



BSI-Tool Sichere UNIX-Administration

Erkennen von Sicherheitslueken in UNIX-Betriebssystemen

- Automatische oder manuelle Durchfuehrung sicherheitsrelevanter Pruefungen
- Lieferbar fuer zahlreiche UNIX-Versionen
- Einsatz sowohl auf Einzelplatz-Rechnern als auch in vernetzten Systemen
- Unterstuetzung neuer UNIX-Releases durch staendige Aktualisierungen



UNIX-Standardinstallationen sind oft nicht sicher

UNIX-Standardinstallationen nutzen oft die in das Betriebssystem implementierten Sicherheitsmechanismen nicht oder nur ungenügend aus. Fast täglich wird über neue Schwachstellen oder Angriffe auf UNIX-Systeme berichtet.

Die Hersteller reagieren darauf zwar relativ schnell mit Updates oder Patches; den Systemverwaltern, die normalerweise neben der Sicherheit noch eine Reihe weiterer Aufgaben zu bewältigen haben, bleibt aber oft nicht genügend Zeit, sich mit diesen Problemen ausreichend auseinanderzusetzen.

Die Verwaltung solcher modernen Systeme, die oft in lokale oder Weitverkehrsnetze (z.B. Internet) eingebunden sind, stellt deshalb Systemadministratoren, die unter anderem auch die Sicherheit der gespeicherten und zu verarbeitenden Informationen zu gewährleisten haben, vor eine Reihe von Problemen.

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

Das Sicherheits-Management-System BSI-Tool Sichere Unix-Administration (UNIX Security Enhancement and Information Tool „USEIT“) ermöglicht auf komfortable Weise, sicherheitsrelevante Einstellungen zu prüfen und entsprechende Probleme aufzuzeigen.

Entwickelt wurde das Programmsystem von der Rohde & Schwarz SIT GmbH im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik.

Dieses Werkzeug dient der sicheren UNIX-Administration, da es die Verwaltung von Systemen unter Sicherheitsaspekten erleichtert bzw. überhaupt erst ermöglicht.

Das BSI-Tool liefert Vorschläge für das Beheben von Sicherheitsmängeln und unterstützt Systemadministratoren mit Hinweisen zur Beseitigung festgestellter Gefahrenquellen.

...ist benutzerfreundlich und manipulationssicher...

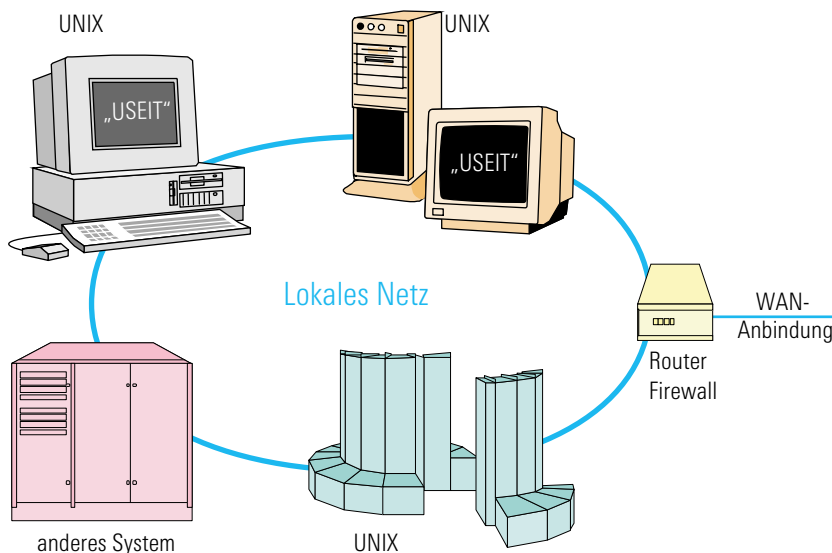
Das BSI-Tool integriert unter einer gemeinsamen Bedienoberfläche einzelne Programme, von denen jedes eine spezielle Prüfung der Konfiguration des Betriebssystemkerns, des Dateisystems oder der Netzwerkkonfiguration durchführt. Jedes Programm lässt sich jedoch auch ohne Aufruf der Bedienoberfläche und im Batch-Betrieb (auch automatisch) von der CD-ROM manipulationssicher starten.

Die Ergebnisse der Prüfung werden in einer Datei ausgegeben und auf dem Bildschirm dargestellt.

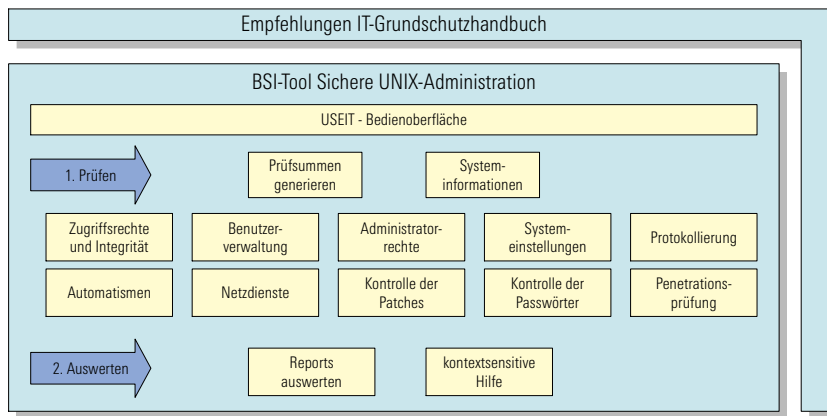
Das BSI-Tool beeinträchtigt oder behindert nicht den normalen Betrieb eines UNIX-Systems bzw. UNIX-Netzwerkes; es ist sowohl auf Einzelplatz-Rechnern als auch in vernetzten UNIX-Systemen ablauf-fähig.

Zahlreiche UNIX-Versionen werden unterstützt (siehe Seite 4).

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-Tools einzuhalten sind.



Das BSI-Tool ist vielseitig einsetzbar: in Einzelplatz-Rechnern sowie in komplexen Netzwerken



Funktionsstruktur: BSI-Tool Sichere UNIX-Administration

...und gibt Meldungen verschiedener Kategorien aus

NOTE

Das Tool 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 Infoausgabe, wenn das BSI-Tool eine Abweichung von den Standardvorgaben entdeckt, 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; es 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 Sicherheits-Management-System 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 zur 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 darüber, was zu tun ist. In der Regel erkennt das BSI-Tool solche Schwachstellen, die das Eindringen in das UNIX-System ermöglichen. Ist das aus-

nahmsweise nicht der Fall, besteht die Möglichkeit, dass der Angreifer eine neue, noch nicht vom BSI-Tool geprüfte Schwachstelle entdeckt und ausgenutzt hat, oder dass eine Schwachstelle 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 anschließend erneut starten.

PARAM

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

CONF

Das Tool hat einen Eintrag in einer seiner Konfigurationsdateien oder eine für den Ablauf der Prüfungen relevante Environmentvariable erkannt. Diese Meldung dient zur 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 UNIX-Betriebssystemen (alphabetisch geordnet):¹⁾

- AIX
- DEC Digital UNIX
- HP-UX
- Linux
- RedHat-Linux
- Reliant UNIX
- Solaris 7 SPARC
- S.u.S:E.-Linux

Die Liste enthält eingetragene Warenzeichen verschiedener Firmen.

¹⁾ Für einige ältere Betriebssystemversionen ist eine frühere USEIT-Version auf der CD enthalten.

Bestellangaben

BSI-Tool Sichere UNIX-Administration
Bestellnummer 3534.4277

Lieferumfang

CD-ROM mit Programmen für alle Plattformen, Benutzerhandbuch auf der CD

Ergänzende Leistungen

(auf Anfrage)

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



ROHDE & SCHWARZ