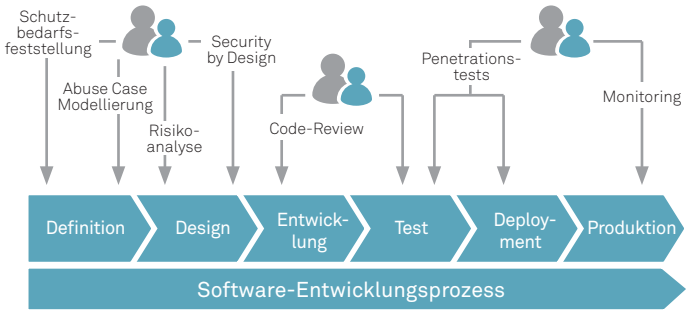
Application Security

Das richtige Maß an Sicherheit für Anwendungen ist unabdingbar

Immer mehr Geschäftsprozesse werden durch IT unterstützt oder ins Internet verlagert. Gerade in kritischen Bereichen und Prozessen ist die Sicherheit der zu Grunde liegenden Applikationen extrem wichtig. Application Security wird daher immer wichtiger und sollte ein fester Bestandteil jeder Anwendungsentwicklung sein.

Definition

Im engeren Sinn wird unter Application Security meist die Code-Sicherheit einer bestimmten Anwendung sowie die Robustheit gegen Angriffe verstanden. Eine darüber hinausgehende Betrachtung subsummiert unter Application Security alle Sicherheitsmaßnahmen, die im Lebenszyklus einer Applikation sinnvollerweise durchgeführt werden. Dies impliziert nicht nur Penetrationstests oder Security-Sourcecode-Reviews, sondern alle Sicherheitsaktivitäten im Software Development Lifecycle – angefangen bei der Schutzbedarfsfeststellung, über „Security by Design" bis hin zu Sicherheitsprüfungen (siehe Abbildung rechts). Das vorliegende Dossier orientiert sich an der umfassenderen Betrachtung.



Web Application Security
- Breite Angriffsfläche (Internet)
- Security by Design
- Schwachstellen in der Applikation (Authentisierung, Autorisierung, SQL-Injection, XSS, uvm.

Infrastructure Security
- Patch Management
- Hardening von Server-Systemen
- Identity Management System
- Betriebsprozesse
- Client Security

Application Security

Security Management
- Management Unterstützung
- Security Development Lifecycle
- Etablierung von Prozessen
- Kontrolle und Monitoring
- Datenschutz-Anforderungen

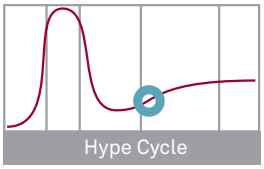
Mobile Security
- Programmierung sicherer Apps
- Angriffspotenzial Luftschnittstelle
- Verschlüsselte Übertragung
- Gerätesicherheit (Schutz vor Verlust und Diebstahl)

Neben einem sicheren Sourcecode ist implizit auch die Sicherheit des Gesamtpakets „Benutzer + Daten + Applikation + Infrastruktur" herzustellen. Dies zeigt, wie vielschichtig und weitreichend sich entsprechende Sicherheitsaktivitäten darstellen. Letztendlich besteht die Herausforderung darin, ein angemessenes und wirksames Sicherheitsniveau zu erreichen ohne dem – in realen Projekten üblichen – Kostendruck zum Opfer zu fallen.

Welche und wie viele Sicherheitsmaßnahmen sinnvoll bzw. angemessen sind, ermittelt man in einer initialen Schutzbedarfsfeststellung zu Projektbeginn. Die Umsetzung der relevanten Maßnahmen wird über den gesamten Software-Entwicklungsprozess verfolgt.

Reifegrad

Application Security ist kein Trendthema, sondern gehört seit langem zu den Kerndisziplinen in der Softwareentwicklung. Viele Unternehmen sehen es heute als essentiell an, um monetäre und Image-Schäden abzuwenden. Allerdings wird die Notwendigkeit von angemessener Sicherheit auch noch oft unterschätzt. Die Verbreitung muss und wird daher zunehmen und sich weiter im Entwicklungsprozess etablieren.



Marktübersicht

Der Kern von Application Security sind Methoden, die häufig durch Tools unterstützt werden.

Alternativen

Alternativen zu Application Security sind auf den ersten Blick nur schwer vorstellbar. Allenfalls die Behandlung von identifizierten Risiken kann – je nach Situation – in unterschiedlicher Art erfolgen: Hier kann in Einzelfällen auch eine Übertragung von Risiken (Versicherung, Verträge) oder auch eine Restrisikoakzeptanz sinnvoll sein. Besteht beispielsweise bei Webapplikationen keine Möglichkeit, diese selbst sicherer zu machen, kann man alternativ eine Web Application Firewall (WAF) vorschalten.

Referenzszenario

Bewährte Vorgehensweisen sind beispielsweise in msg.PROFI, im Security Development Lifecycle (SDL) oder in den Grundschutz-Katalogen des BSI (Bundesamt für Sicherheit in der Informationstechnik) nachzulesen.

Bei angespanntem Budget sollte zumindest eine „Baseline-Security“ etabliert werden. Hierzu ist zunächst eine initiale Bewertung von Schutzzielen und Schutzbedarf erforderlich. Im zweiten Schritt werden zwischen Projektleiter und Sicherheitsberater oder -beauftragten die minimal erforderlichen Sicherheitsmaßnahmen abgestimmt.

Business Impact

Durch eine angemessene Application Security können Risiken abgewendet oder zumindest reduziert werden. Dies gilt vor allem für Produkt- und Individualentwicklungen, aber auch für gekaufte oder übernommene Software und Applikationen.

In der Außendarstellung (Marketing, Vertrieb) können durch Positionierung des Themas Security durchaus Wettbewerbsvorteile erzielt werden. Oftmals wird in Projekten und Ausschreibungen nicht explizit auf Sicherheit eingegangen. Nicht selten herrscht aber seitens des Auftraggebers eine implizite, hohe Erwartungshaltung und Notwendigkeit. Folglich sollten die vorgesehenen Sicherheitsmaßnahmen explizit benannt und geplant werden.

Pro	Contra
Reduktion von Risiken für Daten und Geschäftsprozesse	Application Security kostet Zeit und Geld und ist nicht „Gott gegeben“
Compliance zu gesetzlichen Regelungen und damit Ausschluss von Haftungsrisiken	Spezielles und sich ständig änderndes Know-how erforderlich (Cybercrime)
Sicherstellung der Konkurrenzfähigkeit am Markt („State-of-the-art“)	100%ige Sicherheit kann nie erreicht werden, wenn der Angreifer ausreichend motiviert ist
	Schwer messbarer ROI (Imageschäden, Kundenzufriedenheit, etc.)

msg systems ag
Robert-Bürkle-Straße 1 | 85737 Ismaning/München
Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113
www.msg-systems.com | info@msg-systems.com

Stand: September 2012
http://www.msg-systems.com/techrefresh
XT-120-1209-1