BSI-Tool Sichere UNIX-Administration

Erkennen von Sicherheitslücken in UNIX-Betriebssystemen

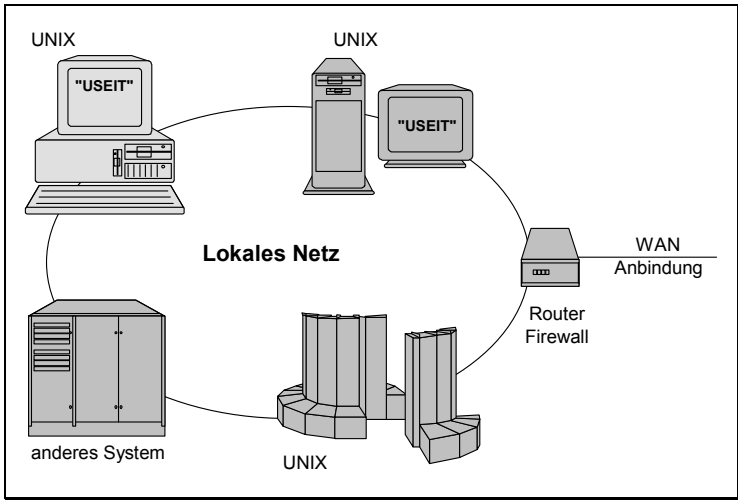
- Automatische oder manuelle Durchführung sicherheitsrelevanter Prüfungen
- Lieferbar für zahlreiche UNIX-Versionen
- Einsatz auf Einzelplatz-Rechnern oder auch in vernetzten Systemen
- Unterstützung neuer UNIX-Releases durch ständige Aktualisierungen

Jetzt verfügbar in neuer Version 2.0 mit erweiterten Funktionen:

- wesentlich verbessertes **Benutzer-Interface**
- **Blättern in den Reports** bereits während der laufenden Prüfungen
- **kontextsensitive Online-Hilfe** zu den Meldungen
- verbesserte Prüfmodule mit Kommandozeilenoptionen für automatisierte **Watchdog-Prüfungen**
- **neue Reportauswertung** mit hierarchischer Navigation nach Meldungsklassen und thematischen Meldungsgruppen
- Filtern von Reports nach **Rechnerklassen**
- neuer **Informationsmodul** zum zu prüfenden System

UNIX ist nach wie vor weit verbreitet

Neben ihrer traditionellen Rolle als zuverlässiger Applikationsserver werden UNIX-Systeme in vielen Unternehmen auch immer häufiger als universelle und flexible Kommunikationsserver eingesetzt. Dabei handelt es sich üblicherweise um recht offene Umgebungen mit Anbindungen an öffentliche Netzwerke wie das Internet.



UNIX-Standardinstallationen sind oft nicht sicher

Eine korrekte Installation und Konfiguration der DV-Systeme ist daher eine wesentliche Voraussetzung für die Absicherung zu verarbeitender und gespeicherter Informationen. Als ausgereiftes Betriebsystem bietet UNIX dazu eine Vielzahl von wirksam implementierten Sicherheitsmechanismen. UNIX-Standardinstallationen nutzen jedoch oft diese Sicherheitsmechanismen nicht oder nur ungenügend aus. Fast täglich wird auch über neue Schwachstellen oder Angriffe auf UNIX-Systeme berichtet. Die jeweiligen Hersteller reagieren darauf zwar relativ schnell mit Updates oder Patches; den Systemverwaltern, die normalerweise neben dem Thema Sicherheit noch eine Reihe weiterer Aufgaben zu bewältigen haben, bleibt aber oft nicht genügend Zeit, sich mit diesen Problemen ausreichend auseinanderzusetzen.

Das BSI-Tool unterstützt Sie in UNIX-Sicherheitsfragen ...

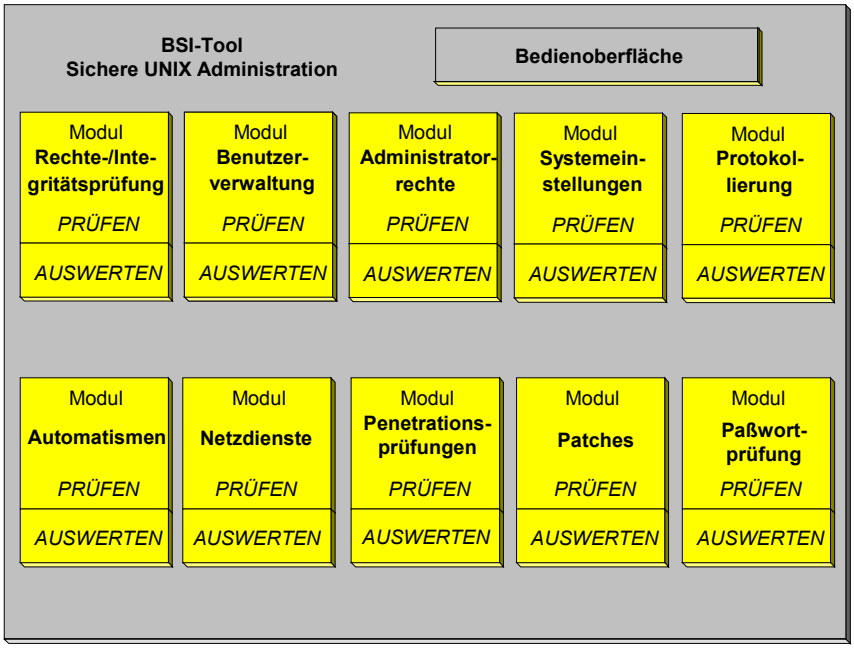
Ein wichtiger Ansatz zur Verbesserung der Informationssicherheit ist der sogenannte IT-Grundschutz, dessen Maßnahmenkatalog durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt und gepflegt wird. Ziel muß sein, den Umfang der Maßnahmen dem Schutzbedarf der jeweiligen IT-Systeme anzupassen. Der IT-Grundschutz zielt dabei auf IT-Systeme mit mittlerem Schutzbedarf. Hier wird der Untersuchungsaufwand aufgrund einer pauschalisierten Gefährdungslage und Betrachtungsweise sowohl bei der Risikoanalyse als auch bei der nachfolgenden Auswahl von empfohlenen Sicherheitsmaßnahmen minimiert.

Das BSI-Tool Sichere UNIX-Administration (UNIX Security Enhancement and Information Tool, "USEIT") ermöglicht auf komfortable Weise, sicherheitsrelevante Einstellungen zu prüfen und entsprechende Probleme aufzuzeigen. Die Prüfungen orientieren sich dabei an den Empfehlungen des IT-Grundschutzhandbuches für vernetzte UNIX-Systeme und ermöglichen somit die werkzeuggestützte Umsetzung der geforderten Maßnahmen.

Entwickelt wurde das Programmsystem von der ROHDE & SCHWARZ SIT GmbH im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik. Es ist ein Werkzeug zur sicheren UNIX-Administration, das die Verwaltung von Systemen unter Sicherheitsaspekten erleichtert bzw. überhaupt erst ermöglicht. Das BSI-Tool liefert Vorschläge für das Beheben von Sicherheitsmängeln und unterstützt Systemadministratoren und Revisoren mit Hinweisen zur Beseitigung festgestellter Gefahrenquellen.

... ist nutzerfreundlich und manipulationssicher ...

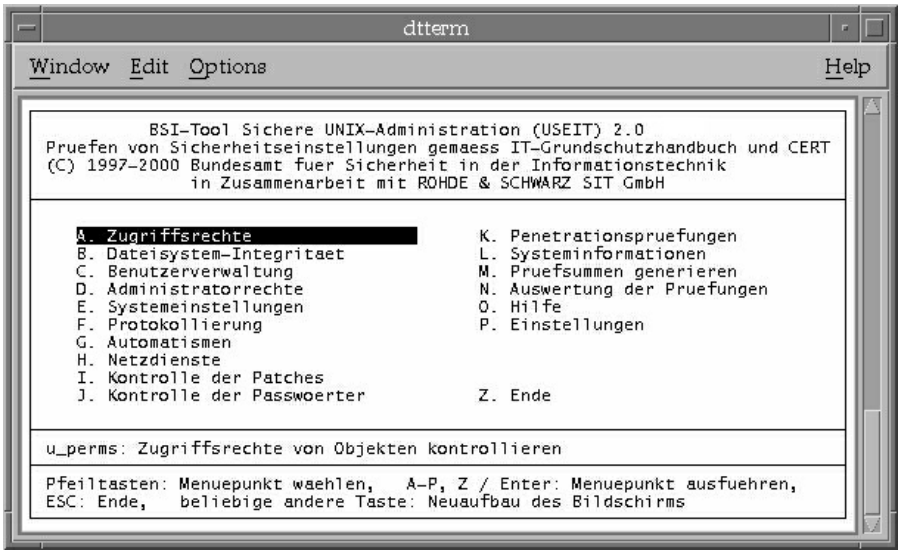
Das BSI-Tool integriert einzelne Programme unter einer gemeinsamen Bedienoberfläche, von denen jedes eine spezielle Prüfung der Konfiguration des Betriebssystemkerns, des Dateisystems oder der Netzwerkfunktionen durchführt. Jedes Programm läßt sich jedoch auch ohne Aufruf der Bedienoberfläche und im Batch-Betrieb (auch automatisch) von CD-ROM manipulationssicher starten. Die Ergebnisse der Prüfung werden in eine Report-Datei ausgegeben und auf dem Bildschirm dargestellt. Für die gezielte Auswertung von Reports steht ein spezielles Modul zur Verfügung.



Das BSI-Tool beeinträchtigt oder behindert nicht den normalen Betrieb eines UNIX-Systems bzw. -Netzwerkes und ist sowohl auf Einzelplatzrechnern als auch in vernetzten UNIX-Systemen ablauffähig. Zahlreiche UNIX-Versionen werden unterstützt (siehe technische Beschreibung).

Das BSI-Tool benötigt Zugriff auf die Massenspeicher des Rechners (Festplatten), auf das Standardausgabemedium (Bildschirm) sowie optional den Zugriff auf das Netzwerk-Interface, sofern der Rechner an ein TCP/IP-Netzwerk angeschlossen ist. Weitere Wechselwirkungen mit anderen Programmen oder anderer Hardware finden nicht statt. Es gibt keine spezifischen technischen Umgebungsbedingungen, die zur Lauffähigkeit des BSI-Tool einzuhalten sind.

... deckt vielfältige Aspekte der Systemkonfiguration ab ...



USEIT besteht aus mehreren Prüfprogrammen mit spezialisierten Aufgaben:

- **Allgemeine Prüfungen des Dateisystems**
  Das Programm u_perms prüft lokale Dateisysteme auf Übereinstimmung der Zugriffsrechte mit den Sollwerten, das Auftreten von Dateinamen mit ungewöhnlichen Zeichen und das Auftreten von Dateien, denen kein gültiger Eigentümer bzw. keine gültige Eigentümergruppe zugeordnet ist.
- **Prüfung der Attribute sowie der Integrität von Objekten des Dateisystems**
  Das Programm u_integrity führt eine Prüfung der Attribute sowie der Integrität von Objekten des Dateisystems durch.
- **Prüfung der Benutzerverwaltung**
  Das Programm u_users führt eine Prüfung der Benutzerverwaltung durch. Dabei werden die die Benutzerverwaltung betreffenden Dateien auf formale Korrektheit und Widerspruchsfreiheit geprüft. Außerdem wird die Existenz und der Inhalt bestimmter sicherheitsrelevanter Dateien in den Home-Verzeichnissen der Benutzer sowie den Verzeichnissen für zeitgesteuerte Aufträge überprüft. Schließlich wird festgestellt, ob Benutzer sich außerhalb der erlaubten Arbeitszeiten am System angemeldet haben.
- **Prüfung der Administratorrechte**
  Das Programm u_root führt eine Prüfung der Administratorrechte durch. Dazu wird festgestellt, ob root-Logins von unsicheren Terminals aus möglich sind oder versucht wurden sowie ob das su-Kommando zur Erlangung von root-Rechten von unsicheren Terminals aus benutzt wurde. Außerdem wird das System nach sicherheitskritischen Dateien mit gesetztem SUID- oder SGID-Bit durchsucht.
- **Prüfung der Systemeinstellungen**
  Das Programm u_sysconf führt eine Prüfung der Systemeinstellungen durch. Dazu wird geprüft, ob es Programmdateien mit gesetztem SUID oder SGID-Bit gibt, die nicht in der Konfigurationsdatei aufgelistet sind. Außerdem werden Prüfungen im Zusammenhang mit Spezialdateien des UNIX-Dateisystems durchgeführt. Schließlich werden Konfigurationseinträge zu Anmeldemöglichkeiten am System, Pfadeinstellungen sowie Zugriffsmöglichkeiten auf externe Datenträger überprüft.
- **Prüfung der Protokollierung**
  Das Programm u_audit führt eine Prüfung der Protokollierung durch. Dabei wird geprüft, ob die geforderten Protokolldateien existieren, ob sie vom System benutzt werden und ob ihre Größe einen vordefinierten Maximalwert erreicht bzw. überschritten hat.
- **Prüfung von Automatismen**
  Das Programm u_ps führt eine Prüfung der Automatismen durch. Dabei werden Konfigurationsdateien des Systems geprüft, die für automatische Systemdienste oder Netzwerkdienste relevant sind. Außerdem werden die Prozeßliste sowie die Liste der aktiven Netzwerkports auf das Vorhandensein in der Konfigurationsdatei eingetragener sicherheitskritischer Prozesse bzw. Dienste überprüft.

- **Prüfung der Netzdienste**
  Das Programm u_net führt eine Prüfung der Netzdienste durch. Dabei werden die Konfigurationen des Mail-Systems, des UUCP-Systems, des Netzwerkdateisystems NFS, der „Trusted Hosts“ (Remote-Kommando-ausführung) sowie des FTP-Dienstes überprüft. Außerdem wird geprüft, ob das System als IP-Gateway (Router) arbeitet.
- **Prüfung von Patches**
  Das Programm u_patches führt eine Prüfung der installierten Patches bzw. Paketversionen durch und kontrolliert, ob die Empfehlungen sicherheitsrelevanter Advisories bzw. Announcements umgesetzt wurden.
- **Prüfung der Paßwörter**
  Das Programm u_passwd führt eine Prüfung der Paßwörter der Benutzer durch. Dabei wird geprüft, ob alle Benutzer ein gültiges Paßwort besitzen. Danach wird für alle oder für ausgewählte Benutzer die Paßwortstärke überprüft, indem mit Hilfe von Wörterbüchern oder durch einen Brute-Force-Angriff versucht wird, das Paßwort zu bestimmen.
- **Penetrationsprüfungen**
  Das Programm u_breakin prüft benachbarte Systeme (im Subnetz) auf die Resistenz gegen Angriffe von außen. Hierzu wird zunächst ermittelt, welche Systeme im Netzwerk aktiv sind. Für alle diese oder ausgewählte Systeme wird danach ermittelt, welche Netzwerkports aktiv sind. Schließlich werden einzelne Netzwerkdienste, bei denen Schwachstellen bekannt sind, gezielt angesprochen und dabei versucht, die Schwachstellen auszunutzen.
- **Anzeige von Systeminformationen**
  Das Programm u_info führt keine Prüfungen durch, sondern gibt allgemeine Informationen über den Rechner und den aktuellen Systemzustand aus.
- **Prüfung der Report-Dateien**
  Das Programm u_report überprüft die Report-Dateien, in denen die einzelnen USEIT-Programme ihre Prüfergebnisse ablegen. Anschließend werden die Reports angezeigt. Es ist möglich, ausgewählte Reports der einzelnen Prüfprogramme, alle Meldungen einer bestimmten Meldungsklasse oder alle Meldungen, die zu einer bestimmten Kategorie (Meldungsgruppe) gehören, anzuzeigen oder auszudrucken. Die Auswertung erfolgt hierarchisch und menügesteuert.
- **Ermittlung der Attribute und der Prüfsummen für Objekte des Dateisystems**
  Das Programm u_gensum bestimmt die Attribute aller in der Datenbank u_gensum.config aufgeführten Objekte. Die gefundenen Attribute sowie die Prüfsummen gewöhnlicher Dateien werden in die Datei u_integrity.var geschrieben und stehen damit als Datenbasis für die Prüfungen durch das Prüfprogramm u_integrity zur Verfügung.
- **Online-Hilfe**
  Das Programm u_help zeigt vom USEIT-Hersteller mitgelieferte Hilfetexte an und bietet Hilfe zu den einzelnen USEIT-Meldungsnummern. Es ermöglicht das Betrachten und Bearbeiten der USEIT-Konfigurationsdateien mit Hilfe eines externen Editors. Außerdem können das IT-Grundschutzhandbuch des BSI, CERT-Advisories und andere sicherheitsrelevante Informationen angezeigt werden.

... und gibt Meldungen verschiedener Kategorien aus:

NOTE
USEIT meldet einen Arbeitsschritt oder informiert über eine festgestellte Systemkonfiguration. Es liegt kein Sicherheitsproblem vor.

INFO
Es werden Texte zu Prüfschritten angezeigt. Darüber hinaus erfolgt eine Informationsausgabe, wenn das BSI-Tool eine Abweichung von den Standardvorgaben entdeckt hat, die aber kein Sicherheitsproblem darstellt. Ein Protokoll wird zur Information zwar ausgegeben, aber es besteht kein Bedarf für Änderungen.

WARN
Das BSI-Tool hat eine Abweichung von den Standardvorgaben entdeckt, die möglicherweise ein Sicherheitsproblem darstellt, ist jedoch nicht in der Lage zu beurteilen, ob die Abweichung tatsächlich eine zu beseitigende Schwachstelle ist. Sollte es sich um eine Schwachstelle unter Sicherheitsaspekten handeln, muß sie manuell beseitigt werden. Das BSI-Tool liefert eine ausführliche Beschreibung des Problems.

FAIL
Das Programmsystem hat eine Schwachstelle entdeckt, die in jedem Fall beseitigt werden muß. Die Schwachstelle sowie ihre möglichen Auswirkungen werden detailliert beschrieben. Der Systemadministrator erhält eine ausführliche Handlungsanweisung für die Fehlerbehebung.

ALERT
Das BSI-Tool hat Anzeichen für einen Einbruch in das System bzw. einen durchgeführten Angriff festgestellt. Das Programmsystem gibt in diesem Fall ausführliche Hinweise, was zu tun ist.
In der Regel erkennt das BSI-Tool Schwachstellen, die das Eindringen in das UNIX-System ermöglichen. Ist das ausnahmsweise nicht der Fall, besteht die Möglichkeit, daß der Angreifer eine neue, noch nicht vom BSI-Tool geprüfte Schwachstelle entdeckt und ausgenutzt hat, oder daß sie im organisatorischen Bereich zu suchen ist (z.B. nicht ausreichend geschütztes Administrator-Paßwort).

ERROR
Eine Prüfung bzw. Teile einer Prüfung konnten aufgrund eines Fehlers nicht durchgeführt werden. Die Störung wird ausführlich beschrieben. Der Systemadministrator muß den aufgetretenen Fehler beseitigen und das BSI-Tool danach erneut starten.

PARAM
USEIT hat einen Aufrufparameter erkannt. Diese Meldung dient zu Kontrolle für den Benutzer und wird in die Reportdatei geschrieben, damit bei einer späteren Auswertung die Prüfbedingungen rekonstruierbar sind.

CONF
USEIT hat einen Eintrag in einer seiner Konfigurationsdateien oder eine für den Ablauf der Prüfungen relevante Envirronmentvariable erkannt. Diese Meldung dient zu Kontrolle für den Benutzer und wird in die Reportdatei geschrieben, damit bei einer späteren Auswertung die Prüfbedingungen rekonstruierbar sind.

Zahlreiche unterstützte Betriebssysteme

Das BSI-Tool läuft auf Rechnern unter folgenden Betriebssystemen (alphabetisch geordnet)[1]:

- AIX 4.3
- Digital UNIX 4.0x
- HP-UX 11.x
- RedHat-Linux mit Kernelversion 2.2.x (z.B. RedHat-Linux 6.1)
- Solaris 7 SPARC
- S.u.S.E.-Linux mit Kernelversion 2.2.x (ab S.u.S.E.-Linux 6.2)
- Reliant UNIX 5.43 [2]

Im Rahmen der Produktpflege und Weiterentwicklung des BSI-Tool Sichere Unix-Administration werden Anpassungen an aktuelle Unix-Versionen und bekanntgewordene Bedrohungen sowie funktionelle Erweiterungen vorgenommen.

Für Anwender des Tool sind Updates zu speziellen Konditionen verfügbar.

[1] Für einige ältere Betriebssystemversionen ist eine frühere USEIT-Version im Verzeichnisbaum `/old` auf der CD enthalten. Für diese Betriebssysteme wird USEIT nicht mehr weiterentwickelt. Zu Details wenden Sie sich bitte an den Hersteller.

[2] voraussichtlich verfügbar in Q1/2001

Weitere Informationen

USEIT für Behörden (Bund, Land, Kommune, etc.)

Bundesamt für Sicherheit in der Informationstechnik
z. Hd. Herrn Wilhelm Merx
Postfach 20 03 63
53133 Bonn
Fax: (0228) 9582-427
E-Mail: useit@bsi.de
Internet: http://www.bsi.de/aufgaben/projekte/useitool/useit.htm

Bestellangaben

USEIT für andere Interessenten (Privatpersonen, Firmen, Vereine, etc.)

ROHDE & SCHWARZ SIT GmbH
Agastraße 3
12489 Berlin
Fax (030) 65884-184
Email: bsi.tool@sit.rohde-schwarz.com
Internet: www.useit.rohde-schwarz.com

BSI-Tool Sichere UNIX-Administration
Bestellnummer: 3534.4277

Lieferumfang
CD-ROM als Einzellizenz mit Programmen für alle Plattformen, Benutzerhandbuch in verschiedenen Formaten (pdf, Postscript, html) auf der CD enthalten

Ergänzende Leistungen

(auf Anfrage)

- Installation
- Einführung in die Bedienung
- Schulung zur Systemsicherheit unter Nutzung des BSI-Tools
- Regelmäßige Aktualisierungen / Updates

Warenzeichen
Alle in diesem Text verwendeten Warenzeichen sind eingetragene Warenzeichen der jeweiligen Hersteller.