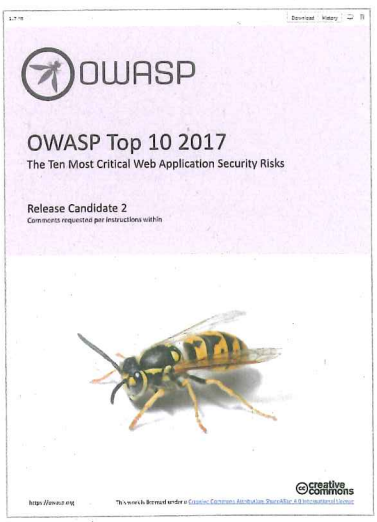
AppSec: Wirbel um die OWASP Top 10

Zielkonflikte

Joshua Tiago

Mit Spannung erwarteten die Besucher der diesjährigen AppSec Neuigkeiten zum Renommierprojekt der OWASP: der Top-10-Schwachstellenliste. Die damit einhergehenden Interessenkonflikte hatten schon im Vorfeld für Unmut gesorgt.

Die IT-Security-Welt ist im Wandel und stets in Bewegung. Noch vor zwei bis drei Jahren wurde auf vielen Security-Konferenzen über das Für und Wider von IoT diskutiert. Einige hielten das Internet of Things für eine Modeerscheinung und bestenfalls relevant für private Nutzer. Heute sieht das Bild grundlegend anders aus. Unternehmen aus allen denkbaren Branchen bieten IoT-Produkte an, meist in Kombination mit diversen Cloud-Diensten. Nun stehen IT-Sicherheitsverantwortliche und Entwickler vor der riesigen Herausforderung, Wege zu finden, die schnell auf den Markt gebrachten Produkte angemessen abzusichern. Diese Entwicklung bestätigte sich auf der diesjährigen AppSec-Konferenz des OWASP (Open Web Application Security Project) in Orlando, Florida. Sicherheitsexperten und Researcher aus aller Welt referierten darüber.



Die neue Top-10-Schwachstellenliste lässt auf sich warten – Grund ist ein Konflikt des Projekts mit der selbstverordneten Produktunabhängigkeit.

IoT-Produkte haben höchst unterschiedliche Einsatzzwecke, aber in der Regel einige Dinge gemeinsam: Oftmals werden Daten lokal erhoben, dann in die Cloud des Anbieters hochgeladen und dem Benutzer abschließend in einem Frontend zur Verfügung gestellt. Im Vortrag „Top 10 Security Best Practices to secure your Microservices" stellte Chintan Jain Maßnahmen vor, Microservices abzusichern. An erster Stelle steht der sichere Transport der Daten. Jain empfahl, diesen mittels TLS zu verschlüsseln. Außerdem sollten alle beteiligten IoT-Komponenten das jeweilige Zertifikat des Endgeräts überprüfen.

Des Weiteren empfahl Jain, den Aufbau der Netzwerkumgebung, in der die Daten entgegengenommen und verarbeitet werden, zu überdenken. Kritische Daten sollten stets in eigenen Netzwerksegmenten vom Rest der Komponenten getrennt werden. Zur Absicherung von Microservices gehören jedoch auch Maßnahmen zum Verhindern von Denial-of-Service-Angriffen. Gelingt es einem Angreifer, die Verfügbarkeit einzuschränken, sind oftmals alle Kunden betroffen. Als Maßnahmen nannte Jain unter anderem „Rate Limiting", „Throttling" oder „Daily Limits". Das begrenzt im Falle eines Angriffs die Auswirkungen.

Die Keynote „Discussion on Application Security" am ersten Konferenztag wurde von allen Konferenzteilnehmern mit Spannung erwartet. Bis kurz vor Beginn war nicht bekannt, über welches Thema Jim Manico und John Steven referieren würden. Manico ist Global Board Member bei der OWASP – und so überraschte es niemanden, dass die Keynote das wichtigste aller OWASP-Projekte zum Inhalt hatte: die Top 10. Bereits im Vorfeld war in diversen Veranstaltungen und Gremien heftig diskutiert worden. Was war geschehen? In den vergangenen Monaten hatten die Projektverantwortlichen einen Release Candidate (RC1) vorgestellt.

Produktempfehlungen nicht akzeptabel

In Security-Kreisen stieß das Dokument sehr schnell auf viel Kritik, da spezielle Sicherheitsprodukte als Maßnahmen empfohlen wurden (Web Application Firewalls (WAF) und Runtime Application Self-Protection Security (RASP)). Wie Manico erklärte, hätte dies zur Folge gehabt, dass viele Unternehmen zu solchen Produkten hätten greifen müssen, um Vorgaben einzuhalten, die explizit die OWASP Top 10 als Mindeststandard fordern. Ein Beispiel hierfür ist PCI/DSS, der Sicherheitsstandard der Kreditkartenindustrie.

Steven stellte klar, dass das OWASP-Projekt nicht interessengesteuert ist, und gab zu, dass solche Alleingänge weder Transparenz noch Vertrauen schaffen. Darum wurde im Vortrag das künftige Vorgehen für das OWASP-Top-10-Projekt vorgestellt. Eine der Konsequenzen traf die Projektleiter: Sie wurden bereits ersetzt. Künftig möchte das OWASP-Top-10-Projekt mehr Offenheit bei der Entscheidungsfindung. Im November soll nun das abschließende OWASP-Top-10-2017-Dokument erscheinen.

Einen kurzen Blick in die Zukunft bot der Vortrag „Leveraging Blockchain for Identity and Authentication in IoT is good for Security", den Donald Malloy präsentierte. Malloy, der sich seit vielen Jahren mit den unterschiedlichsten Technologien und Protokollen für sichere Authentifizierung beschäftigt, stellte einen theoretischen Ansatz vor, Probleme im Bereich Authentifizierung zu lösen. Blockchain ist seit der rasanten Entwicklung von Bitcoin und anderen Kryptowährungen vielen ein Begriff.

Als dezentrales Buchführungssystem bietet die Blockchain-Technologie die Möglichkeit, Transaktionen oder Berechtigungen fälschungssicher zu speichern und diese für alle Parteien überprüfbar zu machen. Die von Malloy präsentierte Lösung ist ein theoretischer Ansatz, für den es noch keine Produkte gibt. Bis dahin gilt es, hier noch einige Hürden zu nehmen. Beispielsweise ist die sogenannte Block Size beschränkt. In einer IoT-Welt, in der jede Sekunde weltweit Tausende von Anfragen sowie An- und Abmeldungen erfolgen, kann eine zu kurz gewählte Block Size schnell zum Problem werden.

Angreifbares NoSQL

An Entwickler und Administratoren richtete sich Johannes Ullrichs spannender Beitrag „NoSQL is Not NoVulnerable". Er beschrieb, wie für viele Unternehmen NoSQL-Datenbanken zum gravierenden Sicherheitsproblem werden. NoSQL ist in den letzten Jahren bei Entwicklern in der Gunst gestiegen. Es gibt viele Bereiche, in denen solche Datenbanken den relationalen Datenbanksystemen überlegen sind. Prominente Vertreter sind MongoDB oder Apache Cassandra. Bekannte Schwachstellen wie SQL Injection sind in diesem Kontext in der Regel ungefährlich. Allerdings eröffnen die vielen komplexen Datentypen, die in NoSQL-Datenbanken unterstützt werden, neue Angriffsvektoren. Einfache Zugriffskontrollen, wie sie bei den meisten Datenbanksystemen bekannt sind, gibt es bei einigen NoSQL-Datenbanken schlichtweg nicht. Somit werden solche Datenbanken zum Angriffsziel, sobald sie im Internet erreichbar sind. Entwickler und Administratoren sollten daher stets prüfen, ob die Konfiguration der Datenbanken entsprechend gehärtet wurde. (ur)