

OSCAL: Die Open Security Controls Assessment Language

Ob Cloud-Dienste, SaaS-Plattformen, Behördenlösungen, Finanzinfrastrukturen oder kritische Systeme: Fast überall müssen Sicherheitsanforderungen dokumentiert, Kontrollen umgesetzt, Nachweise erbracht und Audits bestanden werden. Die Herausforderung an dieser Stelle: Die Informationen liegen in Word-Dokumenten, Excel-Listen, PDF-Berichten, GRC-Tools, Ticket-Systemen und proprietären Plattformen verteilt. Das macht Sicherheitsnachweise schwer vergleichbar, schwer automatisierbar und aufwendig zu pflegen.

[illegible]

Bei OSCAL handelt sich um eine vom US-amerikanischen National Institute of Standards and Technology, NIST, geführte Initiative, die gemeinsam mit Industriepartnern entwickelt wird, um Sicherheits- und Compliance-Prozesse stärker zu standardisieren und zu automatisieren.

OSCAL setzt genau an diesem Punkt an. Die Abkürzung steht für Open Security Controls Assessment Language. Es handelt sich um eine vom US-amerikanischen National Institute of Standards and Technology, NIST, geführte Initiative, die gemeinsam mit Industriepartnern entwickelt wird, um Sicherheits- und Compliance-Prozesse stärker zu stan-

dardisieren und zu automatisieren. OSCAL stellt offene, maschinenlesbare Formate bereit, unter anderem in XML (für komplexe, hierarchische Datenstrukturen), JSON (für leichtgewichtige, webfreundliche Anwendungen) und YAML (für menschenlesbare Konfigurationen und einfache Datenstrukturen). Damit können Informationen zu Sicherheitskontrollen, deren Umsetzung, Prüfplanung, Prüfergebnissen und Massnahmen strukturiert ausgetauscht werden. Details können unter <https://pages.nist.gov/OSCAL/> abgerufen werden.

Was ist OSCAL?

OSCAL ist eine Sprache beziehungsweise ein Datenmodell zur strukturierten Beschreibung von

Sicherheits- und Compliance-Informationen. Im Fokus steht die Idee, dass sicherheitsrelevante Inhalte nicht nur als Fliesstext in Dokumenten vorkommen sollen, sondern in einer Form, die von Menschen gelesen und von Maschinen verarbeitet werden kann. Die klassische Compliance-Dokumentation legt dar, welche Sicherheitskontrollen eine Organisation erfüllen muss, wie diese umgesetzt werden, welche Systeme betroffen sind und welche Ergebnisse ein Audit erzielt hat. In zahlreichen Firmen werden diese Informationen manuell aktualisiert. Das verursacht Medienbrüche, Versionskonflikte und einen hohen Aufwand für die Koordination. OSCAL hat den Ansatz, diese Informationen in standardisierte Bausteine zu unterteilen. NIST beschreibt OSCAL als eine Reihe von hierarchischen Formaten, die Informationen über die Veröffentlichung, Implementierung und Bewertung von Sicherheitskontrollen standardisiert darstellt.

OSCAL ist in verschiedene Ebenen und Modelle gegliedert. Dazu gehören insbesondere:

Control Layer

Diese Ebene enthält Kataloge mit standardisierten Sicherheitskontrollen. Ein Beispiel ist ein Katalog mit Anforderungen aus einem Sicherheitsstandard.

Profile Layer

Profile dienen dazu, aus einem umfassenden Kontrollkatalog eine relevante Teilmenge auszuwählen oder anzupassen. So kann eine Organisation definieren, welche Kontrollen für einen bestimmten Systemtyp oder einen bestimmten Sicherheitslevel gelten. Typische Anpassungen sind

Hinweis

Diverse Tools sind mittels QR-Code zu finden. Auch das BSI hat die Grundschutz-Kataloge sowie den aktuellen Grundschutz++ ins OSCAL-Format überführt.



dabei: Ausschlüsse (modify remove), Hinzufügungen (modify add) oder das Setzen von Parametern. Ein Profil kann auch «aufgelöst» (resolve) werden.

Implementation Layer

Diese Ebene beschreibt, wie Kontrollen konkret umgesetzt werden. Dazu gehören System Security Plans (SSP) und Component Definitions. Damit lässt sich festhalten, welche technischen, organisatorischen oder prozessualen Massnahmen einer bestimmte Kontrolle erfüllen.

Assessment Layer

Diese Ebene unterstützt die Planung und Dokumentation von Prüfungen. Dazu zählen Assessment Plans (AP), Assessment Results (AR) sowie Plans of Action and Milestones, kurz POA&M. Das Assessment-Result-Modell beschreibt beispielsweise strukturierte, maschinenlesbare Berichte darüber, was geprüft wurde, wie geprüft wurde, wer geprüft hat, welche Feststellungen gemacht wurden und welche Risiken identifiziert wurden.

Wichtig zu verstehen ist, dass OSCAL kein einzelnes Audit-Tool und kein Ersatz für Sicherheitsstandards ist. Es handelt sich um ein gemeinsames Austauschformat.

Bedeutung

Da die Compliance immer komplexer wird und Organisationen oft mehrere Standards, Frameworks und gesetzliche Vorgaben parallel berücksichtigen müssen, wird ein gemeinsames Austauschformat immer wichtiger. Das umfasst unter anderem ISO/IEC 27001, NIST SP 800-53, branchenspezifische Vorgaben oder Cloud-Sicherheitsrichtlinien. Je mehr Anforderungen zusammenkommen, desto schwieriger ist es, alles im Blick zu behalten.

Ohne ein gemeinsames Datenmodell entstehen schnell doppelte Arbeiten. Eine Sicherheits-

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

kontrolle wird für ein Audit festgehalten, für ein anderes Audit erneut dokumentiert, in einem dritten Tool anders bezeichnet und in einem vierten Bericht wieder anders dargestellt. Das hat nicht nur ineffiziente Abläufe zur Folge, sondern auch Risiken: Es gibt unentdeckte veraltete Angaben, Nachweise sind inkonsistent, Zuständigkeiten fehlen an Klarheit und Prüfergebnisse sind schwer nachzuvollziehen.

OSCAL spielt eine wichtige Rolle, da es Compliance, Security Engineering und Automatisierung miteinander verbindet. Sicherheitskontrollen gelten nicht mehr als statische Textbausteine, sondern als strukturierte Daten. Es erlaubt eine viel bessere Nachvollziehbarkeit.

Das NIST hat OSCAL so konzipiert, dass es die Sicherheits- und Compliance-Prozesse modernisiert und automatisiert. Ziel ist es, kontrollbasierte Risikoanalysen und Nachweisprozesse effizienter, konsistenter und weniger fehleranfällig zu machen. Moderne IT-Umgebungen ändern sich laufend. Systeme werden automatisiert bereitgestellt, Infrastruktur wird als Code verwaltet, Sicherheitsprüfungen laufen kontinuierlich und Konfigurationen ändern sich dynamisch. Statische Compliance-Dokumente können mit dieser Geschwindigkeit kaum mithalten. Ein maschinenlesbares Format wie OSCAL passt besser zu solchen Betriebsmodellen.

Vorteile

Ein Mehrwert liegt in der Automatisierung. OSCAL ermöglicht es, Sicherheitsinformationen maschinell zu lesen, zu vergleichen, zu validieren und weiterzuverarbeiten. Dadurch lassen sich manuelle Tätigkeiten reduzieren. Beispielsweise können bestimmte Nachweise automatisch aus Systemkonfigurationen, Asset-Datenbanken oder Security-Scanning-Tools generiert und mit OSCAL-Strukturen verknüpft werden.

Auch die Nachvollziehbarkeit verbessert sich. In OSCAL kann abgebildet werden, welche Kontrolle aus welchem Katalog stammt, in welchem Profil sie enthalten ist, wie sie in einem System umgesetzt wird, wie sie geprüft wurde und welche Ergebnisse daraus entstanden sind. Dies

ist besonders wertvoll bei Audits, internen Kontrollen und regulatorischen Prüfungen.

Ein weiterer Vorteil ist die Wiederverwendbarkeit. Wenn ein Unternehmen eine saubere OSCAL-basierte Beschreibung ihrer Kontrollen und Implementierungen aufgebaut hat, kann sie diese Informationen für unterschiedliche Zwecke wiederverwenden: für interne Audits, Kundenanfragen, regulatorische Nachweise, Cloud-Zertifizierungen oder Lieferantenbewertungen.

Anwendungsmöglichkeiten

Eine naheliegende Anwendung ist die Verwaltung von Kontrollkatalogen. Unternehmen können Sicherheitsanforderungen in OSCAL abbilden und damit eine strukturierte Grundlage schaffen. Eine zweite Anwendung ist die Erstellung von Profilen. Ein vollständiger Sicherheitskatalog kann sehr umfangreich ausfallen. Nicht jede Kontrolle ist für jedes System relevant. Mit OSCAL-Profilen lassen sich spezifische Baselines definieren, zum Beispiel für eine Cloud-Anwendung, eine interne Plattform oder ein kritisches System.

Eine dritte Anwendung betrifft System Security Plans. Ein SSP beschreibt, wie ein konkretes System Sicherheitskontrollen erfüllt. In OSCAL kann diese Beschreibung strukturiert erfolgen. Dadurch lässt sich besser nachvollziehen, welche Komponenten, Prozesse und Verantwortlichkeiten zur Erfüllung bestimmter Kontrollen beitragen.

Eine vierte Anwendung ist die Prüfplanung. Mit einem Assessment Plan kann beschrieben werden, welche Kontrollen geprüft werden, welche Methoden verwendet werden, welche Rollen beteiligt sind und welche Systeme oder Komponenten Gegenstand der Prüfung sind.

Eine fünfte Anwendung ist die Dokumentation von Prüfergebnissen. Assessment Results können erfassen, welche Tests durchgeführt wurden, welche Feststellungen entstanden sind und welche Risiken identifiziert wurden. Diese Informationen können anschließend weiterverarbeitet werden.

Eine sechste Anwendung ist das Management von Massnah-

men und offenen Risiken. Das POA&M-Modell beschreibt strukturierte Informationen zu Massnahmenplänen und Meilensteinen. Es eignet sich damit für die Nachverfolgung von Schwachstellen, Audit-Feststellungen oder Compliance-Lücken.

Beispiele

Ein erstes Beispiel ist ein Cloud-Anbieter, der seinen Kunden nachweisen muss, wie bestimmte Sicherheitskontrollen umgesetzt werden. Statt jedem Kunden individuell ein Word-Dokument oder eine Excel-Liste zu liefern, kann der Anbieter seine Kontrollimplementierungen strukturiert in OSCAL beschreiben. Kunden oder Auditoren können diese Informationen automatisiert auswerten und mit eigenen Anforderungen abgleichen.

Ein zweites Beispiel ist ein Unternehmen, das ISO/IEC 27001, NIST SP 800-53 und interne Sicherheitsrichtlinien parallel verwalten muss. Viele Anforderungen überschneiden sich teilweise. Mit OSCAL kann das Unternehmen Kontrollinformationen strukturieren und Beziehungen zwischen Anforderungen, Umsetzungen und Nachweisen besser abbilden. Dadurch wird ersichtlich, welche technische Massnahme mehrere Kontrollen gleichzeitig unterstützt.

Ein drittes Beispiel ist eine Organisation, die regelmässige Audits durchführt. Der Prüfplan kann in OSCAL als Assessment Plan definiert werden. Nach der Prüfung werden die Ergebnisse als Assessment Results dokumentiert. Offene Punkte werden in einem POA&M-Modell erfasst.

Dadurch entsteht ein durchgängiger, maschinenlesbarer Prozess.

Ein viertes Beispiel betrifft DevSecOps. Eine Plattform stellt Infrastruktur automatisiert bereit. Sicherheitskontrollen wie Verschlüsselung, Logging, Netzwerksegmentierung oder Zugriffsschutz werden bereits im Deployment geprüft. Die Ergebnisse dieser technischen Prüfungen können in OSCAL-Strukturen überführt werden.

Fazit

OSCAL ist ein wichtiger Baustein für Sicherheits- und Compliance-Prozesse. Es löst nicht automatisch alle organisatorischen Herausforderungen, ersetzt keine Sicherheitsstrategie und macht auch kein Audit überflüssig. Sein Wert liegt vielmehr darin, dass es Sicherheitsinformationen in eine strukturierte, offene und maschinenlesbare Form bringt.

Informationen sind oft verstreut, manuell gepflegt, schwer vergleichbar und nur begrenzt automatisierbar. OSCAL schafft eine gemeinsame Sprache für Kontrollkataloge, Profile, Implementierungen, Prüfpläne, Prüfergebnisse und Massnahmenpläne. Dadurch können Unternehmen Nachweise einfacher erstellen, Prozesse automatisieren und damit die Nachvollziehbarkeit erhöhen.

Langfristig kann OSCAL helfen, Audits effizienter zu gestalten, Sicherheitsnachweise konsistenter zu führen und Compliance stärker in technische Betriebsprozesse zu integrieren.

Anzeige



BALANCE DRIVE
SWISS MOTION

Kronenrad Royal:

- axiale Freiheit des Ritzels
- Wirkungsgrad > 95 %
- Untersetzungen 1:1 30:1
- einfache Montage
- kompakte Bauweise

balance-drive.com



Kronenrad Royal®