Compliance mit Security Content Automation Protocol (SCAP)

Das Security Content Automation Protocol (SCAP) hilft mit Methoden dabei wichtige Sicherheitsrichtlinien im Unternehmen einzuhalten. Mit Programmen, wie zum Beispiel dem Open Source Tool OpenSCAP, lassen sich die dazugehörigen Richtlinien einlesen und mit den eigenen Systemen vergleichen.

Um die Sicherheit und Compliance der eigenen Systeme im Netzwerk im Griff zu behalten, helfen Methoden und Richtlinien, die das Security Content Automation Protocol (SCAP) zusammenfasst. Da die Sicherheitsrichtlinien ständig geändert, ausgebaut und erweitert werden, ist es notwendig die eigenen Systeme auf Compliance-Anforderungen zu überprüfen. Das Security Content Automation Protocol (SCAP) ist ein Framework von Spezifikationen, das die automatisierte Konfiguration, Schwachstellen- und Patchprüfung, Aktivitäten zur Einhaltung der technischen Kontrolle und Sicherheitsmessungen unterstützt. Um SCAP zu nutzen, müssen die eigenen Systeme also mit dem Framwork untersucht werden.

Die Aufgabe von Compliance-Definitionen für Netzwerke und den darin betriebenen Geräten besteht darin festzulegen, wie Systeme, zum Beispiel auf Basis von Linux sicher zu betreiben sind. Hier spielen auch Vorgaben wie Gesetze und Unternehmensrichtlinien eine Rolle. Dazu kommen Guidelines und Anforderungen von Herstellern des Betriebssystems und der betriebenen Anwendungen, STIG und CIS-Benchmarks sowie PCI/DSS. Sobald klar ist, was konfiguriert werden muss, müssen die entsprechenden Fachkräfte im Unternehmen dafür sorgen, dass Baselines zum sicheren Betrieb vorhanden sind, sowie Basis-Installationen der eingesetzten Server, zum Beispiel für Datenbanken, App- und Web-Server, und alle anderen Komponenten, die eine Rolle spielen.

OpenSCAP und SCAP

Hier hilft Open Source, wie zum Beispiel OpenSCAP. OpenSCAP ist ein Tool zum automatischen Scannen von Systemen. Das Programm kann System-Konfigurationen und Software-Stände überprüfen. Dazu existieren in großer Anzahl auch freie Vorlagen. Die meisten Hersteller von Linux-Distributionen liefern OVAL-Daten.

OpenSCAP hat für seine Unterstützung von SCAP 1.2 eine NIST-Zertifizierung erhalten. OpenSCAP steht kostenlos zur Verfügung und ist quelloffen, sodass Patches und Verbesserungen des Systems

sehr schnell implementiert werden können. OpenSCAP bietet verschiedene Tools für die automatisierte Überprüfung auf Sicherheitsrisiken. Das ermöglicht das ergreifen von Maßnahmen, um Angriffe zu verhindern. Sicherheitslücken und Probleme im Bereich der Compliance werden dadurch sehr schnell erkannt und behoben.

Das OpenSCAP-Team legt großen Wert auf die Einhaltung von Standards. Wir glauben, dass dies der einzige Weg ist, um in der heutigen stark fragmentierten Welt erfolgreich zu sein. OpenSCAP ist 2008 als Open Source-Implementierung des SCAP-Standards gestartet. Seit OpenSCAP 1.0 verfügt OpenSCAP über die NIST SCAP-Zertifizierung. Die Entwickler von OpenSCAP arbeiten mit NIST und MITRE zusammen, um Audit-Anforderungen von Linux-Systemen zu verstehen. OpenSCAP hat einen Sitz im OVAL-Vorstand.

Compliance mit OpenSCAP-Scan überprüfen

Einfach ausgedrückt handelt es sich bei OpenSCAP um ein Scanprogramm, das alle angebundenen Systeme im Netzwerk auf die Einhaltung der verschiedenen Compliance-Richtlinien hin überprüft. Dabei kann es sich um eine einfache Überprüfung des Patchstandes und der Sicherheitskonfiguration handeln, oder um einen umfassenden Scan der Compliance auf Basis der verschiedenen Standards. In diesem Bereich unterstützt OpenSCAP zum Beispiel auch DISA Security Technical Implementation Guide (STIG) und US Government Configuration Baselines (USGCB). OpenSCAP kann auf Basis des Scanvorgangs einen Bericht erstellen, auf dem schnell ersichtlich ist, ob die Systeme im Netzwerk die Compliance auf Basis der verschiedensten Protokolle einhalten.

Für viele Linux-Distributionen, wie zum Beispiel Fedora oder Red Hat Enterprise- Linux stehen vorgefertigte Regeln zur Verfügung, die in OpenSCAP eingelesen werden können. Das hat den Vorteil, dass solche Systeme recht schnell und zuverlässig auf Sicherheitsbrüche gescannt werden können. Wichtig ist natürlich, dass die Vorlagen, die OpenSCAP für die Scans nutzt auch aktuell sind. Hier ist also einiges an Vorarbeit gefragt, um sicherzustellen, dass alle Systeme mit möglichst aktuellen Vorlagen gescannt werden. In OpenSCAP geschieht das über Profile.

Liegen die entsprechenden Guidelines vor, lassen sich Server auf Sicherheitslücken hin überprüfen. Das kann in Red Hat Enterprise Linux zum Beispiel mit dem folgenden Befehl erfolgen:

```
oscap xccdf eval \
--profile stig-rhel-server \
--results results.xml \
--report report.html \
--cpe /usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```

Der Bericht wird anschließend als HTML-Seite gespeichert und ist dadurch über jeden Browser einsehbar. Im Bericht wird angezeigt, wenn bestimmte Konfigurationen nicht dem verwendeten Standard entsprechen, der zum scannen genutzt wird. Auch Hinweise, wie sich die Einstellungen so verbessern lassen, dass sie dem Standard entsprechen, werden angezeigt.

OpenSCAP testen

Um OpenSCAP zu testen, kann die Installation zum Beispiel auf einem Linux-Server erfolgen. Am Beispiel von Ubuntu erfolgt das mit dem Befehl

```
sudo apt-get install libopenscap8 -y
```

OpenSCAP nutzt zum Beispiel OVAL-Definitionen für das Scannen von Computern. Diese lassen sich auf dem Server, auf dem OpenSCAP installiert ist ebenfalls herunterladen und einbinden. Für Ubuntu wird dazu der folgende Befehl genutzt:

```
wget https://people.canonical.com/~ubuntu-
security/oval/com.ubuntu.xenial.cve.oval.xml
```

Danach kann ein Scan-Vorgang gestartet werden. Dazu wird in diesem Beispiel folgender Befehl verwendet:

```
oscap oval eval --results /tmp/oscap_results.xml --report
/tmp/oscap_report.html com.ubuntu.xenial.cve.oval.xml
```

Der Bericht kann danach als HTML-Datei angezeigt werden. Dazu wird der Bericht aus dem TMP-Verzeichnis kopiert, zum Beispiel mit:

```
cp /tmp/oscap_report.html /var/www/html/
```

Natürlich kann der Bericht auch einfach im Browser geöffnet, oder ins Netzwerk kopiert werden.