Die Reifeprüfung: Application Security Audit

Nicht ausreichend gesicherte Webapplikationen öffnen Unberechtigten ein Einfallstor ins interne Firmennetz. Zusätzlich ist die Verfügbarkeit nicht gewährleistet. Wie können Unternehmen diese Achillesferse in ihrer IT-Infrastruktur schützen?

→ **VON CHRISTOPH BAUMGARTNER & JAN ALSENZ**

Seit ein paar Monaten überschlagen sich wieder die Meldungen über spektakuläre Hackerattacken und Datendiebstähle. Die Häufung derartiger Vorfälle hat viele Ursachen, zum Beispiel ein verändertes Rechts- bzw. Unrechtsbewusstsein, gepaart mit monetären Interessen und Geltungsdrang (Steuer-CD oder Wikileaks/Anonymous), oder die Verlagerung von Geheimdienstaktivitäten vom realen in den virtuellen Raum (Hackerangriffe auf EDA und IWF oder Stuxnet). Ein wichtiger Faktor ist auch die zunehmende Komplexität der IT-Infrastrukturen – Buzzword Cloud lässt grüssen. Solange die IT vom Unternehmen selbst betrieben wurde, war die Anzahl der Akteure zumindest überschaubar. Mit dem Outsourcing kritischer Systeme muss man sich vermehrt auf den Wortlaut der Verträge verlassen. Der Vertragsausformulierung kommt damit immer grössere Bedeutung zu, insbesondere, was den Datenschutz (aus Sicht des Konsumenten) und den Informationsschutz (aus Sicht des Unternehmens) betrifft.

Viele Regierungen haben die sich ändernden Rahmenbedingungen erkannt und Cyber-Abwehr-Institutionen geschaffen, die in Zukunft auch international kooperieren. Der Umstand, dass sich anlässlich einer kürzlich durchgeführten Konferenz nicht alle teilnehmenden Länder dazu bereit erklärt haben, Cyber-Delikte wie herkömmliche Delikte zu ahnden, lässt allerdings darauf schliessen, dass sich einige Staaten nicht nur digital verteidigen, sondern auch angreifen.

Christoph Baumgartner ist CEO und Inhaber der auf Security Audits spezialisierten OneConsult GmbH → **www.oneconsult.com**

Jan Alsenz ist Team Leader Security Audits und Teilhaber im selben Unternehmen. Seine Spezialgebiete sind komplexe Security Audits, Systemanalysen und Reverse Engineering

BRAVE NEW WORLD

Heutzutage kann es sich kein überregional tätiges Unternehmen mehr leisten, nicht im Internet präsent zu sein. Was vor zehn Jahren primär der Marketingkommunikation diente, ist mittlerweile zu einem Point of Sales oder einer Service Station geworden. Wir sind es gewohnt, online einzukaufen, Reisen im Internet zu buchen und unsere Zahlungen am Computer zu erledigen. Ganz zu schweigen von Facebook, Xing, Twitter und Co.

Die Verwaltungen ziehen nach, betreiben Onlineschalter und bauen ihr Angebot kontinuierlich aus. Kurzum, heutzutage werden via Internet selbst so hochsensible Informationen wie Patientendaten ausgetauscht, deren Handhabung gesetzlich streng reguliert ist. Hier greift die Verantwortung der Geschäftsleitung, weil per Gesetz gefordert wird, dass die Unternehmen schützenswerte Daten mittels geeigneter Massnahmen vor unberechtigtem Zugriff schützen müssen. Doch was kann man tun? Firewall, Virenschutz und das regelmässige Einspielen von Sicherheits-Patches sollten selbstverständlich sein. Doch reicht dies aus? Machen Sie den Test.

BILD: ISTOCKPHOTO

«Korrekte Authentisierung, Autorisierung und Validierung sind die Säulen der Application Security»

Jan Alsenz

APPLICATION SECURITY AUDIT

Der Application Security Audit ist eine gründliche, technische, unprivilegierte und privilegierte Sicherheitsüberprüfung einer Applikation und der zugehörigen Komponenten aus der Perspektive eines Angreifers mit Skill Level «Hacker/Cracker». Es handelt sich dabei um einen simulierten, realitätsnahen Hackerangriff auf eine Applikation samt zugehöriger Systeme im Front- und Backend. Während der zur Verfügung stehenden Testzeit wird systematisch nach allen Sicherheitslücken gesucht. Untersuchungsobjekt können sowohl Webapplikationen, mobile Apps als auch klassische Client/Server-Applikationen sein. Der Fokus liegt auf allen Schichten und Komponenten, da es einem Angreifer egal ist, ob er eine Schwachstelle im Betriebssystem, im Browser, in der Applikation, in der Datenbank, auf dem PC oder Smartphone ausnutzen kann, um zum Ziel zu kommen. Neben den klassischen Angriffstechniken können beim Application Security Audit auch Techniken wie Code Review, Reverse Engineering (Hardware und Software), API Monitoring, Network Sniffing & Packet Analysis und Injection Tests zum Einsatz kommen. Gerade bei komplexen Applikationen, deren Tiers auf mehrere Provider verteilt sind, ist es oft auch sinnvoll, die Prozesse zu auditieren.

Der Auftraggeber definiert den Informationsgrad beider Parteien, also der Tester und Administratoren/Anwender der zu testenden Systeme. Die Spanne reicht vom Double-Blind-Ansatz, in dem keine Partei besondere Informationen erhält, über den Black-Box-Ansatz, bei dem die Administratoren über den bevorstehenden Test informiert werden, die Tester aber keine Informationen über das Untersuchungsobjekt erhalten, bis zum White-Box- oder Tandem-Ansatz, bei dem beide Parteien volle Informationen erhalten. Aus Kostenüberlegungen wird oft der Grey-Box-Ansatz verfolgt, bei dem die Administratoren über den anstehenden Test informiert werden, und die Tester so viele Informationen über das Untersuchungsobjekt erhalten, wie sie für die Tests benötigen, ohne sich durch Hunderte Seiten Dokumentationen lesen oder Information mühsam zusammensammeln zu müssen.

«Die Kosten von Application Security Audits fallen kaum ins Gewicht – der Nutzen umso mehr»

Christoph Baumgartner

Im Gegensatz zum sogenannten «Security Scan» und «Penetration Test» werden beim Application Security Audit auch privilegierte Tests (mit Kenntnis gültiger Zugriffsinformationen wie User ID/Passwort und Hardware Tokens) durchgeführt. Angegriffen wird also auch aus der Insider-Perspektive. Anschliessend werden die Ergebnisse und passende Massnahmenvorschläge im schriftlichen Schlussbericht dokumentiert.

Für die Durchführung technischer Security Audits bieten sich anerkannte Methoden an, zum Beispiel das «Open Source Security Testing Methodology Manual» (OSSTMM, www.osstmm.org) und speziell für Web Application Security Audits das «Open Web Application Security Project» (OWASP, www.owasp.org).

FINDEN, BEVOR ES DER HACKER TUT

Die Application Security steht und fällt mit der korrekten Umsetzung von Authentisierung, Autorisierung und Validierung. Im Audit-Alltag stösst man öfter auf Webapplikationen, die über keine ausreichende Eingabevalidierung verfügen. Auf dem Applikationsserver kann dann via Kontaktformular die ganze Datenbank im Backend beliebig manipuliert werden – mit zum Teil dramatischen Folgen. Eine falsch implementierte vermeintliche Zugriffskontrolle führte in einem konkreten Fall zum Beispiel dazu, dass in einem Onlinebankingsystem individuell angezeigte Anlageempfehlungen gefälscht werden konnten.

Manchmal findet man im Programmcode auch fest codierte Passwörter oder stellt fest, dass Standardpasswörter nicht abgeändert worden sind. Die vorgenannten Lücken wurden glücklicherweise im Rahmen von Application Security Audits entdeckt und behoben, bevor sie von Hackern ausgenutzt werden konnten.

FAZIT: ES LOHNT SICH

Businesskritische Applikationen kosten oft mehrere Hunderttausend Franken an Lizenzgebühren, Entwicklungs- oder Anpassungsarbeiten. Wenn das Unternehmen Opfer einer erfolgreichen Hackerattacke wird, sind die direkten und indirekten monetären Schäden sowie der Imageschaden erheblich. In diesem Kontext lohnt sich die Durchführung eines Application Security Audits bei einem Kostenpunkt von ein paar Tausend Franken allemal – vor allem, weil man damit Schwachstellen aufdeckt, bevor dies ein Unberechtigter tut, die am Projekt beteiligten Personen sensibilisiert sind und man – last but not least – auch der Sorgfaltspflicht nachkommt. ←