

Toni Gansel (*Sogeti*)

Security - Jetzt erst recht

ASQF
Arbeitskreis Software-Qualität
und -Fortschreibung e.V.

Mehr Qualität mit Software-Projekt-Management

Motivation:
Das L.U.S.T.-Prinzip
Seite 12

Agilität:
(Projekt-)Management in Bewegung setzen
Seite 16

Im Gespräch:
mit Norbert Kastner
Seite 18



Sogeti Deutschland GmbH
Wanheimer Straße 68
40468 Düsseldorf
TEL +49 (0)211 5661-4000
FAX +49 (0)211 5661-4100

kontakt@sogeti.de
www.sogeti.de

Y
O
U
R
D
E
R
N
S

Security – Jetzt erst recht

Toni Gansel

Telegrafen, Telefone, Handys, Smartphones: Mobile Devices! Die Funktionen dieser Geräte sind nicht mehr auf einfache Kommunikation beschränkt. Fitnesstracking, Kartendienste, unterschiedliche Verwaltungstools und eine starke Integration in fast jedes soziale Netzwerk sind Standard-Funktionen, die jedes Smartphone beherrscht. Tablets sind dabei, PCs zu verdrängen, Smartwatches und Wearables sind Vorboten neuer fundamentaler Änderungen in unserem alltäglichen Leben. Diese Geräte unterstützen uns dabei, einfach und günstig zu kommunizieren. Informationen sind für jeden zugänglich – unabhängig von Zeit und Ort. Sie helfen uns dabei, unser Arbeits- und Privatleben zu organisieren, unterhalten uns und wissen immer den richtigen Weg. Mit ihnen können wir jederzeit Fotos schießen und unsere Lieblingslieder hören. Sie unterstützen und verbessern uns: Deus ex machina! Diese neuen Technologien haben neue Märkte erschaffen, deren Gesamtumsatz äußerst schwer zu schätzen ist. Sie berühren nahezu jeden existierenden Markt: Apple ist aufgrund des iPhones das wertvollste Unternehmen der Welt. Videospielehersteller haben eine nie dagewesene Reichweite für ihre Produkte. Automobil- und Kleidungshersteller verbessern ihre Produkte mit neuen Sensoren und Apps.

Jeden Tag werden neue Lösungen entwickelt, die sowohl alte als auch neue Probleme lösen. Auch der Bereich der Cyberkriminalität hat sich an die neuen Technologien angepasst und einen neuen Höhepunkt erreicht. Der Softwarehersteller McAfee schätzt,



dass die Kosten für Cybercrime in Deutschland 1,6 Prozent des Bruttonzialprodukts betragen. Weltweit sollen es rund 575 Milliarden Dollar sein. Der Telekommunikationskonzern Verizon berichtet von 63.437 IT-Sicherheitsvorfällen im Jahr 2014, die Anzahl der Zero-Day-Exploits sei im vergangenen Jahr um 64 Prozent gestiegen. Diese Zahlen sind alarmierend und sie steigen weiter.

Selbst wenn wir heute noch nicht sagen können, welche Daten für die Nutzer, die Regierung oder die Unternehmen bestimmt sind, wissen wir, dass Informationen wertvoll und schützenswert sind. Um einen stärkeren Schutz zu erreichen, entwickeln

die Regierungen Rahmenbedingungen; diverse Institutionen schaffen technische Standards und Unternehmen starten Initiativen, um auf unterschiedliche Weise das Vertrauen ihrer Kunden zu gewinnen.

Was muss man beachten, wenn man sichere Apps entwickeln will? Wo fängt Sicherheit an und wo hört sie auf? Häufig sind sehr grundsätzliche Probleme gar nicht adressiert und simple Lösungen werden nicht genutzt. Hier ist eine kleine Hilfestellung.

Design und Usability

Wenn man mit einem modernen Auto losfährt ohne angeschnallt zu sein,

wird das Auto anfangen zu piepen. Es ist ein nervendes Piepen, es ist klar was das Auto will: „Schnall Dich an!“ Bei diesem Verhalten wird ganz bewusst auf Usability verzichtet, um die Sicherheit der Autoinsassen zu erhöhen.

Schon beim Entwurf von App Software stellen sich sehr grundsätzliche Fragen, die die IT-Sicherheit des betreffenden Produktes wesentlich beeinflussen. Bei einem Instant-Messenger könnte man beispielsweise fragen: „Ist es wirklich notwendig, die Kommunikation endlos zu protokollieren, oder reicht es, wenn die Nachrichten nur innerhalb eines bestimmten Zeitraumes abrufbar sind?“.

Wenn man den Benutzern die Möglichkeit bietet Inhalte zu kommentieren, ist es meistens sinnvoll, anonyme Kommentare anzubieten. Generell sollte genau geprüft werden, welche Benutzerdaten erhoben werden müssen und welche Berechtigungen eine App auf einem Smartphone benötigt. Braucht ein QR-Code-Scanner wirklich Zugriff auf die Kontakte?

Des Weiteren sollten die Standardeinstellungen einer App auf die maximale Sicherheit zielen. Nicht jede dieser Einstellung muss änderbar sein. Falls doch, sollte der Benutzer über die Risiken aufgeklärt werden. Hier kann man gut von Apple lernen. Stichwort: Security by default.

Typische Fehler vermeiden

In den „OWASP Top 10 Mobile Risks“ sind die häufigsten Sicherheits-Probleme von Mobile Apps beschrieben, dort werden auch passende Lösungen angeboten. Probleme wie Client-Side-Injections, Poor-Authorization and Authentication und Weak-Server-Side-Controls sind auch nicht Mobile-spezifisch. Diese Probleme

sind schon seit Jahren sehr zentrale Sicherheitslücken in der Software und sie werden immer wieder ausgenutzt.

Es gibt zahlreiche Testdienstleister, die eine App günstig hierauf prüfen können. Hier sollte man das Geld in die Hand nehmen und diese Tests durchführen lassen. Es ist nicht teuer, bringt aber sehr viel. Diese Tests nicht durchzuführen, kann sehr viel teurer werden und wäre verantwortungslos.

Sichere IT-Infrastruktur schaffen

Eine sichere App betrifft nicht nur das Endprodukt, sondern auch die Infrastruktur im Unternehmen. Es ist sicherzustellen, dass die Software in einer sicheren Umgebung entwickelt wird. Hier bietet das BSI mit dem IT-Grundschutz eine starke, staatlich anerkannte Basis. Diese konkurriert mit vielen branchenspezifischen Standards. Es gibt hier zahlreiche etablierte Standards, die dabei helfen, Sicherheit und Vertrauen zu schaffen – man muss nur einen wählen.

Ebenso wichtig, ist die Frage, wie mit Sicherheitslücken umgegangen wird, wenn welche bekannt werden. Ein Security-Response-Prozess wird benötigt. In diesem ist beschrieben, wie die Sicherheitslücken kommuniziert und Patches ausgeliefert werden. Man sollte davon ausgehen, dass Schwachstellen auftreten werden. Dies wird erst dann zu einem Problem, wenn man schlecht reagiert.

Fazit

Im Informationszeitalter ist der Schutz sensibler Daten wichtiger als er je zuvor war. Dies betrifft Unternehmensdaten genauso wie die Daten für und von den Endbenutzern. Sicherheit herzustellen ist kein Zauberwerk, es ist mit einfachen Mitteln möglich. Es ist

kein Feature, sondern eine zwingende Anforderung an jedes Unternehmen, welches mit IT arbeitet. Besonders, wenn das Unternehmen Apps entwickelt und Benutzerdaten erhebt.

Unternehmen wie Volvo haben bereits gezeigt, dass Sicherheit eine Marketingstrategie ist, Microsoft hat dies auf die harte Tour gelernt. Apple, Google und Facebook versprechen, die Anstrengungen in diese Richtung zu erhöhen. Datenschutz und IT-Sicherheit sind adressiert, forciert und gefordert. Es wäre wünschenswert, wenn Nutzer bald sagen könnten: „Meine Daten sind sicher.“ ■



Toni Gansel ist Mobile Security-Experte bei Sogeti. Er hat mehrere Jahre unterschiedliche Unternehmen dabei unterstützt, Software-Lösungen zu entwickeln und deren Qualität zu erhöhen.

Sogeti ist spezialisiert auf innovative, geschäftlich getriebene Qualitätssicherungs- und Testdienstleistungen und ist größter Testdienstleister in Europa und den USA. Wir unterstützen unsere Kunden dabei, aus ihren IT-Systemen den bestmöglichen geschäftlichen Nutzen zu ziehen. Unsere Kunden profitieren von den messbaren Ergebnissen unserer kosteneffizienten kosteneffiziente Onshore-, Nearshore und Offshore Testlösungen: Managed Testing Services, TMap®-basiertes Projekt- und Programmtesten und TPI® (Test Process Improvement). Unser Expertenwissen drückt sich in den durch uns entwickelten QSMethoden TMap® und TPI® aus, die praxisorientiert und im Markt international anerkannt sind. Hierzu wird von Sogeti Fachliteratur veröffentlicht. Zur Vorbereitung auf Zertifizierungstests bietet Sogeti sowohl standardisierte als auch maßgeschneiderte Trainings an.

Sogeti ist ein führender Anbieter professioneller Technologiedienstleistungen, spezialisiert auf Applikationsmanagement, Infrastrukturmanagement, High-Tech-Entwicklung und Testen von Software. Die enge Zusammenarbeit mit seinen Kunden befähigt Sogeti, diese technologische Innovation effektiv einzusetzen und höchste Ergebnisse zu erreichen. Sogeti bringt mehr als 20.000 IT-Professionals in 15 Ländern zusammen und ist an über 100 Standorten in Europa, den USA und Indien vertreten. Sogeti ist eine hundertprozentige Tochter von Capgemini und an der Pariser Börse notiert.

TMap®, TMap NEXT®, TPI® und TPI NEXT® sind eingetragene Warenzeichen der Sogeti Nederland B.V.

Für weitere Fragen stehen wir Ihnen unter der angegebenen Rufnummer bzw. unter der E-Mail-Adresse kontakt@sogeti.de zur Verfügung.

Kontakt

Sogeti Deutschland GmbH
Wanheimer Str. 68
40468 Düsseldorf
Tel.: +49 (0)211 5661-4000



kontakt@sogeti.de
www.sogeti.de

