, an einem IT-System oder in einer IT-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden. Aus technischen Gründen (z. B. damit alle offenen Dateien geschlossen werden) sollten auch dann Regelungen für die Abmeldung von IT-Systemen und IT-Anwendungen getroffen werden, wenn keine Zugriffskontrolle realisiert ist.

Bildschirmsperre

Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen (siehe auch M 4.2 *Bildschirmsperre*). Bei längerer Abwesenheit sollte die Bildschirmsperre automatisch aktiviert werden.

automatisches Abmelden

Einige IT-Systeme und IT-Anwendungen bieten die Möglichkeit, einen Zeitraum vorzugeben, nach dessen Ablauf ein Benutzer bei Inaktivität automatisch vom System abgemeldet wird. Es sollte überlegt werden, ob dieses Verfahren benutzt wird, da es auch zu Datenverlusten führen kann. Eine automatische Abmeldung kann z. B. bei PC-Pools mit starkem Publikumsverkehr zum Einsatz kommen, da hier ein angemeldeter Benutzer den Arbeitsplatz mit Hilfe der Bildschirmsperre unberechtigterweise blockieren kann.

Je nach Arbeitsplatzumgebung ist abzuwägen, welche Vorkehrungen für kurzfristige Abwesenheiten von Benutzern zu treffen sind. So sollte eine automatische Aktivierung der Bildschirmsperre bei Mehr-Benutzer-Systemen schneller erfolgen als bei solchen für einen Benutzer, also z. B. bereits nach 5 Minuten.

Ergänzende Kontrollfragen:

- Werden neue Mitarbeiter oder Vertreter gleichfalls verpflichtet?
- Wird an die Verpflichtung zum Abmelden regelmäßig erinnert?

M 4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement, Datenschutzbeauftragter, Verantwortliche der einzelnen IT-Anwendungen

Verantwortlich für Umsetzung: Beschaffungsstelle, Administrator

Je nachdem, welche Sicherheitsanforderungen an ein IT-System gestellt werden, reichen eventuell die vorhandenen Sicherheitsfunktionalitäten nicht aus, so dass zusätzlich geeignete Sicherheitsprodukte eingesetzt werden sollten. Typische Beispiele dafür sind Zugangskontrolle, Zugriffsrechteverwaltung und -prüfung, Protokollierung oder Verschlüsselung.

Bei IT-Systemen muss beispielsweise sichergestellt werden, dass

- nur autorisierte Personen das IT-System benutzen können (siehe auch BDSG, Zugangskontrolle). Hierfür sind geeignete Authentisierungsmechanismen auszuwählen.
- die Benutzer auf die Daten nur in der Weise zugreifen können, die sie zur Aufgabenerfüllung benötigen. Hierbei unterstützen geeignete Benutzertrennung und Rechtevergabe.
- Unregelmäßigkeiten und Manipulationsversuche erkennbar werden. Hierbei helfen Protokollierungsfunktionen, Verschlüsselung und digitale Signatur.
- Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle). Hierbei unterstützen beispielsweise Backup-Programme.

Reichen die Protokollierungsmöglichkeiten des IT-Systems nicht aus, um eine ausreichende Beweissicherung zu gewährleisten, so müssen diese nachgerüstet werden. Hierzu gibt es auch verschiedene Gesetze, die dies erfordern. Beispielsweise ist nach BDSG, bei der Eingabekontrolle "zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind".

Ist es mit dem IT-System nicht möglich, den Administrator daran zu hindern, auf bestimmte Daten zuzugreifen oder zumindest diesen Zugriff zu protokollieren und zu kontrollieren, dann kann z. B. mit einer Verschlüsselung der Daten verhindert werden, dass der Administrator diese Daten im Klartext liest, wenn er nicht im Besitz des zugehörigen Schlüssels ist.

Empfohlene Mindestfunktionalitäten:

IT-Systeme sollten mindestens die folgenden Sicherheitseigenschaften besitzen. Wenn diese nicht im Standardumfang vorhanden sind, sollten diese über zusätzliche Sicherheitsprodukte nachgerüstet werden.

- *Identifikation und Authentisierung*: Es sollte eine Sperre des Systems nach einer vorgegebenen Anzahl fehlerhafter Authentisierungsversuche statt finden, die nur ein Administrator zurücksetzen kann. Wird ein

Passwort verwendet, sollte das Passwort mindestens acht Stellen umfassen und darf nicht unverschlüsselt im System gespeichert werden.

- *Rechteverwaltung und -kontrolle*: Es sollte eine Rechteverwaltung und -kontrolle auf Festplatten und Dateien vorhanden sein, wobei zumindest zwischen lesendem und schreibendem Zugriff unterschieden werden soll. Für Benutzer sollte kein Systemzugriff auf Betriebssystemebene möglich sein.
- *Rollentrennung zwischen Administrator und Benutzer*: Es sollte eine klare Trennung zwischen Administrator und Benutzer möglich sein, wobei nur der Administrator Rechte zuweisen oder entziehen können sollte.
- *Protokollierung* der Vorgänge Anmelden, Abmelden und Rechteverletzung sollte möglich sein.
- *Automatische Bildschirmsperre*: Nach zeitweiser Inaktivität der Tastatur oder Maus sollte eine Bildschirmsperre automatisch aktiv werden. Diese sollte sich auch direkt aktivieren lassen. Der erneute Zugriff auf das IT-System darf erst nach erfolgreicher Identifikation und Authentisierung wieder möglich sein.
- *Boot-Schutz* soll verhindern, dass der Rechner unbefugt von anderen Medien gebootet werden kann.

Sollte ein oder mehrere dieser Sicherheitsfunktionalitäten nicht vom Betriebssystem unterstützt werden, so müssen ersatzweise geeignete zusätzliche Sicherheitsprodukte eingesetzt werden.

Zusätzliche Forderungen an Sicherheitsprodukte:

- *Benutzerfreundliche Oberfläche* zur Erhöhung der Akzeptanz.
- Aussagekräftige und nachvollziehbare Dokumentation für Administrator und Benutzer.

Wünschenswerte Zusatzfunktionalität von Sicherheitsprodukten:

- *Rollentrennung zwischen Administrator, Revisor und Benutzer;* nur der Administrator kann Rechte zuweisen oder entziehen und nur der Revisor hat Zugriff auf die Protokolldaten,
- *Protokollierung* von Administrationstätigkeiten,
- *Unterstützung der Protokollauswertung* durch konfigurierbare Filterfunktionen,
- *Verschlüsselung* der Datenbestände mit einem geeigneten Verschlüsselungsalgorithmus und in einer Weise, dass ein Datenverlust bei Fehlfunktion (Stromausfall, Abbruch des Vorgangs) systemseitig abgefangen wird.

Die Realisierung dieser Funktionalität kann sowohl in Hardware wie auch in Software erfolgen. Bei der Neubeschaffung eines Produktes sollte Maßnahme M 2.66 *Beachtung des Beitrags der Zertifizierung für die Beschaffung* berücksichtigt werden.

Übergangslösung:

Sollte es nicht möglich sein, kurzfristig ein geeignetes Sicherheitsprodukt zu beschaffen, sind andere geeignete Sicherheitsmaßnahmen zu ergreifen. Diese sind dann typischerweise organisatorischer Natur und müssen von den Benutzern konsequent eingehalten werden. Wenn ein IT-System beispielsweise keine Bildschirmsperre hat, muss dieses in den kurzen Phasen, wo es nicht benutzt wird, ein- oder weggeschlossen werden.

Ergänzende Kontrollfragen:

- Wurde vor der Beschaffung von IT-Systemen überprüft, ob diese angemessen Sicherheitsfunktionalitäten bieten?

M 4.56 Sicheres Löschen unter Windows-Betriebssystemen

Verantwortlich für Initiierung: IT-Sicherheitsmanagement, Administrator

Verantwortlich für Umsetzung: Benutzer, Administrator

Windows NT/2000/XP/Server 2003

Das Windows Dateisystem NTFS legt in einer Master Dateitabelle (MFT) alle Dateiinformationen wie Namen, Pfad und Attribute ab. Diese Angaben werden nicht verschlüsselt. Programme, die direkt auf die Festplatte zugreifen können, können unter Umgehung der Sicherheitsmechanismen von Windows NT/2000/XP/Server 2003 auf alle Dateien beliebig zugreifen. Dies gilt insbesondere für Programme, die unter einem anderen Betriebssystem als Windows auf demselben Rechner laufen.

Beim Löschen einer Datei unter dem Dateisystem NTFS wird diese nicht physikalisch gelöscht oder überschrieben, sondern lediglich dem Zugriff entzogen, wobei jedoch unter Windows NTFS - im Gegensatz zu der Situation bei MS-DOS - sichergestellt ist, dass ein Zugriff auf diese gelöschten Daten, etwa mit einem Rekonstruktionsprogramm oder unter Verwendung direkter Plattenzugriffe, nicht mehr möglich ist. Dennoch können gelöschte Dateien unter anderen Betriebssystemen als Windows mit Programmen, die direkt auf die Festplatte zugreifen können, wieder hergestellt werden.

Aus diesen Gründen muss Windows als einziges Betriebssystem installiert sein, und es muss verhindert werden, dass andere Betriebssysteme gestartet werden können (siehe auch M 4.52 *Geräteschutz unter NT-basierten Windows-Systemen* und M 4.55 *Sichere Installation von Windows NT*).

Papierkorb unter Windows

Unter Windows werden Dateien beim Löschen, sofern der Benutzer nicht ausdrücklich ein direktes Löschen verlangt, zunächst in einen benutzerspezifischen Bereich, den sogenannten "Papierkorb", verlagert. Aus diesem Bereich werden sie erst dann entfernt, wenn der von gelöschten Dateien belegte Speicherplatz die für das betreffende Plattenlaufwerk vorgegebene Größe überschreitet oder wenn der Benutzer explizit den Papierkorb leert. Der Inhalt des Papierkorbs sollte daher regelmäßig gelöscht werden, damit die Festplatte nicht zu voll wird und der Benutzer nicht den Überblick verliert. Die maximale Größe des für den Papierkorb reservierten Speicherplatzes kann auch unter "*Eigenschaften*" des Icons "Papierkorb" auf einen geeigneten kleineren Wert, z. B. 2 MByte, eingestellt werden. Dateien mit sensitivem Inhalt sollten nicht in den Papierkorb verschoben werden, sondern explizit gelöscht werden, indem beim Löschen die Umschalttaste gedrückt wird.

Unter Windows besteht zudem die Möglichkeit aus dem Papierkorb gelöschte Dateien durch Hilfsprogramme zu rekonstruieren. Dateien mit besonders sensitivem Inhalt sollten daher vollständig überschrieben werden statt sie in den Papierkorb zu verschieben (siehe M 2.3 *Datenträgerverwaltung*).

Windows XP/Server 2003 bietet die Möglichkeit an, die Dateien direkt und nicht über den Papierkorb zu löschen. Direktes Löschen von Dateien kann in Eigenschaften des Papierkorbs (*Dateien sofort löschen*) oder durch das Aktivieren der Richtlinie *Benutzerkonfiguration* | *Administrative Vorlagen* | *Windows-Komponenten* | *Windows Explorer* | *Gelöschte Dateien nicht in Papierkorb verschieben* erzwungen werden. Hierauf sollten die Benutzer hingewiesen werden.

Unter Windows XP/Server 2003 ist es möglich, den gesamten freien Plattenplatz eines Datenträgers oder eines Unterverzeichnisses mit dem Kommando *cipher.exe /w* zu überschreiben. *cipher.exe* macht insgesamt drei Schreibdurchgänge und überschreibt den freigegebenen Platz im ersten Durchgang mit 0x0, im zweiten mit 0xF und im dritten mit pseudo-zufälligen Daten. Bei der Benutzung dieses Kommandos soll jedoch berücksichtigt werden, dass die Inhalte kleiner Dateien (unter 4 KB), die gelöscht wurden, unüberschrieben bleiben können, wenn sie direkt in der Master File Table (MFT) und nicht in separaten Datenträger-Clustern abgelegt sind. Das Verfahren ist auch geeignet, um verschlüsselte Dateien von unverschlüsselt zwischengespeicherten Datenresten zu bereinigen.

Damit Dateien tatsächlich unwiederbringlich gelöscht werden, sollten spezielle Löschprogramme eingesetzt werden, mit denen alle Restinformationen zu dieser Datei auf dem Datenträger überschrieben werden.

Ergänzende Kontrollfragen:

- Ist die Größe des Papierkorbs auf einen sinnvollen Wert eingestellt?
- Sind alle Benutzer darüber informiert, dass über den Papierkorb gelöschte Dateien nicht zuverlässig gelöscht sind?

M 4.57 Deaktivieren der automatischen CD-ROM-Erkennung

Verantwortlich für Initiierung: IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Unter Windows können CD-ROMs automatisch erkannt und bearbeitet werden. Dadurch können auch auf der CD-ROM gespeicherte Programme automatisch auf dem Rechner ausgeführt werden. Die automatische CD-ROM-Erkennung sollte daher *permanent* unterbunden werden.

Unter Windows 95 ist dafür auf der Registerkarte GERÄTEMANAGER unter der Systemsteuerungsoption SYSTEM für die CD-ROM die Eigenschaft *Automatische Benachrichtigung beim Wechsel* zu deaktivieren.

Unter Windows NT 4.0 und Windows 2000 ist für die permanente Deaktivierung der automatischen CD-ROM-Erkennung in der Registrierung der Eintrag *Autorun* im Schlüssel *SYSTEM \ CurrentControlSet \ Services \ CD-ROM* im Bereich *HKEY_LOCAL_MACHINE* auf den Wert *REG_WORD = 0* zu setzen. Unter Windows XP kann dies auch durch das Setzen der Richtlinie *Computerkonfiguration | Administrative Vorlagen | System | Autoplay deaktivieren* auf den Wert *Alle Laufwerke* erfolgen. Die Deaktivierung der automatischen CD-ROM-Erkennung kann auch auf Benutzerbasis erfolgen (Richtlinie *Benutzerkonfiguration | Administrative Vorlagen | System | Autoplay deaktivieren*). Die Richtlinien können sowohl in lokalen als auch Active Directory-basierten Gruppenrichtlinien definiert werden.

Falls die automatische CD-ROM-Erkennung nicht generell deaktiviert wird, sollte dies dokumentiert werden. Im Einzelfall kann die automatische CD-ROM-Erkennung *für jede CD-ROM einzeln* durch Drücken der Shift-Taste beim Einlegen verhindert werden. Erfahrungsgemäß wird dies in der Praxis allerdings selten gemacht.

Ergänzende Kontrollfragen:

- Ist die automatische CD-ROM-Erkennung ausgeschaltet?
- Sind die Benutzer informiert, wie sie die automatische CD-ROM-Erkennung temporär verhindern können?

M 4.74 Vernetzte Windows 95 Rechner

Verantwortlich für Initiierung: Leiter IT

Verantwortlich für Umsetzung: Administrator

Werden Windows 95 Rechner in einem Netz betrieben (Novell Netware oder Windows NT), so sollte die Möglichkeit genutzt werden, die jeweiligen Systemrichtlinien auf Netzservern zu speichern und diese dort zentral zu verwalten.

Mit Hilfe der SYSTEMSTEUERUNG unter NETZWERK wird hierbei die primäre Netzwerkanmeldung, d. h. der Pfad für die Systemrichtlinien festgelegt. Standardmäßig werden die Benutzerprofile auf einem Novell Netware Server unter SYS:PUBLIC abgelegt. Erfolgt die primäre Netzanmeldung an einem Windows NT Rechner, so werden die Benutzerprofile standardmäßig unter NETLOGON (*%SystemRoot%\SYSTEM32\REPL\IMPORT\SCRIPTS*) abgelegt.

Die Aktivierung der Benutzerprofile wird mit Hilfe der SYSTEMSTEUERUNG-KENNWÖRTER-BENUTZERPROFILE sichergestellt.

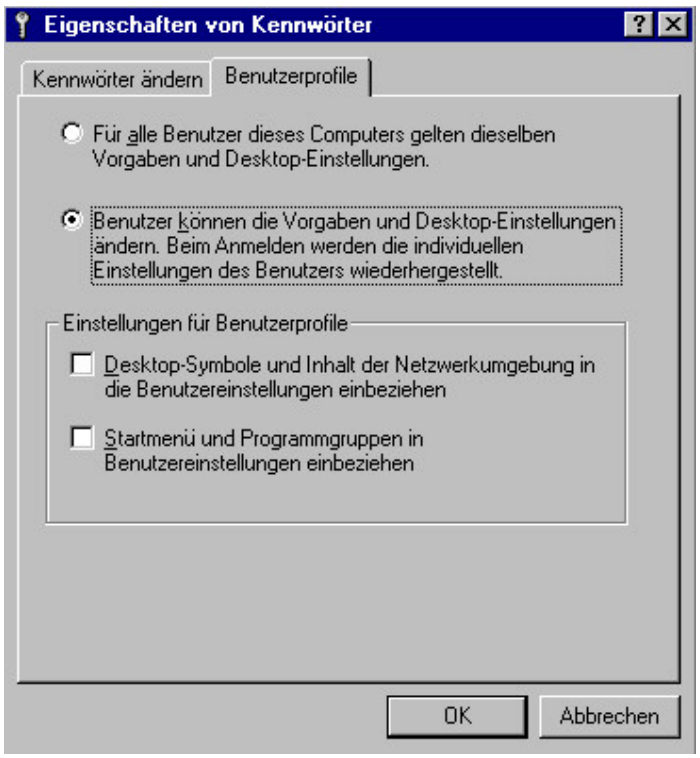


Abbildung: Eigenschaften von Kennwörtern

Weiterhin sollte zudem der Betrieb von Windows 95 ohne Netzwerkanmeldung gesperrt werden um eine Umgehung der Systemrichtlinien auf lokaler Basis zu verhindern. Hierzu sollte mit Hilfe von *POLEDIT.EXE* unter lokaler Computer-Netzwerk-Anmeldung die Option *NETZWERKBESTÄTIGUNG FÜR WINDOWS ZUGRIFF FORDERN* aktiviert werden.

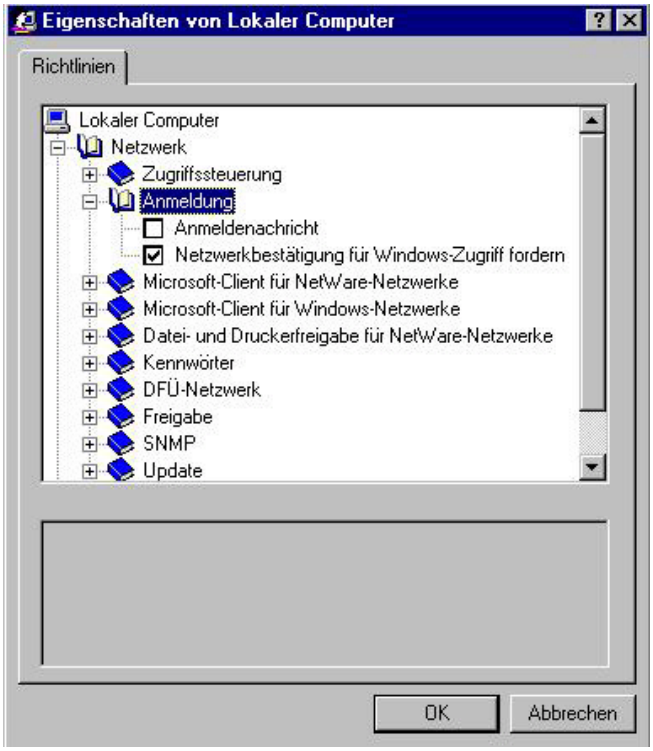


Abbildung: Eigenschaften von Lokaler Computer

Gruppenrichtlinien werden unter Windows 95 über SYSTEMSTEUERUNG-SOFTWARE-WINDOWS-SETUP installiert und befinden sich standardmäßig in dem Verzeichnis

ADMIN\APPTOOLS\POLEDIT\GROUPPOL.INF.

Die Namen der jeweiligen Benutzergruppen müssen hierbei den eingerichteten Benutzergruppen unter Novell Netware bzw. Windows NT entsprechen.

Um den ordnungsgemäßen IT-Betrieb sicherzustellen, sollte zusätzlich beachtet werden, dass das Programm *POLEDIT.EXE* nicht auf dem lokalen Windows 95 Rechner installiert werden darf, da mit diesem Programm die gültigen Systemrichtlinien von jederman dauerhaft verändert werden können.

Ebenso sollte in der Datei MSDOS.SYS der Wert BootKeys verändert werden (BootKeys=1) um den Start von Windows 95 im "abgesicherten Modus" zu unterbinden. Dies verhindert, dass die Systemrichtlinien nicht zur Anwendung kommen.

Das BIOS des Computers sollte zudem einen Systemboot über Diskette verhindern, sowie das Diskettenlaufwerk mit einem Schloss versperrt werden, um Einsatz von unautorisierter Software zu erschweren.

M 6.45 Datensicherung unter Windows 95

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Benutzer

Generell zu beachten sind die Anforderungen aus M 6.32 *Regelmäßige Datensicherung*. Nachfolgend soll aufgezeigt werden, welche besonderen Aspekte unter Windows 95 zu berücksichtigen sind.

Unter Windows 95 sollten nach Möglichkeit nur Programme zur Datensicherung eingesetzt werden, die lange Dateinamen unterstützen (zum Beispiel das Windows 95 Programm *BACKUP.EXE*). Zur Konvertierung langer Dateinamen in die 8.3-Dateinamen-Konvention steht das zum Lieferumfang gehörenden Programm *LFNBK.EXE* zur Verfügung. Allerdings ist beim Einsatz dieses Programmes besondere Vorsicht geboten, da möglicherweise Dateinamen oder sogar einzelne Dateien nicht rekonstruiert werden können, falls nach der Sicherung Veränderungen an der Verzeichnisstruktur auf dem PC, von dem gesichert wurde, vorgenommen worden sind.

Ergänzende Kontrollfrage:

- Werden Programme zur Datensicherung eingesetzt, die lange Dateinamen nicht verarbeiten können?

M 6.46 Erstellung von Rettungsdisketten für Windows 95

Verantwortlich für Initiierung: Leiter IT, IT-Sicherheitsmanagement

Verantwortlich für Umsetzung: Administrator, Benutzer

Für jeden Windows 95-Rechner sollten Rettungsdisketten erstellt werden, um bei Systemproblemen den Rechner wieder starten und ggf. benutzerspezifischen Profile wieder herstellen zu können.

Dazu benötigt man zum einen eine startfähige Systemdiskette, die für alle Rechner gemeinsam genutzt werden kann, zum anderen eine rechner- und benutzerspezifische Diskette, die die individuellen Einstellungen des Benutzers und des jeweiligen Rechners enthält.

Erzeugen der startfähigen Systemdiskette

Eine für alle Rechner nutzbare Systemdiskette kann mit der Registerkarte *STARTDISKETTE* unter der Systemsteuerungsoption *SOFTWARE* erzeugt werden. Allerdings benötigt man dazu eine Windows 95 CD. Stattdessen kann der erfahrene Benutzer alle relevante Dateien auch manuell auf die Diskette kopieren. Dazu gehören beispielsweise *COMMAND.COM*, *IO.SYS*, *DRVSPACE.BIN* und *MSDOS.SYS*. In diesem Fall sollten außerdem der deutsche Tastaturtreiber *KEYB.COM* sowie *KEYBOARD.SYS*, *COUNTRY.SYS* und ggf. weitere Systemdateien (z. B. einen CD-ROM-Treiber) kopiert werden. Die deutsche Tastatur stellt man dann mit dem Befehl *KEYB GR,,KEYBOARD.SYS* ein. Für andere notwendige Dateien, z. B. einen Editor, Programme zur Festplattendekomprimierung oder Backup-Programme, kann ggf. eine zusätzliche Diskette verwendet werden.

Erzeugen von rechner- und benutzerspezifischen Disketten

Hierzu wird für jeden Rechner eine vorformatierte Diskette und das Programm *EMERGENCY RECOVERY UTILITY (ERU)* benötigt, welches zum Systemumfang gehört. Dieses wird zwar nicht standardmäßig installiert, befindet sich aber auf der mitgelieferten Windows 95 CD-ROM. Mit diesem Programm lassen sich in einfacher Weise die relevanten und aktuellen Systemdateien, insbesondere die Datei mit den Benutzereinstellungen *USER.DAT* bzw. die Datei mit den Systemeinstellungen *SYSTEM.DAT*, auf Diskette kopieren. Die Dateien *USER.DAT* und *SYSTEM.DAT* beinhalten die entsprechenden Informationen, die unter Windows 3.x in den *ini*-Dateien gespeichert sind. Diese Diskette sollte bei umfangreichen oder wichtigen Änderungen an der Rechnerkonfiguration oder an den Benutzereinstellungen aktualisiert werden.

Nach dem Erstellen der Rettungsdisketten sollten diese auf Computer-Viren überprüft und danach schreibgeschützt werden.

Nutzung der Start-Diskette

Um von der Systemdiskette zu starten, wird diese in das Diskettenlaufwerk eingelegt, die Start-Reihenfolge im BIOS zugunsten des Diskettenlaufwerkes

priorisiert und der Rechner neu gestartet. Der Rechner fährt dann im Zeilenmodus hoch.

Nutzung der rechner- und benutzerspezifischen Diskette

Falls der Rechner ordnungsgemäß startet (mit oder ohne Start-Diskette), die rechner- und benutzerspezifischen Dateien jedoch zerstört sind, können diese mit dem Programm *ERD.EXE*, das sich auf der rechner- und benutzerspezifischen Diskette befindet, zurückgespielt werden. Die korrespondierende Dateien auf der Festplatte werden zuvor in das Verzeichnis *C:\WINDOWS\ERUNDO* verschoben und können mit den Befehl *ERD /UNDO* ggf. rekonstruiert werden.

Hinweis: Für die Nutzung des Programmes *ERD.EXE* ist es notwendig, den Rechner im Zeilenmodus zu starten. Dies erreicht man zum Beispiel, indem man von der Startdiskette startet, beim Beenden von Windows 95 *COMPUTER IM MS-DOS MODUS STARTEN* wählt oder beim Starten des Rechners während der Nachricht "Windows 95 wird gestartet" die F8-Taste betätigt und anschließend"*5. Nur Eingabeaufforderung*" wählt. Letzteres ist allerdings nur dann möglich, wenn in der Datei *MSDOS.SYS* die Zeile **BootKeys=1** eingetragen ist.

Ergänzende Kontrollfragen:

- Wurde für Windows 95 Rechner eine startfähige Systemdiskette erstellt?
- Wurde für **jeden** Windows 95 Rechner eine rechner- und benutzerspezifische Rettungsdiskette erstellt?