Application Security Audits – Stresstest fürs Tafelsilber

Wer den Worten von FBI-Direktor Robert Mueller vom 4. März 2012 Glauben schenken will, muss mit folgender Aussage leben: «Es gibt nur zwei Firmentypen, solche die gehackt wurden, und solche, die es noch werden.» Dieser Artikel zeigt auf, was man tun kann. Christoph Baumgartner, Tobias Gamper

Die zunehmende Anbindung von Geschäftsprozessen ans Internet macht Unternehmen anfällig für Angriffe von ausserhalb ihres Einflussbereichs. Nur wer sich diesem Trend entzieht und damit bewusst Kundenbedürfnisse ignoriert, kann solche Bedrohungen vermeiden. Der Preis dafür ist jedoch hoch. Es gibt beispielsweise keinen Detailhandelskonzern mehr, der auf Onlineshops verzichtet, da deren Produktauswahl oft das Angebot des Ladens um die Ecke übertrifft. Im Gegensatz zu früher geht heutzutage kaum noch jemand auf die Post oder die Bank, um Zahlungen zu tätigen. Shoppen und administrative Aktivitäten lassen sich bequem von zuhause aus oder mithilfe eines mobilen Geräts auch unterwegs erledigen.

Das Prinzip des Onlineshops funktioniert jedoch nur, wenn der ganze Prozess von der Produktpräsentation über den Einkauf bis hin zur Onlinebezahlung in Echtzeit erledigt und die daraus resultierende Bestellverarbeitung zeitnah abgewickelt werden kann. Mangels anderer etablierter Zahlungsalternativen bleibt hier oft nur der Griff zur Kreditkarte oder Postcard. Noch vor gut zwei Jahren hätte keine Bank ernsthaft darüber nachgedacht, Mobile Banking für Smartphones anzubieten – die Sicherheitsbedenken waren zu gross. Heute bleiben zwar die Vorbehalte, aber aufgrund der explosionsartigen Verbreitung von Smartphones, Tablets und Co. sehen sich viele Banken genötigt, diesen Schritt dennoch zu wagen. Somit bestehen immer mehr Interaktionsmöglichkeiten für die Kunden und leider auch für ungebetene Gäste. Im Folgenden werden verschiedene Aspekte von Applikationen sowie geeignete Tests vorgestellt.

Christoph Baumgartner ist CEO und Inhaber der One Consult GmbH. Am Hacking Day 2013 am 16. Mai 2013 bei Digicomp spricht Christoph Baumgartner zusammen mit Dirk Schmidt von Coop in der Keynote über das Thema «IT-Security im Web und Time-to-Market».

Tobias Gamper ist Team Leader Security Audits & Digital Forensics bei der One Consult GmbH.

Designtypen – Mobile Web oder Mobile App

Im Vergleich zum ursprünglichen, reinen Onlineshop, auf den via Browser zugegriffen wird und der beispielsweise aus einem Applikationsserver, dem Datenbankserver im Backend und einer Anbindung an das SAP-System besteht, kommen im mobilen Bereich zusätzliche Technologien zum Zug.

Bei den Mobile Apps unterscheidet man beim Security-Design zwischen Apps, bei denen die Datenhaltung und -verarbeitung auf dem mobilen Gerät erfolgt, wie beispielsweise Games, und Apps, die als reine Terminals im Sinne eines Bilderrahmens agieren und bei denen die ganze Intelligenz auf dem zugehörigen Server verbleibt, wie etwa Onlineshops. Im letzteren Fall kann entweder auf sogenannte Webservices zugegriffen werden, deren Client die zugehörige Mobile App ist, oder es kann alternativ eine für die Bildschirmauflösung des mobilen Geräts optimierte Version der Website, zum Beispiel des Onlineshops, angezeigt werden.

Application Security Audit – systematische Sicherheitskontrolle

Ein Application Security Audit bietet die Möglichkeit, Sicherheitslücken aufzudecken, bevor sie von Unberechtigten ausgenutzt werden können. Er umfasst einerseits sogenannte unprivilegierte Tests, bei denen ohne Kenntnis von gültigen Benutzer-Accounts mehr oder minder systematisch nach Sicherheitslücken im Betriebssystem und in den Basisdiensten gesucht wird. Dies ist auch die klassische Ausgangslage eines Hackers. Zusätzlich werden privilegierte Tests durchgeführt, bei denen mittels gültiger User-IDs, Passwörter und allenfalls weiterer Authentisierungsinformationen und -mechanismen geprüft wird, ob es unter anderem möglich ist, vom Kontext eines Users in den Kontext eines anderen einzudringen – was per se höchstens für den Administrator möglich sein sollte. Ausserdem wird versucht, Administratorrechte auf der Applikation zu erlangen, was selbstredend nicht möglich sein sollte, genauso wenig wie das Auslesen von sensitiven Datensätzen. Diese Aufgabenstellung zeigt, dass man hierbei Tester-Know-how und Kreativität anstatt automatisierte Tool-Power benötigt.

Die unprivilegierten Tests zielen auf die klassischen Sicherheitslücken ab, die meistens auf fehlende Security Patches oder aber Konfigurationsmängel zurückzuführen sind. Diese Lücken werden üblicherweise auch bei Vulnerability Scans (automatisierte Tests ohne Verifikation der Ergebnisse) und Security Scans (automatisierte Tests mit manueller Verifikation der Ergebnisse zwecks Aufdeckung von Falschmeldungen) entdeckt. Diese Tests bilden die Basis für alle gründlichen Application Security Audits. Denn was nützt es, wenn die Applikation perfekt gehärtet, das darunter liegende System aber löchrig wie ein Schweizer Käse ist?

Kritische Bereiche

Die wichtigsten sicherheitsrelevanten Bereiche jeder Applikation und damit die kritischen Angriffspunkte sind die Authentisierung (Identitätsprüfung), die Autorisierung (Zuweisung der zugehörigen Nutzerrechte), die Validierung (primär Blockieren von unerwünschten Eingaben und Integritätssicherung), die Kommunikation sowie die Datenhaltung und -verarbeitung. Bei Multi-Tier-Applikationen können die einzelnen Bereiche auf unterschiedliche Tiers verteilt sein. In solchen Fällen muss sichergestellt werden, dass sich beispielsweise die Authentisierung auf dem mobilen Gerät nicht umgehen lässt, indem direkt mit dem Applikationsserver kommuniziert werden kann.

Testtypen

Viele Web Application Security Audits werden remote via Internet durchgeführt. Somit

können nur die Bereiche getestet werden, die auch via Internet zugänglich sind. Wer eine Applikation jedoch gründlicher untersuchen möchte, kann zusätzlich Tests aus der DMZ oder vom LAN her ausführen und dabei die Firewall so konfigurieren, dass sie den von der IP-Adresse des Testers kommenden Netzwerkverkehr nicht filtert. So kann überprüft werden, wie gut die Applikation vor Angriffen geschützt ist, wenn die Firewall ihren Zweck aus irgendwelchen Gründen nicht erfüllen sollte. Im Weiteren lassen sich die technischen Tests mit einem Code Review ergänzen, der den Fokus auf die vorgenannten Bereiche der Applikation legt. Dies setzt voraus, dass der Tester Zugriff auf den Quellcode erhält. Falls dies nicht möglich ist, kann die Applikation als Blackbox betrachtet und einem Reverse Engineering unterzogen werden (wenn im entsprechenden Land legal, wie etwa in der Schweiz). Bei Multi-Tier-Applikationen bietet sich auch das sogenannte Network Sniffing mit anschliessender Traffic-Analyse an, bei dem der Datenverkehr aufgezeichnet und analysiert wird, um zu erkennen, ob sensitiver Content adäquat geschützt ist.

Bei Shopping- oder Internetbanking-Mobile-Apps sollte der Datenverkehr analysiert werden, weil es in vielen Fällen zu einem regen Datenaustausch zwischen den Mobile Apps und deren Hersteller kommt, was üblicherweise nicht im Sinne des Betreibers und dessen Kunden ist.

Normen und Standards

Da es sich bei den technischen Security Audits um eine relativ junge Disziplin handelt, gibt es bisher noch keinen offiziellen ISO-Standard. Das frei verfügbare «Open Source Security Testing Methodology Manual» (OSSTMM) bietet neben Anleitungen zur Planung, Durchführung und Dokumentation von Security Audits mit dem Risk Assessment Value (kurz RAV) auch die Möglichkeit, das Sicherheitsniveau als neutralen Zahlenwert zu ermitteln. Ausserdem wird das OSSTMM derzeit im ISO-Gremium geprüft, mit dem Ziel, Teil eines zukünftigen ISO-Standards für technische Security Audits zu werden.

Das «Open Web Application Security Project» (OWASP) ist eine Non-Profit-Organisation, die bezweckt, die Sicherheit von Applikationen und Services im WWW zu verbessern. OWASP erarbeitet in verschiedenen Arbeitsgruppen Empfehlungen und Tools. Zwei sehr empfehlenswerte Publikationen sind die «OWASP Top 10» (für Webapplikationen) und die «OWASP Mobile Top 10» für Mobile Apps. Darin werden jeweils die zehn gravierendsten Arten von Schwachstellen beschrieben.

Erfahrungswerte

Aufgrund der Erfahrungen von One Consult aus über 650 technischen Security-Audit-Projekten im In- und Ausland – darunter mehr als 200 Überprüfungen von Webapplikationen wie Onlineshops und Internetbanking-Lösungen sowie Dutzende Tests von Mobile Apps – ergibt sich unter anderem folgendes Bild:

- Bei sämtlichen Audits wurden Schwachstellen gefunden, wobei einige davon lediglich sogenannte Informationsabflüsse betrafen, wie beispielsweise die Offenlegung von Softwarenamen und -version einer Applikation. Dies stellt zwar noch keine gravierende Sicherheitslücke dar, liefert aber einem Angreifer unnötig Informationen, die für einen Angriff ausgenützt werden könnten.
- Generell ist das angetroffene Sicherheitsniveau in der Finanzbranche und bei grossen Onlineshop-Betreibern höher als beispielsweise bei Unternehmen der Fertigungsindustrie. Aber es wurden auch in Internetbanking-Lösungen und Webshops gravierende Sicherheitslücken gefunden, bei denen die Betreiber nur pures Glück hatten, noch nicht Opfer einer erfolgreichen Hackerattacke geworden zu sein.
- Ein Grossteil der Lücken von Webapplikationen und den dazugehörigen Systemen basiert auf einem schlecht gepflegten Basisbetriebssystem. Missstände, die durch zeitnahes Security Patching behoben werden können.
- Mobile Apps leiden oft unter dem «Calling Home Syndrom», indem sie Daten an ihren Hersteller senden; ausserdem speichern sie oft zu viele sensitive Daten auf dem mobilen Gerät.
- Des Weiteren fällt auf, dass Spezialentwicklungen für einen einzigen Kunden tendenziell mehr Sicherheitslücken aufweisen und die Schliessung dieser Lücken mehr Zeit in Anspruch nimmt als bei Software von der Stange.
- Bei Unternehmen, die die Sicherheitsüberprüfung ihrer Applikationen bereits in einer frühen Projektphase planen, werden tendenziell weniger Sicherheitslücken gefunden – die Prozesse scheinen durchwegs einen höheren Maturitätsgrad zu haben.
- Kommerzielle Software im CMS-Bereich weist tendenziell weniger Sicherheitslücken auf als Open Source und deren Schliessung erfolgt zeitnaher. Dies mag daran liegen, dass die Hersteller ein wirtschaftliches Interesse daran haben, ihre Software zu pflegen, um weiterhin Lizenzen zu verkaufen. Bei Open Source ist man auf den Goodwill der Community angewiesen.
- Zu guter Letzt: Leider werden in zirka einem Drittel der Projekte bei der nächsten Durchführung wieder die alt bekannten Sicherheitslücken gefunden. Dies spricht nicht gerade für ein funktionierendes Patch Management.

Generelle Empfehlungen

Wer proaktiv agieren will, führt bereits in der Konzeptionsphase der Applikation einen Design- oder Architektur-Review durch, um Schwachstellen bereits auf dem Papier zu erkennen, bevor eine einzige Zeile Code geschrieben wurde. Wie bei allen Projekten bringt Management Attention auch bei Security Audits das Projekt weiter – nicht zuletzt in Bezug auf eine konsequente Massnahmenpriorisierung und darauffolgende Schliessung der detektierten Sicherheitslücken. Idealerweise werden Security Audits auf einer der produktiven Infrastruktur möglichst nahen Umgebung durchgeführt. Selbstredend sollten Application Security Audits ein fester Bestandteil der Projektplanung sein und mögliche externe Security Auditoren frühzeitig avisiert werden. Durch die Wahl des richtigen Partners wird auch sichergestellt, dass es sich um ein gemeinsames Projekt handelt, mit dem Ziel, das angestrebte Sicherheitsniveau zu gewährleisten und Fingerpointing zu vermeiden. Bei zu vielen negativen Befunden gilt es auch abzuwägen, ob der Launch einer Applikation verschoben werden soll, anstatt die negative Medienpräsenz aufgrund einer Hackerattacke zu riskieren. Selbst wenn nur wenige Sicherheitsmängel gefunden werden, wird die Security Awareness der am Projekt beteiligten Personen in jedem Fall gesteigert.

Fazit

Application Security Audits zeigen Sicherheitslücken auf und erlauben deren Schliessung, bevor Hacker diese ausnutzen. Nur wer den Kopf in den Sand steckt, knirscht irgendwann mit den Zähnen und gibt Robert Mueller Recht. <

VERANSTALTUNG

Am 16. Mai findet der «Hacking Day 2013 – Security Lifecycle» statt. Laden Sie sich die Präsentationen des Tages rund um Hacking auf der Digicomp-Website herunter: www.digicomp.ch/hackingday