Neue Sicherheitsrisiken im Fokus

Dr. Marius Hofmeister, OPITZ CONSULTING Deutschland GmbH

Die OWASP-Top-10 ist eine weltbekannte Rangliste der wichtigsten Sicherheitsrisiken für Anwendungen im Web. Sie wird in regelmäßigen Abständen vom Open Web Application Security Project (OWASP) herausgegeben. Ende 2017 wurde eine neue Version veröffentlicht, die zahlreiche Änderungen enthält. Neue Risiken sind hinzugekommen, alte wurden entfernt. Auch sonst gibt es einiges zu berichten.

Ziel von OWASP ist es, Einzelpersonen und Unternehmen dabei zu unterstützen, sichere Anwendungen zu entwickeln, zu kaufen und zu warten. Security für Software soll sichtbar sein. Die Non-Profit-Organisation legt Wert darauf, kommerzielle Produkte oder Services weder aktiv zu bewerben noch Empfehlungen auszusprechen, um die eigene Neutralität zu wahren *[1]*. Jeder, der Interesse an Security-Themen hat, ist aufgerufen, sich im Projekt einzubringen und einen Teil zu dessen Erfolg zu leisten. Auf den entsprechenden Webseiten finden sich Literatur, Werkzeuge und Standards zur Anwendungssicherheit. Konferenzen und Stammtische finden an zahlreichen Orten statt, regelmäßig auch in deutschen Städten.

Als eines von mehr als 90 aktiven OWASP-Projekten trägt die Top 10 dem übergeordneten Ziel der Schaffung von Awareness für Security seit der ersten Ausgabe 2003 kontinuierlich Rechnung. Die Rangliste der zehn wichtigsten Sicherheitsrisiken für Web-Anwendungen wird in der Regel alle drei bis vier Jahre neu aufgestellt und veröffentlicht.

Der lange Weg zur OWASP-Top-10

Grundlage für die Zusammenstellung der OWASP-Top-10 ist ein Pool von Daten. Im Mai 2016 wurde daher ein Data Call auf der OWASP-Website veröffentlicht. Mehr als 40 Einreichungen von Unternehmen, die auf Anwendungssicherheit spezialisiert sind, kann die neue Top 10 vorweisen. Darin enthalten sind Schwachstellen von Hunderten Organisationen sowie von mehr als 100.000 realen Applikationen und APIs. Um diese zu selektieren und zu priorisieren, finden unterschiedliche Faktoren Beachtung. Dazu gehören:

- Die Ausnutzbarkeit, Verbreitung und Auffindbarkeit einer Schwachstelle
- Die technischen Auswirkungen eines Angriffs *(siehe Tabelle 1)*

Durch die Multiplikation der gemittelten Einflussfaktoren mit den technischen Auswirkungen lässt sich so eine Rangfolge der Risiken ableiten. Keine Beachtung finden dabei die jeweiligen anwendungsspezifischen Bedrohungsquellen oder die geschäftsspezifischen Auswirkungen auf das konkrete Unternehmen. So kommen als Bedrohungsquellen einer Anwendung beispielsweise alle Nutzer des Internets oder alternativ auch nur unternehmensintern freigeschaltete Personen in Betracht. Ferner wird sich die Auswirkung eines erfolgreichen Angriffs auf das Unternehmen dahingehend unterscheiden, ob dabei hochsensible, personenbezogene Daten entwendet wurden oder nur wenige sicherheitsbedürftige Inhalte.

Neben den datengestützt erhobenen Risiken finden sich auch zwei sogenannte „Forward-looking Items" im Ranking. Es handelt sich hierbei um Risiken, die aus Expertensicht als für die Zukunft besonders relevant eingeschätzt werden. Sie wurden online über eine Umfrage unter Industrievertretern ermittelt, an der sich mehr als 500 Personen beteiligten.

Tabelle 2 stellt die OWASP-Top-10 aus dem Jahr 2017 im Vergleich zur Version von 2013 dar. Erkennbar ist, dass drei neue Risiken hinzugefügt und zwei zusammengeführt wurden (gelb markiert). Zwei Risiken aus der bisherigen Rangliste sind gänzlich verschwunden.

Bedrohungsquellen	Schwachstelle Ausnutzbarkeit	Schwachstelle Verbreitung	Schwachstelle Auffindbarkeit	Technische Auswirkungen	Auswirkungen auf das Unternehmen
Anwendungsspezifisch	Einfach	Sehr häufig	Einfach	Schwerwiegend	Anwendungs-/ Geschäftsspezifisch
	Durchschnittlich	Häufig	Durchschnittlich	Mittel	
	Schwierig	Selten	Schwierig	Gering	

Tabelle 1: Bewertungsschema für Risiken der OWASP-Top-10 [2]

OWASP-Top-10 – 2013		OWASP-Top-10 – 2017
A1: Injection	→	A1: Injection
A2: Fehler in Authentifizierung und Session-Management	→	A2: Fehler in Authentifizierung
A3: Cross-Site Scripting (XSS)	↘	A3: Verlust der Vertraulichkeit sensibler Daten
A4: Unsichere direkte Objektreferenzen	U	A4: XML External Entities (XXE) – NEU
A5: Sicherheitsrelevante Fehlkonfiguration	↘	A5: Fehler in Zugriffskontrollen – zusammengeführt
A6: Verlust der Vertraulichkeit sensibler Daten	↗	A6: Sicherheitsrelevante Fehlkonfiguration
A7: Fehlerhafte Autorisierung auf Anwendungsebene	U	A7: Cross-Site Scripting (XSS)
A8: Cross-Site Request Forgery (CSRF)	X	A8: Unsichere Deserialisierung - NEU
A9: Verwendung von Komponenten mit bekannten Schwachstellen	→	A9: Verwendung von Komponenten mit bekannten Schwachstellen
A10: Ungeprüfte Um- und Weiterleitungen	X	A10: Unzureichendes Logging & Monitoring – NEU

Tabelle 2: OWASP-Top-10 im Jahr 2017 im Vergleich zur Version von 2013 [2]

Im Vergleich zur ursprünglichen zeitlichen Planung ist die Top 10 im Jahr 2017 später als erwartet erschienen. Hintergrund waren kontroverse Diskussionen, die sich auf dem OWASP Summit 2017 entzündeten. Der dort diskutierte erste Release-Kandidat der Top 10 fand so wenig Anklang unter den Anwesenden, dass er schlichtweg abgelehnt wurde. Bemängelt wurden die zu geringe Datenbasis auf der einen Seite als auch die konkrete Auswahl der „Forward-looking Items" auf der anderen Seite. Die hier ursprünglich vorgeschlagenen Punkte „Ungenügende Angriffserkennung" und „Ungeschützte APIs" wurden zurückgestellt und später durch die Ergebnisse der Industrieumfrage ersetzt. Zwei der Gründerväter des Projekts, Dave Wichers und Jeff Williams, zogen sich im Laufe dieses Prozesses aus dem Projekt zurück. Die Leitung übernahm Andrew van der Stock mit den Stellvertretern Brian Glas, Neil Smithline und Torsten Gigler. Wer das Projekt in den letzten Jahren aufmerksam verfolgt hat, dem wird aufgefallen sein, dass sich die personellen Veränderungen auch in den neu veröffentlichten Top 10 wiederfinden. Große Teile des Dokuments wurden textuell neu verfasst, und häufiger als zuvor wird auf moderne Technologien und Architekturen wie Microservices und Single-Page-Applikationen Bezug genommen.

Die Risiken an der Spitze

An der Spitze der Top 10 rangieren wie schon im Jahr 2013 die Injection-Angriffe – trotz der Tatsache, dass der Bekanntheitsgrad dieser Schwachstelle größer kaum sein könnte. Offensichtlich ist noch viel Legacy-Code im Einsatz, der für die große Verbreitung der Schwachstelle sorgt. Schadhafte Daten werden ungefiltert an einen Interpreter weitergeleitet, der diese dann ausführt. Dies kann zu unerwünschten Lese- und Schreib-Operationen führen, bis hin zur feindlichen Übernahme eines Systems. Auch wenn die bekannteste Variante, SQL-Injection, meist die volle Aufmerksamkeit auf sich zieht, sollten je nach Anwendung auch Anfälligkeiten für beispielsweise LDAP-, XPath- oder NoSQL-Injection-Angriffe untersucht werden.

Im Gegensatz zu dieser konkreten Angriffsform auf Web-Anwendungen handelt es sich beim zweiten Risiko der Top 10 um eine grundsätzlichere Problematik: Der Punkt „Fehler in Authentifizierung" stellt fehlerhafte und damit anfällige Authentifizierungsmechanismen in den Mittelpunkt. Die Behebung von Schwachstellen in diesem Bereich ist meist aufwendiger, da Angriffe auf unterschiedliche Weise vonstattengehen können. Wie bei allen Risiken bietet OWASP in seinen Top 10 eine Liste von Literatur-Referenzen zum Umgang mit solchen Schwachstellen an; so wird, wenn möglich, der Einsatz von Multi-Faktor-Authentifizierung empfohlen, also die zeitgleiche Verwendung mehrerer unterschiedlicher Authentifizierungstechniken. Dies beugt Brute-Force-Attacken vor und erschwert das Entwenden von Zugangs-Informationen. Ferner ist zu erwarten, dass auch der Einsatz biometrischer Eigenschaften im Rahmen von Authentifizierungsszenarien zukünftig zunehmen wird. In den Top 10 auf Platz drei aufgerückt und damit an Bedeutung gewonnen hat der „Verlust der Vertraulichkeit sensibler Daten". Häufigstes Problem an dieser Stelle ist die nicht vorhandene oder mangelhafte Verschlüsselung sensibler Datenbestände. Zu Beginn steht eine Untersuchung des Schutzes, den Daten in der Übertragung und Speicherung brauchen. Wie sensibel sind die Daten, die erhoben werden? Werden aktuelle Verschlüsselungsalgorithmen eingesetzt? Ist eine Speicherung und Übertragung dieser Daten wirklich notwendig? Dies sind nur einige der Fragen, denen sich Entwickler stellen sollten.

Neue Risiken im Jahr 2017

Drei neue Risiken haben den Weg in die Top 10 gefunden. „XML External Entities" (XXE) wurde datengestützt erhoben, während „Unsichere Deserialisierung" und „Unzureichendes Logging & Monitoring" über die Industrie-Umfrage als „Forward-looking Items" Einzug gehalten haben.

Ursache für XML-basierte Angriffsszenarien ist die Möglichkeit, externe Entitäten anzugeben, die über einen URI referenziert werden. Wenn derartiges XML ungeprüft von Anwendungen entgegengenommen wird, können schützenswerte Daten freigelegt werden, bis hin zur Ausführung von Denial-of-Service-Attacken. Die „Billion Laughs"-Attacke, die über die Expandierung einer Milliarde Entitäten den zur Verfügung stehenden Speicherplatz eines Prozesses überschreitet, ist ein bekanntes Beispiel für einen XML-basierten Angriff. In jedem Fall empfiehlt es sich, wenn XML-Parser im Einsatz sind, diese entsprechend den Hinweisen des XML External Entity (XXE) Prevention Cheat Sheet *[3]* der OWASP zu konfigurieren.

Nächster Punkt sind die über Industrie-Umfragen ermittelten Risiken. Dass „Unsichere Deserialisierung" gewählt wurde, zeigt, wie sehr die Diskussionen der letzten Jahre (besonders auch im Java-

Umfeld) das Bewusstsein für diese Angriffsart geschärft haben. Durch Serialisierung werden strukturierte Daten zur Speicherung oder Übertragung auf eine sequenzielle Form abgebildet. Um einen Endpunkt zur Deserialisierung anzugreifen, müssen sogenannte „Gadgets" vorliegen, also ausnutzbare Klassen auf dem Klassenpfad der angegriffenen Anwendung. So kann es zu einer Remote Code Execution kommen, dem Ausführen von Schadcode auf den Servern der jeweiligen Webanwendung. Umfassende Abhilfe schafft hier einzig die Vermeidung von Deserialisierung aus nicht vertrauenswürdigen Quellen.

Das zweite „Forward-Looking Item" der Industrie-Umfrage, „Unzureichendes Logging & Monitoring", nimmt sich der Problematik an, dass Sicherheitslücken oftmals nicht zeitnah erkannt werden und lange verfügbar bleiben. In sensiblen Anwendungen ist es empfehlenswert, mithilfe von Detection-Points Ereignisse wie fehlerhafte Log-ins oder verdächtige Eingaben zu erkennen und dann bei Überschreitung gewisser Thresholds eine entsprechende Aktivität wie die Sperrung eines Accounts durchzuführen. Im Idealfall reagiert die Anwendung somit selbstständig auf Angriffe.

Neben diesen drei neu hinzugekommenen Risiken wurden „Unsichere direkte Objekt-Referenzen" und „Fehlerhafte Autorisierung auf Anwendungsebene" zusammengefasst. Dies kam insofern wenig überraschend, als es sich hierbei bereits in früheren Versionen der Top 10 um einen gemeinsamen Punkt handelte. Das Ziel, durch Aufsplittung höhere Aufmerksamkeit für die Thematik zu erreichen, wurde in den Augen vieler erreicht.

Altbekanntes auf wechselnden Plätzen

Weiterhin in den Top 10 vertreten sind die Risiken „Sicherheitsrelevante Fehlkonfiguration", „Cross-Site Scripting (XSS)" sowie die „Verwendung von Komponenten mit bekannten Schwachstellen". „Sicherheitsrelevante Fehlkonfiguration" rückt die fehlerhafte Konfiguration von Anwendungen, Frameworks, Applikations-, Web- und Datenbank-Servern sowie deren Plattformen in den Fokus. Voreinstellungen müssen gewartet und Updates regelmäßig eingespielt werden, damit bekannte Sicherheitslücken nicht allzu leicht ausgenutzt werden können.

„Cross-Site Scripting (XSS)" hat demgegenüber glücklicherweise einen Bedeutungsverlust in den Top 10 zu verzeichnen. Lange Zeit handelte es sich hierbei um die Schwachstelle mit der weitesten Verbreitung in Web-Anwendungen. Ähnlich wie bei den Injection-Angriffen liegt eine Ursache für diese Lücke darin, dass eine Anwendung ungeprüft Daten annimmt und diese dann zusätzlich noch ungeprüft wieder ausgibt. Angriffsziel ist der Browser des Website-Nutzers, in dem dann in der Regel JavaScript-Schadcode ausgeführt wird. Benutzerdaten können so ausgelesen und Sessions übernommen werden.

Das letztgenannte Risiko, „Verwendung von Komponenten mit bekannten Schwachstellen", thematisiert, dass häufig anfällige Komponenten eingesetzt werden, die dringend ausgetauscht oder aktualisiert werden sollten. Ungenutzte Abhängigkeiten sollten regelmäßig entfernt und Scans mit Werkzeugen wie den OWASP Dependency Checks *[4]* durchgeführt werden.

Ganz aus den Top 10 verabschiedet haben sich die alten Bekannten „Cross-Site Request Forgery (CSRF)" sowie „Ungeprüfte Um- und Weiterleitungen". Während Frameworks wie Java Server Faces (JSF) heutzutage standardmäßig Schutzmechanismen gegen CSRF bieten, hat die Ausnutzung ungeprüfter Um- und Weiterleitungen schlichtweg an Bedeutung verloren.

Neue Transparenz in den Top 10 und Durchhaltevermögen in der Umsetzung

Mit dem Jahr 2017 ist die OWASP-Top-10 transparenter geworden denn je. Auf GitHub *[5]* sind große Teile der Projekt-Kommunikation einsehbar. Die Beteiligung an aktuellen Diskussionen ist ohne große Umschweife möglich. Zu betonen ist jedoch, dass auch eine vollständige Beachtung der Rangfolge keine umfassende individuelle und ganzheitliche Analyse der eigenen Anwendung ersetzen kann. Unzählige Sicherheitsrisiken, die individuell gefährlich werden können, existieren über die Top 10 hinaus.

Gefordert ist in jedem Fall Durchhaltevermögen, wenn Sicherheitsthemen angegangen werden. Oft lassen sich Schwachstellen nicht von heute auf morgen beseitigen, geschweige denn erkennen. Aber wer mit Ausdauer dabeibleibt und das Ziel einer „möglichst sicheren" Webanwendung nicht aus den Augen verliert, der wird damit auch langfristig erfolgreich sein.

Literatur

[1] OWASP Website: *https://www.owasp.org*
[2] OWASP-Top-10 – 2017: *https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*
[3] XML External Entity (XXE) Prevention Cheat Sheet: *https://www.owasp.org/index.php/XML_External_Entity_(XXE)_Prevention_Cheat_Sheet*
[4] OWASP Dependency Check: *https://www.owasp.org/index.php/OWASP_Dependency_Check*
[5] OWASP Top 10 GitHub Issues: *https://github.com/OWASP/Top10/issues*

Dr. Marius Hofmeister
marius.hofmeister@opitz-consulting.com

Dr. Marius Hofmeister ist als Senior Consultant und Entwicklungsleiter in Kundenprojekten bei OPITZ CONSULTING Deutschland beschäftigt und widmet sich schwerpunktmäßig dem Entwurf und der Implementierung von Web-Anwendungen in Back- und Frontend. Von besonderem Interesse für ihn sind dabei Security-Aspekte der verwendeten Technologien.