Viele Analysten sind der Ansicht das Sicherheitslücken in Webapplikationen zu den größten Sicherheitsbedrohungen gehören, denen Unternehmen heutzutage ausgesetzt sind. Mittlerweile wurden viele Anstrengungen unternommen um die Risiken zu verstehen, die von schadhaften Eingaben mit SQL-Injektionen , Cross-Site-Scripting (XSS) und anderen Gefährdungen für Java Webapplikationen ausgehen.

Signifikant weniger Aufmerksamkeit scheint allerdings die Frage zu erhalten, was Anwendungsentwickler wissen müssen um die Wahrscheinlichkeit einer auftretenden Sicherheitslücke beim Schreiben ihrer Software zu reduzieren.

Eine Gruppe von Sicherheitsmanagern, von einem Dutzend Organisationen, inklusive Booz Allen Hamilton, Deloitte & Touche, Boeing und Ounce Labs, hoffen diesem Defizit entgegenwirken zu können. Sie sind im Begriff ein Dokument zu veröffentlichen das als Richtschnur für die Entwicklung von sicheren Webapplikationen dienen soll. Das Dokument ist als eine Liste mit grundlegenden Tipps und Hinweisen für Programmierer zu verstehen.

Die Gruppe wurde zusammengestellt von dem Bethesda, Md.-based SANS Institut . SANS ist eines der renommiertesten Institute auf diesem Gebiet und die mit Abstand größte Quelle für Sicherheitstraining, Zertifizierung und Forschung weltweit. Das Ziel war es ein Dokument zu verfassen, dass es Java Entwicklern ermöglicht zu verstehen wo die gängigen Sicherheitsprobleme in Bezug auf Webapplikationen liegen, sagte Alan Paller, Direktor für Forschung bei SANS.

Das Dokument wird für öffentliche Kritiken und Verbesserungsvorschläge in den nächsten Wochen zur Verfügung stehen. Die endgültige Version wird in Form eines blaugedruckten Sicherheitsdokuments für Java Anwendungsentwickler Anfang des nächsten Jahres erscheinen.

Viele der in der Liste enthaltenen wichtigen Anweisungen, beziehen sich auf bereits eingehend bekannte Aspekte innerhalb der Community, meint Ryan Berg, Chief Security Officer am Ounce Labs. Die Idee hinter dem Dokument ist, einen Fokus auf die allgemeinen Schwachpunkte in

Java zu richten, die man oft in vielen Java Quellcodes sehen kann. Es gilt das Wissen über die Sicherheit bei allen kompetenten Java-Programmierern zu erweitern. "Das sind die wesentlichen Punkte die wir erreichen wollen und das jeder Entwickler in die Lage versetzt wird, die Richtlinien effizient in seiner Applikation zu implementieren." sagte Berg.

Nach Ansicht der Gruppe, sind die folgenden Punkte für jeden Java-Programmierer von Bedeutung:

- *Eingabebehandlung.* Um ihren Code gegen Cross-Site Scripting , SQL-Injektionen und ähnlichen Angriffen zu schützen, müssen Java-Programmierer in der Lage sein Programme zu schreiben, die die Benutzereingaben richtig auswerten (validieren) und verarbeiten. Sie müssen wissen *wann* sie die Eingaben auswerten müssen und nicht nur *was* sie daran auswerten müssen. Programmierer müssen die allgemeinen Quellen für Eingaben in ihren Anwendungen erkennen, wie beispielsweise HTTP-Requests, Applet Sockets und Backend Datenbanken.

- *Authentifizierung und Sessionverwaltung.* Das ist laut Berg, einer der Bereiche denen Java-Programmierer eine besondere Aufmerksamkeit widmen müssen. Java Anwendungen erfordern oft sicherheitsrelevante Überlegungen basierend auf der Identität einer Person. Daher müssen Java-Programmierer den Authentifizierungsprozess verstehen, wie man Verschlüsselungen und Zertifizierungstechnologien einsetzt um die verschiedenen Prozesse zu schützen und wie man den Dokumentenstatus mithilfe einer Session verwaltet.

- *Zugriffskontrolle.* Java-Programmierer müssen verstehen, wie man Anwendungen schreibt, die diverse Zugriffskontrollregeln unterstützen. Sie müssen Funktionen bereitstellen, die den Zugriff auf Systemressourcen einschränken und Funktionen die auf bestimmten Regeln basieren. Darüberhinaus müssen sie verstehen, wie die Java Authentifizierungs- und Autorisierungsdienste funktionieren und wie sie damit eine Zugriffskontrolle implementieren können.
- *Fehler- und Ausnahmebehandlung.* Das ist eines der Bereiche dem Java-Programmierer bisher auch zu wenig Aufmerksamkeit geschenkt haben, der aber sehr wichtig ist, sagte Berg. Entwickler müssen die Prinzipien hinter sicherheitsrelevanten Anmeldungsereignissen, wie Benutzeranmeldungen und Abmeldungen, und Änderungen in den Benutzerberechtigungen verstehen. Sie sollten wissen wieviele Informationen aufgezeichnet werden sollten, wenn ein Fehler oder eine Ausnahme ausgelöst wird.
- *Verschlüsselungsdienste.* Entwickler müssen wissen wann und wie sie Verschlüsselung einsetzen müssen, um sensitive Daten zu schützen. Sie sollten auch Verantwortung im Umgang mit externen Links tragen und darauf achten, welche Verbindungen über sichere, verschlüsselte Kanäle (SSL) laufen müssen und welche nicht.

Neben den genannten Bereichen mit denen man sich vertraut machen sollte, beinhaltet die SANS Liste andere wichtige Sicherheitsaspekte für Java-Programmierer. Diese umfassen Kenntnisse in der Art und Weise, wie die eigene Anwendung mit anderen Anwendungen interagiert und wie man diese Interprozesskommunikation absichert. Java-Programmierer sollten auch die sicherheitsrelevanten Auswirkungen von eingebauten Datentypen und die Funktionsweise der Java Speicherverwaltung kennen.

Vielen Programmierern - auch nicht Java-Programmierern - wird das Dokument von SANS dabei helfen sichereren Code zu schreiben. Sobald die endgültige Version des Dokuments erscheint, wird dieses selbstverständlich auch auf der Seite CodePlanet veröffentlicht werden.