Dipl.-Inf. Max Ziegler,
SKYTALE Online-Akademie für IT-Sicherheit

App-solut sicher?!?

Web-Applikationen sind die digitalen Eingangspforten der Kaufhäuser und Dienstleister im Internet. Die Kunden betreten die Online-Shops, Versicherungen und Banken über Eingabemasken und Login-Bereiche und wickeln dort ihre Geschäfte ab. Doch auch Hacker begehren Einlass und nehmen die Anwendungen genauer unter die Lupe. Die Erfahrung der vergangenen Jahre zeigt: Noch immer sichern nicht alle Seitenbetreiber ihre Web-Apps angemessen ab. Viele altbekannte Schwachstellen und Sicherheitslücken sind nach wie vor häufig präsent.

Es ist eine Hitliste der besonderen Art, die das Open Web Application Security Project (OWASP) seit 2003 regelmäßig veröffentlicht: die zehn häufigsten Sicherheitsrisiken von Web-Applikationen, die erhebliche Gefahren für Unternehmen und ihr Kerngeschäft bergen können. Auch die letzte Analyse aus dem Jahr 2013[1] basiert auf Datenerhebungen von Firmen, die sich auf Anwendungssicherheit spezialisiert haben. Die Daten umfassen mehr als 500.000 Schwachstellen aus hunderten von Unternehmen. Voraussichtlich 2016 werden die Top-10-Themen vom OWASP neu aufgelegt und zusammen mit Einschätzungen zur Ausnutzbarkeit, Auffindbarkeit und den Auswirkungen gewichtet.

Sicher ist nur, dass viele Web-Apps immer noch unsicher sind

Werden die Injection Flaws ihre Spitzenposition auch im sechsten Jahr in Folge halten können? Wird es die Cross-Site Request Forgery (CSRF) – derzeit auf Platz 8 – auch 2016 wieder in die Hitliste schaffen? Welche Schwachstelle steigt auf, welche steigt ab und welche wird erstmals in die Top 10 aufgenommen? Die Antworten bleiben bis zur Veröffentlichung der offiziellen OWASP-Release-Version natürlich ungewiss, denn nur so viel ist sicher: Es mangelt nicht an Kandidaten, die Liste zu füllen. Und mit großer Wahrscheinlichkeit werden sich alte Bekannte wie sicherheitsrelevante Fehlkonfigurationen oder der Verlust der Vertraulichkeit sensibler Daten als Evergreen im Feld der Favoriten behaupten können.

Es sei die Frage gestattet: Warum ist das so, obwohl das Thema IT-Sicherheit in jüngster Vergangenheit an nie da gewesener Bedeutung gewonnen hat? Warum scheinen alle Appelle von Verbänden, Politik und Wirtschaft zu verhallen, die sicherheitsrelevanten Schwachstellen in den Griff zu bekommen? Wieso tun sich die Unternehmen so schwer damit, ihre digitalen Pforten und Portale adäquat zu sichern? In der realen Welt mangelt es schließlich auch nicht an Kaufhausdetektiven, Wachmännern, Überwachungskameras und Diebstahldetektoren, die lautstark alarmieren, sobald nicht bezahlte Ware durch die Hintertür verschwindet oder der Tresor geknackt wurde.

Den Gegner und seine Methoden kennen

Möglicherweise spielt bei den Defiziten der IT-Sicherheit, die auch die Studie des Bitkom[2] aus dem Frühjahr 2015 attestiert hat, ein wichtiger Aspekt eine zentrale Rolle, der in der öffentlichen Diskussion zu wenig Beachtung findet: Die Mitarbeiter und IT-Verantwortlichen müssen schon bei der Entwicklung und Implementierung von Web-Applikationen wissen, welche Risiken drohen, wie Schwachstellen für zweifelhafte Machenschaften ausgenutzt werden können, wie die Angriffe auf die Server ablaufen, wie Hacker denken, handeln und welche Werkzeuge sie benutzen. Schließlich kann nur derjenige geeignete und projektspezifische Sicherheitsmaßnahmen entwickeln, der die Vorgehensweise und die Methoden der Angreifer im Detail kennt.

Doch diese Sichtweise, auch die Perspektive der Gegner einzunehmen, ruft in unserer Gesellschaft und in den Unternehmen nicht selten Irritationen hervor. Denn schließlich stehen die Hacker zusammen mit Räubern, Banditen und Kriminellen in einer Ecke. Die eigenen Mitarbeiter als rechtschaffende Menschen sind aufgefordert, sich zu distanzieren von derlei Machenschaften und sich an die geltenden Gesetze rund um die Informationssicherheit zu halten. Diese Forderungen sind absolut berechtigt und durch die aktuelle Gesetzeslage gut begründet. Dennoch verkennt derjenige den Ernst der Lage, der annimmt, ein umfassender Schutz der Web-Applikation kann erreicht werden, auch ohne mögliche Angriffsszenarien durchzuspielen. Denn dass die Hacker zuschlagen und sich dabei vor allem auf die „leichte Beute“ konzentrieren, steht nicht erst seit der Studie des Bitkom außer Frage.

Vorsicht ist besser als Nachsicht

Doch der Blick in die betriebliche Praxis in vielen Unternehmen zeigt: Die Web-Security fristet bei Entwicklung und Implementierung allzu oft ein Schattendasein, wenn diese nicht das eigentliche Kerngeschäft darstellt oder dieses stark gefährdet. Dann stehen meist Nutzerfreundlichkeit, Performance, Kompatibilität, Ressourcen- und Kosteneffizienz sowie Optik und Design im Vordergrund. Ohne Zweifel hat ein Entwicklerteam damit schon genügend Herausforderungen und Projektdruck zu meistern, sodass die Sicherheit schnell hinten ansteht. Indes wäre es dem gesamten Projekt und seinem Erfolg zuträglich, wenn jeder der Beteiligten auch den Blickwinkel der Hacker einnehmen könnte.

Unter dieser Prämisse programmiert, wird ein Sicherheitsaudit durch unabhängige Experten und Spezialisten dann gute Arbeit bei der Applikation bescheinigen – und nicht wie sonst vielfach üblich auf die vielfältigen Schwachstellen und den Nachbesserungsbedarf hinweisen. Denn ist der Quell-Code erst einmal geschrieben und das Serversystem konfiguriert, dann ist es meistens schwer, die Einfallstore effektiv und kostengünstig abzusichern. ◀

[1] *https://www.owasp.org/images/4/42/OWASP_Top_10_2013_DE_Version_1_0.pdf*

[2] *https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html*

Produktanbieter:

Berater/Dienstleister: