Fraunhofer Institut
Experimentelles
Software Engineering

Analyse von Programmwerkzeugen zur Unterstützung von Schwachstellenanalysen im Bereich IT-Sicherheit

Autor:
Gregor Blanz

IESE-Report Nr. 052.02/D
Version 1.0
Oktober 2002

Eine Publikation des Fraunhofer IESE

Das Fraunhofer IESE ist ein Institut der Fraunhofer-Gesellschaft.
Das Institut überträgt innovative Software-Entwicklungstechniken, -Methoden und -Werkzeuge in die industrielle Praxis. Es hilft Unternehmen, bedarfsgerechte Software-Kompetenzen aufzubauen und eine wettbewerbsfähige Marktposition zu erlangen.

Das Fraunhofer IESE steht unter der Leitung von
Prof. Dr. Dieter Rombach
Sauerwiesen 6
67661 Kaiserslautern

Inhaltsverzeichnis

1	**Einleitung**	**1**
1.1	Motivation	1
1.2	Untersuchte Werkzeuge zur Schwachstellenanalyse	1
1.3	Vorgehensweise	2
1.4	Aufbau der Arbeit	3
2	**Analyse der Schwachstellenanalysewerkzeuge**	**4**
2.1	Die Werkzeuge und Hersteller im Überblick	4
2.2	Allgemeine Eigenschaften der untersuchten Programmwerkzeuge	6
2.3	Funktionen der untersuchten Programmwerkzeuge	7
2.4	Zusammenfassung der Werkzeugeigenschaften	12
3	**Kosten-/Nutzen-Analyse**	**13**
3.1	Nutzwertanalyse	13
3.2	Szenario für eine Kosten-/Nutzenberechnung	15
4	**Literatur**	**18**
5	**Anhang**	**19**

Copyright © Fraunhofer IESE 2002

1 Einleitung

1.1 Motivation

Die Wahrung der IT-Sicherheit ist nach dem Stand der Praxis eine Herausforderung für IT-Hersteller und Betreiber, da es keine Sicherheit ohne Schwachstellen gibt. Unter Schwachstellen versteht man beispielsweise mangelhafte Software, schlecht konfigurierte und administrierte Systeme oder Sicherheitsprobleme der Kommunikationsprotokolle und Passwörter.

Bei der Gestaltung eines effizienten und Sicherheitsprogramms für die Informationstechnologie spielt die Schwachstellenanalyse eine wesentliche Rolle. Unternehmen brauchen sie, um ihren aktuellen Sicherheitsstatus mit der von ihnen angestrebten Sicherheitsstufe zu vergleichen und zu bewerten. Ziel ist es, ein umfassendes und verständliches Bild der Einhaltung von Sicherheitsrichtlinien innerhalb der IT-Infrastruktur zu liefern.

Bisher mangelte es an systematischen, effizienten Verfahren, um verlässliche Sicherheitsanalysen durchzuführen. Das Aufspüren und Beheben von Sicherheitsschwachstellen ist ein hochkreativer Prozess, der erhebliches Spezialwissen, Erfahrung und auch ein gewisses Maß an Intuition erforderte. Schwachstellen-Analysewerkzeuge schaffen Abhilfe. Sie ermöglichen und erleichtern es dem Administrator, Schwachstellen aufzuspüren, den aktuellen Sicherheitsstatus mit Sicherheitsrichtlinien des Unternehmens zu vergleichen und dementsprechende Maßnahmen einzuleiten.

1.2 Untersuchte Werkzeuge zur Schwachstellenanalyse

Verschiedene Firmen bieten Werkzeuge zur Unterstützung von Schwachstellenanalysen im Bereich IT-Sicherheit an. Ziel des Projekts war es, drei dieser Programmwerkzeuge zu analysieren und zu vergleichen. Zu diesem Zweck wurden das Tool **NIXE™** vom Fraunhofer Institut für Experimentelles Software Engineering (IESE), das UNIX Security Enhancement and Information Tool (**USEIT**) Version 2.0 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Symantec Enterprise Security Manager 5.5 (**ESM**) einander gegenüber gestellt:

– **NIXE™**-: Für UNIX-Plattformen hat das Fraunhofer IESE das Revisionswerkzeug NIXE™ konzipiert und entwickelt. Das im Jahr 2001 mit dem rheinland-pfälzischen Innovationspreis ausgezeichnete Programmwerkzeug dient dazu, sicherheitsrelevante Schwachstellen in der Konfiguration eines UNIX-Systems aufzuspüren. Es vergleicht die Systemkonfiguration mit den Prüf-

Copyright © Fraunhofer IESE 2002

vorgaben und fasst alle festgestellten Mängel in einem Prüfprotokoll zusammen. Die Idee besteht darin, die Werkzeugkonfiguration von einem Referenzsystem abzuleiten, das den zu prüfenden IT-Systemen entspricht. **NIXE™** extrahiert in einem Konfigurationslauf die relevanten Sicherheitsmerkmale des Referenzsystems und bildet daraus entsprechende Prüfvorgaben.

– **USEIT**: Das im Auftrag des BSI entwickelte Tool USEIT unterstützt den Administrator bei der Verwaltung von UNIX-Systemen hinsichtlich von Sicherheitsaspekten. Dem IT-Sicherheitsbeauftragten wird die Möglichkeit gegeben, die Sicherheit der eingesetzten Systeme zu prüfen und mit Hilfe der mitgelieferten Informationsdatenbestände zu beurteilen. Neben der Prüfung der Grundsicherheitseinstellungen können, Auswertungen für spezielle Einsatzumgebungen wie Server im Internet oder minimal installierte UNIX-Systeme für spezielle Anwendungen durchgeführt werden.

– **ESM**: Mit dieser Lösung können IT-Administratoren und Sicherheitsexperten die Richtlinien für die Netzwerksicherheit ihres Unternehmens zentral planen, umsetzen und von jedem beliebigen Standort aus überwachen. Das Tool überprüft die Einhaltung der Sicherheitspolitik in wichtigen E-Business-Anwendungen und Betriebssystemen im gesamten Unternehmen und erkennt Sicherheitslücken und Abweichungen von definierten Sicherheitsrichtlinien in Diensten, die wichtige Anwendungen und Daten im Netzwerk bereitstellen.

1.3 Vorgehensweise

Am Anfang des Projekts findet eine eingehende Informationsrecherche statt. Dabei werden zunächst über das Internet Nachforschungen über die Hersteller der Programmwerkzeuge sowie über die Werkzeuge selbst angestellt Handbücher **NIXE™**, **USEIT** und **ESM**. Des weiteren halfen Artikel und Fachbücher zum Thema IT-Sicherheit, sich einen Einstieg in die Thematik zu verschaffen Bruce Schneier 2001 und Kai Fuhrberg1998. Durch Fachgespräche mit Fraunhofer IESE Mitarbeitern, die wesentlich an der **NIXE™**-Entwicklung beteiligt waren, konnten ebenfalls erste Informationen bezüglich Schwachstellenanalyse-Tools eingeholt werden.

Die Programmwerkzeuge **USEIT** und Symantec **ESM** wurden von den jeweiligen Herstellern bezogen, d.h. beim BSI bzw. der Firma Symantec. Das Werkzeug **NIXE™** wurde vom Fraunhofer IESE zur Verfügung gestellt. Es gilt zu beachten, dass es sich bei den untersuchten Programmwerkzeugen um Testversionen handelt, die bei einer Laufzeit von vier Wochen lediglich eingeschränkt nutzbar sind.

Copyright © Fraunhofer IESE 2002

Nach der Produktinstallation durch den Systemadministrator werden zunächst mit Hilfe der Handbücher allgemeine Tool-Eigenschaften verglichen. Dies umfaßte Kriterien wie z. B. Dokumentation, Konfiguration und Installation, eventuell erforderliche Grundkenntnisse der User, Systemvoraussetzungen sowie die Darstellung der Auswertungsergebnisse. Im Anschluss daran werden die Prüfwerkzeuge im Hinblick auf ihre Funktionen untersucht. Mit Hilfe der Handbücher und Testläufe der einzelnen Programme werden die verschiedenen Prüfmodule beschrieben und einander gegenübergestellt. Die Analyseergebnisse werden schließlich in tabellarischer Form dokumentiert. Dies ermöglichte einen direkten Vergleich der Schwachstellen-Analysewerkzeuge **NIXE™,** Symantec **ESM** und **USEIT**.

Die Wirtschaftlichkeit einer Schwachstellenanalyse wurde durch eine Kosten-Nutzen-Analyse untersucht. In Gesprächen mit IESE-Mitarbeitern wurden relevante Angaben und Zahlen für ein passendes Szenario erarbeitet. Diese steht einer Schachstellenanalyse, die mit Hilfe des Programmwerkzeuges **NIXE™** durchgeführt wird, einer manuellen Analyse gegenüber.

1.4 Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich folgendermaßen:

- In Kapitel 2 werden die Schwachstellenanalysewerkzeuge **NIXE™**, **USEIT** und Symantec **ESM** analysiert und miteinander verglichen. Als Einstieg wird im Kapitel 2.1 zunächst ein Überblick über die Werkzeuge und deren Hersteller gegeben. Im Anschluss daran sind zum einen die allgemeinen Eigenschaften der untersuchten Programmwerkzeuge aufgelistet (2.2), zum anderen ihre wichtigsten Funktionen (2.3). Kapitel 2.4 gibt schließlich eine Zusammenfassung der Werkzeuge.

- Kapitel 3 untersucht durch eine Kosten-Nutzen-Analyse die Wirtschaftlichkeit der mit Hilfe der Programmwerkzeuge durchgeführten Schwachstellenanalyse.

- Im Anhang werden die Start- und Auswertungsanzeigen der jeweiligen Programmwerkzeuge in Form von Screenshots mit kurzen Erläuterungen präsentiert.

Copyright © Fraunhofer IESE 2002

2 Analyse der Schwachstellenanalysewerkzeuge

2.1 Die Werkzeuge und Hersteller im Überblick

Tabelle 1 gibt einen Überblick der Literaturrecherche über die untersuchten Programmwerkzeuge und deren Hersteller.

	Fraunhofer IESE	**Symantec**	**BSI**
Kontaktdaten	Fraunhofer IESE Sauerwiesen 6 D-67661 Kaiserslautern Tel: +49-(0)6301 707 166 Fax: +49-(0)6301 707 200 E-Mail: info@iese.fraunhofer.de URL: http://www.iese. fraunhofer.de	Symantec GmbH, Kaiserswerther Str.115 D-40880 Ratingen Tel: +49 (0) 2102 7453 0 Fax: +49 (0) 2102 7453 922 URL: http://www.symantec.de	BSI Postfach 200363 D-53133 Bonn Tel: +49 (0)1888 9582-0 Fax: +49 (0)1888 9582-400 E-Mail: bsi@bsi.bund.de URL: http://www.bsi.de
Unterneh-mensprofil	Das Fraunhofer-Institut für Experimentelles Software Engineering in Kaiserslautern konzentriert sich seit 1996 auf angewandte Forschung und Technologietransfer in verschiedenen Bereichen des Software Engineering. Dazu werden neue Techniken, Methoden, Verfahren und Werkzeuge erarbeitet, die die industrielle Software-Entwicklung auf eine solide ingenieurwissenschaftliche Basis stellen. Branchen- und größenunabhängig werden Firmen bei der Verbesserung ihrer Software (-Entwicklungs)-Kompetenz vom IESE durch Beratung, Auftragsforschung und Technologietransfer unterstützt.	Symantec ist weltweit auf dem Gebiet der Internet-Sicherheit tätig. Die umfangreiche Palette an Lösungen in den Bereichen Content und Netzwerk-Sicherheit für Privatanwender, Unternehmen und Internet-Dienstleister umfasst Virenschutz, Firewalls und Virtual Private Networks ebenso wie Schwachstellen Management, Intrusion Detection, Internet- und E-Mail-Filter sowie Technologien für die Fernverwaltung und Sicherheitsservices für Unternehmen und Internet-Dienstleister weltweit.	Das Bundesamt für Sicherheit in der Informationstechnik ist im Vergleich zu sonstigen europäischen Einrichtungen einzigartig, da hier die verschiedensten Aspekte der IT-Sicherheit in einer Behörde zusammengefasst werden. Mit der rasanten Fortentwicklung der Informationstechnik ist es die Aufgabe des BSI, sich mit den neu entstehenden Sicherheitslücken zu befassen.

Copyright © Fraunhofer IESE 2002

	Fraunhofer IESE	**Symantec**	**BSI**
Programm-werkzeug	**NIXE™**	**Symantec Enterprise Security Manager 5.5**	**USEIT Version 2.0**
Leistungsum-fang der Werkzeuge	Aufspüren sicherheitsrelevanter Schwachstellen in der Konfiguration eines UNIX-Systems. NIXE™ vergleicht die Systemkonfiguration mit den Prüfvorgaben und fasst festgestellte Mängel in einem Prüfprotokoll zusammen. Einzelbefunde werden nach ihrer Brisanz klassifiziert. Das Konzept adressiert gezielt die Praxisanforderungen des Sicherheitsrevisors. Es benötigt keine besondere Laufzeitunterstützung und ist im Produktivbetrieb nebenwirkungsfrei anwendbar, sowie mit Standard-Prüfvorgaben vorkonfiguriert. Ein automatischer Konfigurationslauf erlaubt seine schnelle Anpassung an spezifische Sicherheitsanforderungen der Einsatzumgebung und ermöglicht regelmäßige Wiederholungsprüfungen. Mit einmal erstellten Prüfvorgaben kann eine große Zahl gleichartiger Systeme nach einheitlichen Anforderungen effizient auditiert werden.	Sicherheitsanalyse der für E-Business wichtigen Anwendungen und Betriebssysteme. Intelligente Bewertung von Netzwerkschwachstellen durch über 1.500 Sicherheitsverwaltungen. Schwachstellenanalyse und Einhaltung der Richtlinien von einer zentralen Konsole aus und/oder Verteilung der Überwachung von Bereichen auf mehrere Personen, auch über das Internet. Gleichzeitige Überprüfung mehrerer Systeme auf Abweichungen von den Sicherheitsrichtlinien.	USEIT ist in der Lage, den lokalen UNIX-Rechner auf Schwachstellen und richtige Konfiguration in bezug auf Sicherheit zu überprüfen und hilft, gefundene Fehler zu beheben. Darüber hinaus kann USEIT auch auf benachbarten UNIX-Rechnern über Netzwerkzugriffe Penetrationsprüfungen durchführen. Der normale Betrieb eines UNIX-Systems bzw. eines UNIX-Netzwerkes wird durch den Einsatz von USEIT weder beeinträchtigt noch behindert. USEIT ist ein System von einzelnen Programmen, von denen jedes einzelne eine spezielle Prüfung der Konfiguration des Betriebssystems, des Dateisystems oder der Netzwerkkonfiguration durchführt. Die Ergebnisse der Prüfungen werden in eine Datei ausgegeben bzw. auf dem Bildschirm dargestellt.

Tabelle 1: Überblick über die Werkzeuge und deren Hersteller.

Copyright © Fraunhofer IESE 2002

2.2 Allgemeine Eigenschaften der untersuchten Programmwerkzeuge

Zum Vergleich von NIXE , USEIT und ESM wurden in Tabelle 2 allgemeine Eigenschaften von Auditwerkzeugen aufgelistet, die in Gesprächen mit den IT-Sicherheitsfachkräften des Fraunhofer IESE erarbeitet wurden.

Allgemeine Eigenschaften	**NIXE**	**USEIT**	**ESM**
Dokumentation			
Liegt ein Handbuch vor?	Ja	Ja	Ja
Gibt es Installationsanweisungen, um das Programm selbst weiter zu entwickeln?	Ja	Nein	Nein
Ist dazu ein Handbuch für Entwickler vorhanden?	Ja	Nein	Nein
Sprache des Handbuchs			
Deutsch	Ja	Ja	Nein
Englisch	Nein	Ja	Ja
Werkzeugeigenschaften			
Liegt der Quellcode vor, um das Werkzeug eigenständig zu erweitern?	Ja	Nein	Nein
Stört das Werkzeug den normalen Betriebsablauf, in dem es Anwenderspuren hinterlässt?	Nein	Nein	Nein
Kann das Werkzeug in der Wirkbetriebsumgebung gefahrlos eingesetzt werden?	Ja	Nein	Ja
Ist ein Update des Werkzeuges möglich?	Ja	Ja	Ja
Wird im Programm eine Hilfe angeboten?	Nein	Ja	Ja
Konfiguration			
Kann die Sollkonfiguration von einem Referenzsystem abgeleitet werden?	Ja	Ja	Ja
Bedarf es einer separaten Referenzinstallation um den Konfigurationslauf durchzuführen?	Nein	Ja	Ja
Kann mit dem Werkzeug nur geprüft werden, d.h. ohne Systemeinstellungen zu verändern?	Ja	Ja	Ja
Lässt sich die Prüftiefe der einzelnen Werkzeuge selbst bestimmen?	Ja	Ja	Ja
Lassen sich aufwendige Sicherheitsüberprüfungen unterdrücken?	Ja	Ja	Ja
Ist das Werkzeug einfach an wechselnde Bedürfnisse des Benutzers anzupassen?	Ja	Ja	Ja
Installation			
Wird die Installation mit einem Assistenten durchgeführt?	Nein	Ja	Ja
Kann das Werkzeug per Ferninstallation auf andere Systeme installiert werden?	Nein	Nein	Ja
Muss das Werkzeug manuell installiert werden?	Ja	Nein	Nein
Erforderliche Grundkenntnisse			
Erfordert das Installieren betriebssystemabhängige Kenntnisse?	Ja	Ja	Nein
Erfordert der eigentliche Prüflauf Spezialkenntnisse?	Nein	Nein	Nein
Ist zur Auswertung des Prüfprotokolls ein Spezialist nötig?	Ja	Ja	Ja
Ist zur Systemkonfiguration nach einem Prüflauf ein Spezialist nötig?	Ja	Ja	Ja

Copyright © Fraunhofer IESE 2002

Allgemeine Eigenschaften	NIXE	USEIT	ESM
Systemvoraussetzungen			
Windows NT 4.0, Windows 2000, Windows XP	Nein	Nein	Ja
Solaris, SunOS, SPARC	Ja	Ja	Ja
Linux	Ja	Ja	Ja
HP-UX	Ja	Ja	Ja
AIX	Ja	Ja	Ja
IRIX	Nein	Nein	Ja
Netware	Nein	Nein	Ja
Digital UNIX	Ja	Ja	Ja
Sequent	Nein	Nein	Ja
VMS	Nein	Nein	Ja
Auswertungsergebnisse			
Werden die Auswertungsergebnisse grafisch dargestellt?	Nein	Nein	Ja
Besteht die Möglichkeit, einzelne Auswertungsergebnisse herauszufiltern?	Ja	Nein	Ja
Sind die Auswertungsergebnisse einzeln abrufbar?	Nein	Ja	Ja
Werden die Auswertungen aller Prüfläufe gesichert?	Nein	Ja	Ja
Preise der Programmwerkzeuge			
Euro	2000,-	500,-	4652,-

Tabelle 2: Allgemeine Eigenschaften der untersuchten Programme

2.3 Funktionen der untersuchten Programmwerkzeuge

Die Funktionalität der Prüfwerkzeuge ist auf verschiedene Prüfmodule aufgeteilt, die jeweils einen bestimmten Aspekt der Systemkonfiguration untersuchen. In Tabelle 3 werden die einzelnen Module (45) und ihre Funktionen genauer beschrieben. Ob die Prüfwerkzeuge die jeweilige Funktion erfüllen, wird in der nachfolgenden Gegenüberstellung mit Ja, Nein oder n/a gekennzeichnet:

- Ja: Funktion wird angeboten.
- Nein: Funktion wird nicht angeboten.

Falls eine Funktion aufgrund sonstiger Eigenschaften des Programms (z. B. Systemplattform) nicht von Relevanz ist, wird dies mit n/a bezeichnet:

- n/a: Funktion nicht anwendbar.

Copyright © Fraunhofer IESE 2002

Funktionen	NIXE	USEIT	ESM
1. Prüfung der Passwörter			
a) Prüfung der Passwortstärke (leicht zu bestimmen) Mit Hilfe von Wörterbüchern wird versucht, die Passwörter der Benutzer zu bestimmen. Je schwerer ein Passwort zu bestimmen ist, desto höher ist die Passwortstärke.	Ja[1]	Ja	Ja
b) Prüfung der Passwortliste Stimmt der formale Aufbau der Passwortliste (7 Einträge pro Zeile) und gibt es zu jeder Kennung einen Passworteintrag?	Ja	Ja	Ja
c) Prüfung, ob alle Benutzer in der Passwortliste ein Benutzerverzeichnis besitzen Existieren die in der Passwortdatei angegebenen Benutzerverzeichnisse?	Ja	Ja	n/a
d) Prüfung der Shadowpasswortliste Besitzt ein Betriebssystem eine Shadow-Datei (Passwortdatenbank), so wird diese in die Prüfung einbezogen und auf ihr korrektes Format (7 Einträge pro Zeile) überprüft.	Ja	Ja	n/a
2. Prüfung des Dateisystems			
a) Prüfung der Zugriffsrechte Entsprechen die Zugriffsrechte auf reguläre Dateien den gesetzten Vorgaben?	Ja	Ja	Ja
b) Prüfung von Dateinamen mit ungewöhnlichen Zeichen Dateinamen dürfen nur Buchstaben, Ziffern und Sonderzeichen sowie Umlaute und ß des ISO 8859- und IBM-Zeichensatzes enthalten. Jeder Dateiname mindestens ein Buchstabe, erstes Zeichen kein Bindestrich.	Nein	Ja	Nein
c) Prüfung von Dateien ohne gültigen Eigentümer oder Benutzergruppe Dateisysteme werden nach Dateien durchsucht, die keinem Benutzereintrag in der Passwortdatei bzw. Gruppendatei zugeordnet sind.	Ja	Ja	Nein
3. Prüfung der Benutzererkennung/-verwaltung			
a) Prüfung der vorgegebenen Benutzererkennung, Gruppen und Gruppenmitgliedschaften Sind vorgegebene Benutzerkennungen, Gruppen und Gruppenmitgliedschaften korrekt eingerichtet?	Ja	Ja	Ja
b) Prüfung der Zugriffsrechte von ausgesuchten Dateien im Benutzerverzeichnis Entsprechen die Zugriffsrechte ausgesuchter Dateien in dem Benutzerverzeichnis der getroffenen Sicherheitspolitik?	Ja	Ja	Ja
c) Prüfung von Dateien im Benutzerverzeichnis, die nicht dem Benutzer gehören Enthält das Benutzerverzeichnis Dateien, die nicht dem Benutzer gehören?	Ja	Nein	Nein
d) Prüfung, ob eine Aufzeichnung der vom Benutzer zuletzt eingegebenen Kommandos vorhanden ist Bietet die Benutzererkennung eine Aufzeichnung der zuletzt eingegebenen Kommandos?	Ja	Nein	Nein
e) Prüfung, ob Benutzer sich außerhalb von bestimmten Zeiten am System angemeldet haben Haben sich Benutzer außerhalb der erlaubten Arbeitszeit am System angemeldet?	Nein	Ja	Ja

[1] eingeschränkt

Copyright © Fraunhofer IESE 2002

Funktionen	NIXE	USEIT	ESM
4. Prüfung von Diensten zur zeitgesteuerten Ausführung von Programmen			
a) Prüfung von at-Dienst Wird der Zugriff auf den at-Dienst für bestimmte Benutzer sicher eingeschränkt?	Ja	Nein	n/a
b) Prüfung von cron-Dienst Wird der Zugriff auf den cron-Dienst für bestimmte Benutzer sicher eingeschränkt?	Ja	Nein	n/a
c) Prüfung der cron-Tabellen Enthalten die cron-Tabellen Leerzeilen, ungültige Befehle oder Befehle mit relativen Pfadnamen?	Ja	Nein	n/a
5. Prüfung von Spezialdateien			
a) Prüfung der Zugriffsrechte der Spezialdateien im Verzeichnisbaum dev (Geräteverzeichnis) Entsprechen die Zugriffsrechte auf die im Verzeichnisbaum dev enthaltenen Spezialdateien den gemachten Vorgaben?	Ja	Ja	n/a
b) Prüfung von regulären Dateien im Verzeichnisbaum dev Enthält der Verzeichnisbaum unter dev reguläre Dateien?	Ja	Nein	n/a
c) Prüfung von Spezialdateien außerhalb des Verzeichnisbaums dev Sind auf dem untersuchten System Spezialdateien außerhalb des Verzeichnisbaumes dev vorhanden?	Ja	Nein	n/a
6. Prüfung der Netzdienste			
a) Prüfung des Mailsystems Entspricht die Konfiguration der Mailprogramme (z.B. sendmail) den gemachten Vorgaben?	Ja	Ja	Nein
b) Prüfung des UUCP Systems Das Home-Verzeichnis des Benutzers uucp wird überprüft. uucp ist ein unsicherer Dienst und sollte nicht benutzt werden.	Ja	Ja	n/a
c) Prüfung des Netzwerk-Filesystems NFS (Network File System) Unbeschränkte NFS-Mounts sollten nicht zugelassen sein. Unbeschränkte NFS-Exports dürfen nicht zugelassen sein. Das Verzeichnis "/" darf in keinem Fall exportiert werden.	Ja	Ja	n/a
d) Prüfung des FTP-Dienstes (File Transport Protocol) Werden sicherheitskritische Kennungen von der Benutzung des FTP-Dienstes ausgeschlossen (z.B.: Systemadministratoren, Pseudobenutzer)?	Ja	Ja	Nein
e) Prüfung der IP-Konfiguration des Systems Können die zu analysierenden Parameter überhaupt ermittelt werden, und wenn ja, entsprechen ihre Werte den getroffenen Vorgaben?	Ja	Nein	Ja
f) Prüfung, ob IP-Konfiguration aktiviert ist Das Modul überprüft die Einstellungen der IP-Schnittstelle des Systems. IP-Forwarding sollte nicht aktiviert sein.	Ja	Ja	Nein

Copyright © Fraunhofer IESE 2002

Funktionen	NIXE	USEIT	ESM
7. Prüfung der Log-Aktivitäten			
a) Prüfung von Protokolldateien Der Einsatz der Protokollmechanismen wird kontrolliert.	Ja	Ja	Ja
b) Prüfung der Zugriffszeiten Überprüfung, ob die Zugriffszeiten nicht länger als 72 Stunden zurückliegen.	Nein	Ja	Nein
c) Prüfung von Logon- / Logoff-Informationen (An- / Abmeldeinformationen) Werden aktuelle und historische Login -/ Logoff-Informationen protokolliert, sind die Zugriffsrechte für die Log-Dateien richtig und korrekt gesetzt?	Ja	Nein	Ja
d) Prüfung des Process-Accounting (Protokollierung der ausgeführten Befehle) Ist detailliertes Prozess-Accounting aktiviert, d.h. werden die ausgeführten Befehle protokolliert und ist die zugehörige Log-Datei vor unerlaubten Zugriffen gemäß den Vorgaben geschützt?	Ja	Nein	Nein
e) Prüfung der Benutzerauthentisierung und -identifikation Wurden fehlerhafte Authentisierungsversuche protokolliert? Gab es auffällige oder gehäufte Wechsel der Benutzeridentifikation? Information über die aufgetretenen Wechsel der Benutzeridentifikationen.	Ja	Nein	Ja
8. Prüfung der Login Einstellungen (Anmeldevorgang)			
a) Prüfung der Passwort Einstellungen für den Anmeldevorgang Entsprechen die Zugriffsrechte der Konfigurationsdatei des Log-Dienstes und aller Konfigurierten Log-Daten den Vorgaben? Wie oft darf ein Anmeldeversuch fehlschlagen und wiederholt werden? Ist eine Anmeldung nach Ablauf der Gültigkeitsdauer des Benutzerpasswortes noch möglich oder nicht?	Ja	Nein	Ja
b) Prüfung der Anmeldeeinstellungen Ist die Größe von Dateien eingeschränkt? Werden Anmeldungen des Systemadministrators vom Systemlog-Dienst protokolliert?	Ja	Nein	Ja
9. Prüfung der Administratorrechte			
a) Prüfung der entsprechenden root-Konfigurationsdatei Es wird festgestellt, ob ein root-Login nur an einer bestimmten Konsole erlaubt ist.	Nein	Ja	n/a
b) Prüfung der entsprechenden root-Log-Dateien Es wird geprüft, ob der Benutzer root versucht hat, sich von seriellen Terminals aus am System anzumelden.	Nein	Ja	n/a
10. Prüfung der Patches Sind alle geforderten Patches eingespielt? Sind verbotene Patches vorhanden? Gibt es zueinander inkompatible Patches? Fehlen Patches, die vorausgesetzt werden müssen?	Ja	Ja	Ja
11. Prüfung der Automatismen (laufende Prozesse)			
a) Prüfung und Suche von nicht empfohlenen Diensten sowie Prozessen Die Prozesstabelle enthält keine sicherheitskritischen Prozesse.	Ja	Ja	Ja
b) Prüfung, ob alle relevanten Dienste und Prozesse tatsächlich korrekt laufen und aktiv sind Laufen relevante Dienste unter den für sie vorgesehenen Benutzererkennungen? Sind alle geforderten Dienste tatsächlich aktiv?	Ja	Nein	Ja

Copyright © Fraunhofer IESE 2002

Funktionen	NIXE	USEIT	ESM
12. Prüfung der installierten Datei- und Verzeichnispfade.			
a) Prüfung, ob es Pfade mit Schreibrecht für die Allgemeinheit gibt. Sind Pfade vorhanden, die von allen Benutzern verändert werden können?	Ja	Nein	Ja
b) Prüfung, ob alle ursprünglich installierten Pfade noch vorhanden sind. Sind alle Pfade, die bei einer Installation erstellt wurden, noch vorhanden?	Ja	Nein	Ja
c) Prüfung, ob die Pfadattribute noch dem ursprünglichen Wert entsprechen. Entsprechen die Pfadattribute (Dateigröße, Eigentümer- und Gruppenzuordnung, Zugriffsrechte) noch dem ursprünglichen Wert?	Ja	Nein	Ja
13. Penetrationsprüfung			
a) Prüfung benachbarter Systeme auf die Resistenz gegen Angriffe von außen Ist der Rechner an ein Netzwerk angeschlossen und ist das benachbarte System gegen Angriffe von außen geschützt?	Nein	Ja	Nein
b) Prüfung von bekannten Schwachstellen und ob diese ausgenutzt werden können Es werden einzelne Netzwerkdienste, bei denen Schwachstellen bekannt sind, gezielt angesprochen und dabei versucht, die Schwachstellen auszunutzen.	Nein	Ja	Nein
14. Anzeigen von Systeminformationen Listet allgemeine Informationen über den Rechner und den aktuellen Systemzustand auf.	Nein	Ja	Nein
15. Prüfung der Internet Daemon Services Konfiguration Der Internet Daemon Service startet dynamisch Netzdienste. Es wird geprüft, ob nicht empfohlene sicherheitskritische Dienste konfiguriert sind.	Ja	Nein	Nein
16. Prüfung der flexiblen Benutzerauthentisierung (Pluggable Authentication Modules) Entsprechen die Zugriffsrechte, sowie die Konfiguration der verwendeten Programme den gemachten Vorgaben?	Ja	Nein	Nein
17. Prüfung der internen Ports (und der dazu gehörenden Dienste) Sind alle vorgefundenen Dienste erlaubt? Sind alle vorgeschriebenen Dienste verfügbar? Gibt es unerwartet offene Ports?	Ja	Nein	Ja

Tabelle 3: Funktionen der untersuchten Programmwerkzeuge

Copyright © Fraunhofer IESE 2002

2.4 Zusammenfassung der Werkzeugeigenschaften

NIXE™: Das deutschsprachige Handbuch ist übersichtlich gestaltet und führt Schritt für Schritt durch das Programm. Es wird vorausgesetzt, dass der Anwender über grundlegende UNIX-Kenntnisse verfügt, um das Werkzeug zu installieren. Das Werkzeug besitzt keine Benutzeroberfläche, sondern wird per Befehlsaufruf gestartet. Der Prüflauf ist leicht durchzuführen, die Grundkonfiguration muss jedoch von einem Sicherheitsspezialisten eingestellt werden. Diese dient dann als Vorlage für weitere Referenzsysteme. Das bedeutet, dass viele Systeme innerhalb kürzester Zeit auf Schwachstellen überprüft werden können, ohne dass ein Sicherheitsspezialist anwesend sein muss. Direkt mit dem Prüflauf werden die Auswertungen angezeigt und zum Schluss in einer Textdatei gespeichert. Die Prüfergebnisse bezüglich der Schwachstellen müssen allerdings von einem Sicherheitsspezialisten analysiert und behoben werden.

USEIT: Die einzelnen Kapitel des deutschsprachigen Handbuches erleichtern die Handhabung des kompletten Programms. Das Werkzeug besitzt ein kleines Installationsprogramm, das die Installation auf der UNIX-Plattform durchführt. Auch hier muss der Anwender über UNIX-Kenntnisse verfügen. Das Programm verfügt über eine übersichtliche Benutzeroberfläche, in der die Prüfläufe aufgelistet sind und gestartet werden können. Auch hier muss die Grundkonfiguration durch den Sicherheitsspezialisten vorgenommen werden. Nur der Administrator kann die Prüfläufe durchführen, da nur er die erforderlichen root-Rechte besitzt. Bei der Prüfung von weiteren Systemen muss der Installations- und Konfigurationsvorgang immer aufs Neue durchgeführt werden. Die Auswertungen werden nach einem Prüflauf direkt im Anschluss angezeigt und danach in einer Textdatei gespeichert. Die Analyse und Behebung der Schwachstellen liegt im Verantwortungsbereich des Sicherheitsspezialisten.

Symantec ESM: Das englischsprachige Handbuch beschreibt ausführlich die Funktionalität des Werkzeugs. Wie bei Windows führt ein Assistent durch die Installation. Die Bedienbarkeit wird durch die grafische Benutzeroberfläche erleichtert. Um die einzelnen Prüfläufe durchzuführen, steht ebenfalls ein Assistent zur Verfügung. Die einzelnen Sicherheitskriterien der Prüfläufe müssen auch hier vom Sicherheitsspezialisten konfiguriert werden. Um weitere Systeme zu überprüfen reicht es aus, eine Komponente des Programms auf dem jeweiligen System zu installieren. Daraus ergibt sich die Möglichkeit, die Prüfungen von einem zentralen System auf weitere Systeme auszuweiten. Die allgemeinen Auswertungsergebnisse werden in Form von Diagrammen dargestellt. Die genauere Auswertung der Schwachstellen erfolgt in tabellarischer Form. Für die Analyse und die Behebung der Schwachstellen ist ein Sicherheitsspezialist verantwortlich.

Copyright © Fraunhofer IESE 2002

3 Kosten-/Nutzen-Analyse

3.1 Nutzwertanalyse

Es gibt kein einfaches Mittel, um die Wirtschaftlichkeit von IT-Maßnahmen zu bewerten, denn „die Abhängigkeit eines Unternehmens von der Informationstechnologie, seine IT-Ausstattung sowie seine Verwundbarkeit bezüglich spezifischer Angriffe ist offenbar so projekt- und branchenspezifisch, dass sich keine einfachen Faustregeln aufstellen lassen“ (Schwarz 2000: S. 202). Die Fragestellung, bis zu welchem Grad es wirtschaftlich sinnvoll ist, sich gegen Sicherheitszwischenfälle zu wappnen, und ab welchem Zeitpunkt es wirtschaftlicher ist, bestehende Restrisiken in Kauf zu nehmen liegt im Verantwortungsbereich der Entscheidungsträger.

In Tabelle 4 wird die Kosten-/Nutzwertanalyse im Überblick dargestellt und mit einem Punkte-System bewertet.

			NIXE™			**USEIT**			**ESM**		
	Kriterien	**Gewichtung**		**Punkte**	**P*G**		**Punkte**	**P*G**		**Punkte**	**P*G**
1	Preis in Euro	40	2000,-	6	240	500,-	10	400	4652,-	3	120
2	Quellcode	20		10	200		0	0		0	0
3	Anzahl der Prüfpunkte (von 45) % Anteil	25	37 82,22	8	200	25 55,55	6	150	19 42	4	100
4	Speicher-platz	15	1 MB	10	150	1MB	10	150	50MB	6	90
5	**Summe**	**100**			**790**			**700**			**310**
6	**Rangfolge**				**1**			**2**			**3**

Tabelle 4: Kosten-/Nutzwertanalyse

Damit lässt sich je nach Blickwinkel folgende Produktempfehlung aussprechen:

Copyright © Fraunhofer IESE 2002

1. kaufmännische Gesichtspunkte

Berechnung des Preis-/Leistungsverhältnisses:

Rangfolge x Preis

NIXE™:	1 x 2000 = 2000
USEIT:	2 x 500 = 1000
ESM:	3 x 4652 = 13956

Fazit:

NIXE™:	mittleres Preis-/Leistungsverhältnis
USEIT:	Sehr gutes Preis-/Leistungsverhältnis
ESM:	Schlechtestes Preis-/Leistungsverhältnis

2. technische Gesichtspunkte

- Quellcode

NIXE™:	Aufgrund des Quellcodes hat der Nutzer die Möglichkeit das Programm nach seinen Bedürfnissen zu ändern.
USEIT / ESM:	Änderungen bzw. Erweiterungen von Prüfmodulen können nur vom Hersteller programmiert werden, sind dann jedoch kostenpflichtig.

- Speicherbedarf:

NIXE™/ USEIT:	sehr gering ca. 1MB
ESM:	mit 50MB relativ groß

Copyright © Fraunhofer IESE 2002

3.2 Szenario für eine Kosten-/Nutzenberechnung

Ein durch Schwachstellen im IT-System entstandener Schaden lässt sich jedoch im Rahmen einer Kosten-/Nutzen-Analyse nur schwer einschätzen. Aufgrund dieser Tatsache soll an dieser Stelle stattdessen ein Szenario vorgestellt werden, das den Aufwand für Prüfläufe (s. Maßnahmen in Kapitel 2.1) mit Hilfe des **NIXE™** -Tools dem Aufwand eines Administrators gegenüberstellt, der die Analyse ohne Programmwerkzeugunterstützung durchführt. Nach einer Einschätzung der Dauer für die manuelle Durchführung einer Maßnahme wird der Zeitraum auf Personentage und entsprechende Kosten umgerechnet. Auf diese Weise wird untersucht, ob und ab welchem Zeitpunkt sich die Anschaffung eines Programmwerkzeuges rentiert.

Es wird folgendes Szenario angenommen: Untersucht wird der Aufwand einer Schwachstellenanalyse für einen UNIX-Rechner des Fraunhofer IESE, in diesem Fall ein E-Mail-Server. Man geht von 200 Benutzern, 125 sicherheitskritischen Dateien und 20 Cron-Tabellen aus. Die Unix-Dienste „cron“ und „at“ ermöglichen jedem Benutzer, Programme zu einem bestimmten Zeitpunkt automatisch vom System ausführen zu lassen. Um welche Programme es sich dabei handelt und wann diese ausgeführt werden sollen kann jeder Benutzer in einer nur ihm zugänglichen Datei, der sogenannten Cron – bez. At-Tabelle festlegen. Der Personentagessatz liegt bei 1022,68 Euro bei 7,7 h Arbeitszeit. Die Lizenzkosten für das Programmwerkzeug NIXE™ betragen 2000 Euro, die Konfigurationsdauer beträgt 1 Tag. Der Schulungsaufwand für einen Administrator wird mit 1 Woche veranschlagt, die Auswertung der Schwachstellenanalyse dauert schätzungsweise 1h.

Tabelle 5 stellt den Aufwand der in Kapitel 2.1 aufgeführten Prüfmaßnahmen („Funktionen“) während einer manuellen Schwachstellenanalyse dar. Die nicht erfassten Funktionen werden entweder von **NIXE™** nicht durchgeführt („nein“) oder sind reine Tool-Anwendungen, die sich deshalb nicht mit dem manuellen Aufwand vergleichen lassen. Die Dauer der Einzelmaßnahmen verstehen sich als Minuten pro Benutzer (1. und 3.) bzw. Datei (2.) oder Cron-Tabelle (4c):

Copyright © Fraunhofer IESE 2002

Maßnahme	Dauer Einzelmaß-nahme in Minuten	Faktoren zur Multiplikation	Gesamtdauer in Minuten
1. a)+b)	1 pro Benutzer	200 Benutzer	200
c)	1 pro Benutzer	200 Benutzer	200
d)	1 pro Benutzer	200 Benutzer	200
2. a)+b)+c)	0,5 pro Datei	125 Dateien	62,5
3. a)	1 pro Benutzer	200 Benutzer	200
b)	3 pro Benutzer	200 Benutzer	600
c)	1 pro Benutzer	200 Benutzer	200
d)+e)	1 pro Benutzer	200 Benutzer	200
4. a)	5		5
b)	5		5
c)	5 pro Cron-Tabelle	20 Cron-Tabellen	100
5. a)	30		30
b)+c)	30		30
6. a)	30		30
b)	5		5
c)	15		15
d)	15		15
e)+f)	15		15
7. a)	60		60
c)	5		5
d)	5		5
e)	30		30
8. a)	15		15
b)	15		15
9. a)+b)			
10.	120		120
11. a)	30		30
b)	30		30
12. a)+b9+c9			
13. a)+b)			
14.			
15.	60		60
16.	120		120
17.	30		30
Gesamtdauer in Minuten	**684,50**		**2632,50**
Gesamtdauer in h	**11,41**		**43,88**
Personentage	**1,49**		**5,70**
Kosten in Euro			**5829,28**

Tabelle 5: Aufwand zur Durchführung einer manuellen Schwachstellenanalyse

Die Kosten für einen einmaligen manuellen Prüfdurchlauf belaufen sich also auf rund **5829,28 Euro**.

Copyright © Fraunhofer IESE 2002

Tabelle 6 gibt nun einen Überblick über die Aufwendungen für eine einmalige Schwachstellenanalyse mit Hilfe des Programmwerkzeugs NIXE™:

Schwachstellenanalyse mit Programmwerkzeug	
	Dauer in h
Schulungsaufwand Administrator einmaliger Aufwand	38,5
Initialkonfiguration einmaliger Aufwand	7,7
Auswertung	1
Gesamtdauer in h	**47,2**
Personentage	**6,1**
Kosten in Euro	**6268,9**

Tabelle 6: Aufwand für Schwachstellenanalyse mit Programmwerkzeugunterstützung

Zu den einmaligen Prüfdurchlaufkosten kommen noch **Lizenzkosten in Höhe von 2000,- Euro.** Insgesamt belaufen sich die Kosten einer einmaligen Schwachstellenanalyse mit Programmwerkzeugunterstützung demnach auf einen Betrag von rund **8300,- Euro**.

Die Untersuchung zeigt, dass sich die Anschaffung eines Programmwerkzeugs zur Unterstützung der Schwachstellenanalyse bereits bei einem zweiten Prüfdurchlauf rentiert.

Copyright © Fraunhofer IESE 2002

4 Literatur

[BSI 2000] Handbuch: BSI–Tool Sichere UNIX-Administration (USEIT), Version 2.0, Rohde &Schwarz SIT GmbH,

[ESM 2001] Handbuch: Symantec EnterpriseSecutity Manager™, Version 5.5, 2001

[Fuhrberg 1998] Fuhrberg, Kai: Internet-Sicherheit - Browser, Firewalls und Verschlüsselung, Carl Hanser Verlag München/Wien, 1998

[NIXE™ 2002] Handbuch: NIXE™ – Ein Werkzeug für Unix Sicherheit Version 1.0, 2002

[Schneier 2001] Schneier, Bruce: Secrets & Lies IT-Sicherheit in einer vernetzten Welt, dpunkt.verlag, 2001

[Schwarz 2000] Schwarz, Reinhard: Methoden zur systematischen Bekämpfung von Sicherheitsschwachstellen, IESE Report Nr. 087.00/D. Version 1.0., 2000

Copyright © Fraunhofer IESE 2002

5 Anhang

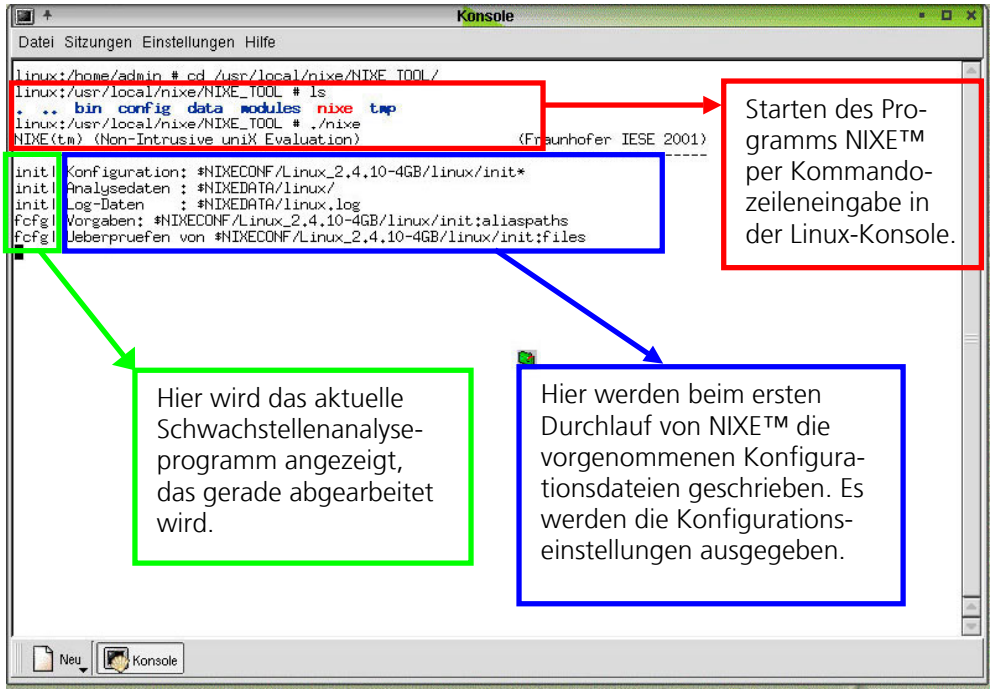

Abbildung 1: NIXE™ Startseite

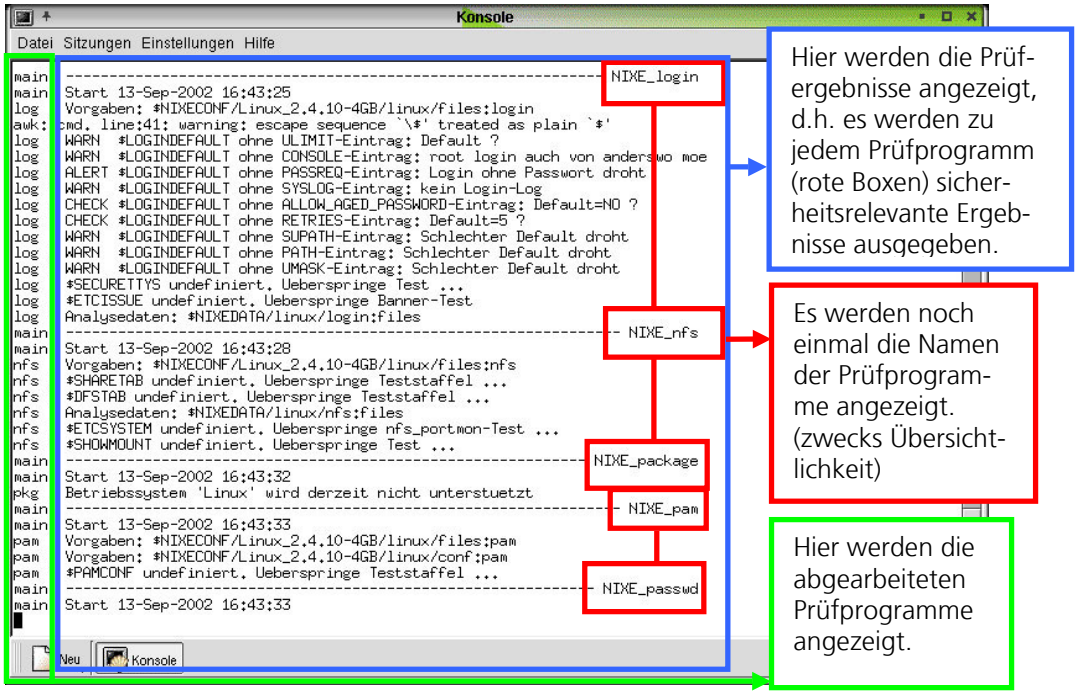

Abbildung 2: NIXE™ Auswertung

Copyright © Fraunhofer IESE 2002

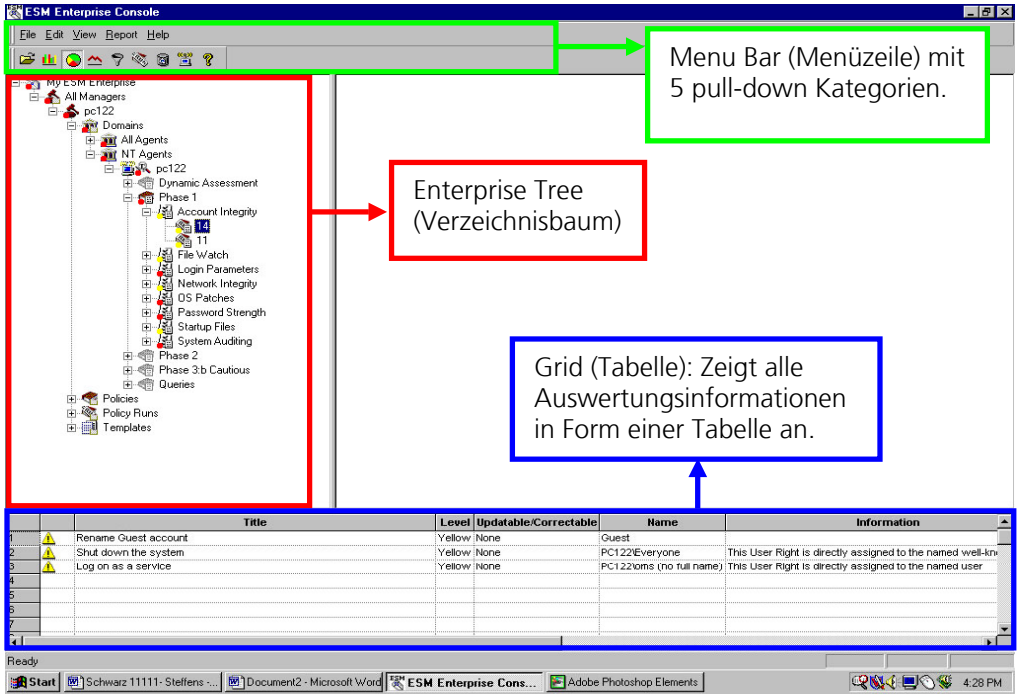

Abbildung 3: ESM Startseite

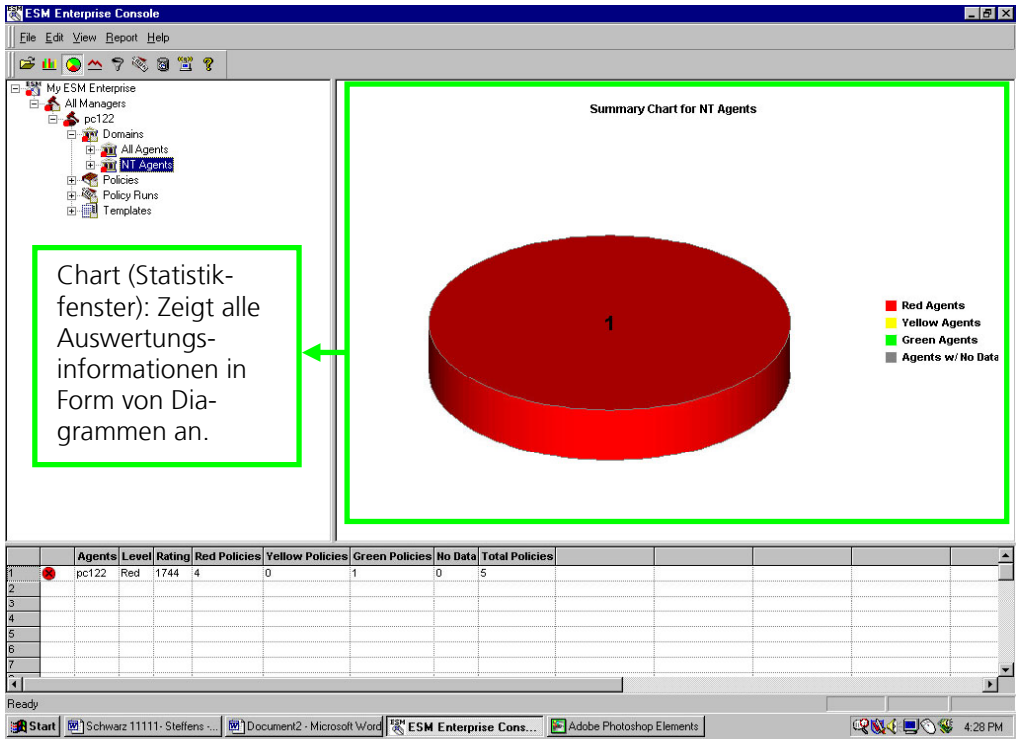

Abbildung 4: ESM Auswertung

Copyright © Fraunhofer IESE 2002

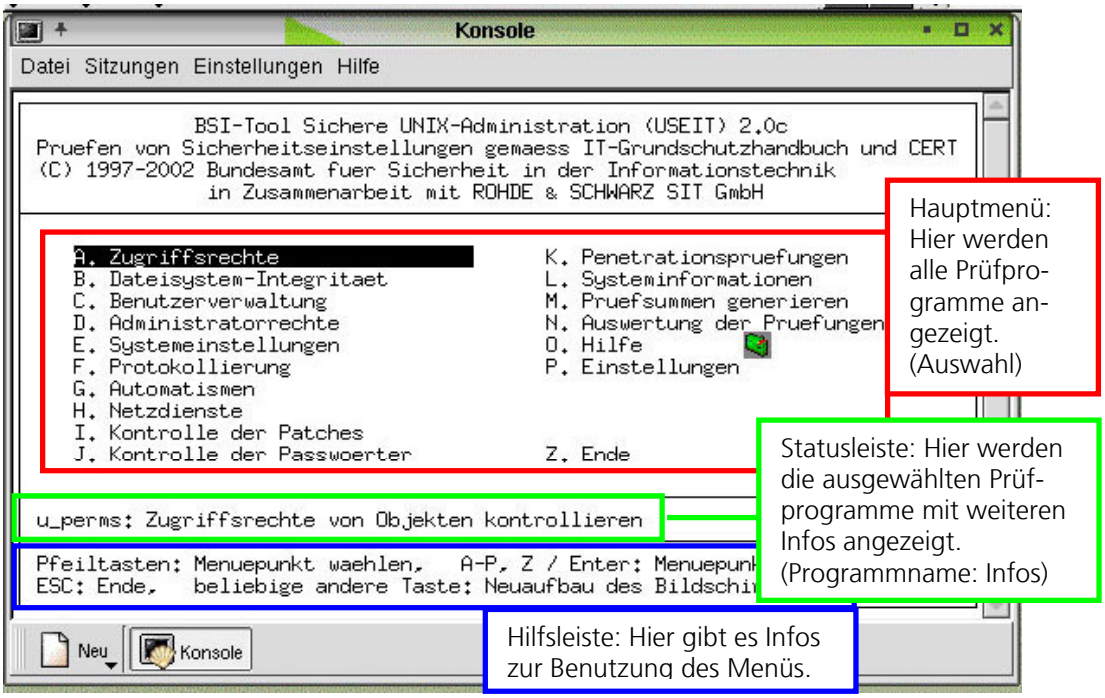

Abbildung 5: USEIT Startseite

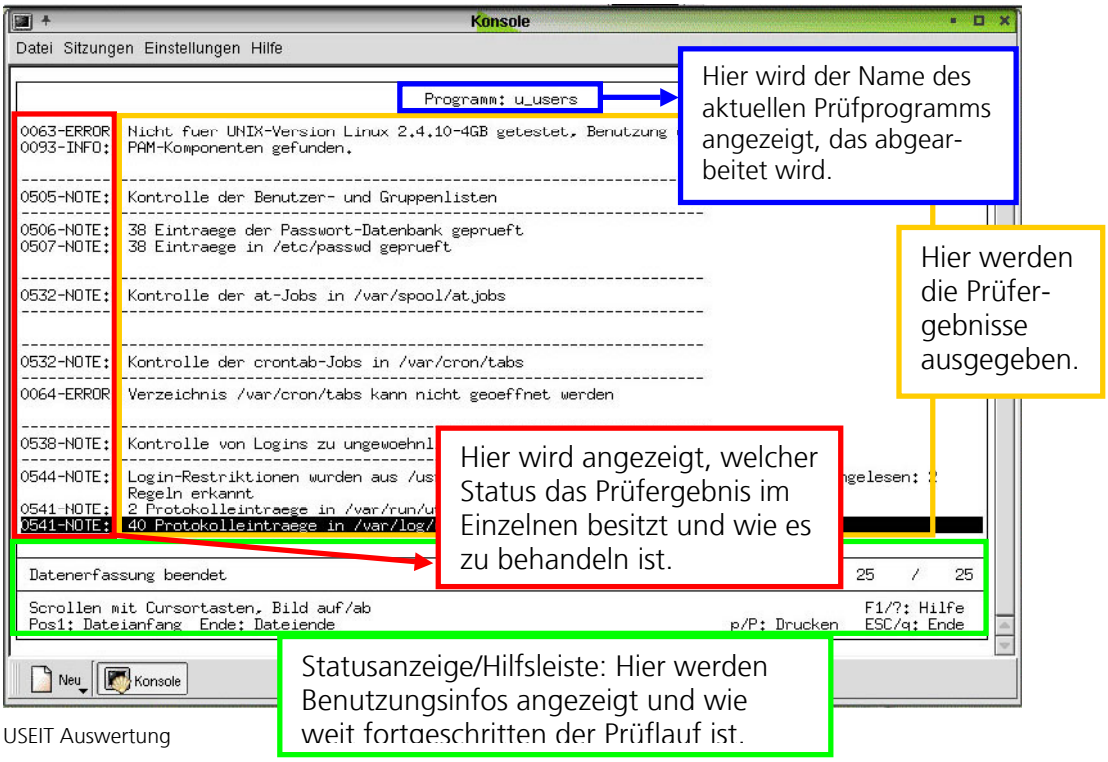

Abbildung 6: USEIT Auswertung

Copyright © Fraunhofer IESE 2002

Dokumenten Information

Titel:	Analyse von Programmwerkzeugen zur Unterstützung von Schwachstellenanalysen im Bereich IT-Sicherheit
Datum:	Oktober 2002
Report:	IESE-052.02/D
Status:	Final
Klassifikation:	Öffentlich

Copyright 2002, Fraunhofer IESE.
Alle Rechte vorbehalten. Diese Veröffentlichung darf für kommerzielle Zwecke ohne vorherige schriftliche Erlaubnis des Herausgebers in keiner Weise, auch nicht auszugsweise, insbesondere elektronisch oder mechanisch, als Fotokopie oder als Aufnahme oder sonstwie vervielfältigt, gespeichert oder übertragen werden. Eine schriftliche Genehmigung ist nicht erforderlich für die Vervielfältigung oder Verteilung der Veröffentlichung von bzw. an Personen zu privaten Zwecken.