Berliner Hochschule für Technik

Fachbereich VI - Informatik und Medien
Studiengang IT-Sicherheit Online / Medieninformatik

Vertiefung 2

PARETO CONSULTING

Modul: Sicherheitsmanagement

Dozent: Sven Zehl

vorgelegt von: Gruppe 1
Christine Kuczera
Dirk Drutschmann
Hicham Naoufal
Michael Schröter
Jan Zimmermann
Ivo Valls

Aufgabe 1) Erläutern Sie die Qualitätskriterien für Software. Wo finden sich hier Betriebssicherheit und wo Datensicherheit?

Antwort

Nach ISO/IEC 25010 zeichnet sich qualititiv hochwertige Software durch folgende acht Kriterien aus: [^1]

Wartbarkeit

Software sollte immer modular aufgebaut, wiederverwendbar,analysierbar und testbar sein, v.a. aber anpassbar.

Funktionalität

Die funktionale Vollständigkeit, Korrektheit und Angemessenheit der Software unverzichtbar.

Performance

Das jeweilige Zeitverhalten, die Ressourcennutzung und Kapazität der Software sind wichtige Bestandteile.

Kompatibilität

Um das Zusammenspiel mit anderen Software-Komponenten zu gewährleisten, sollte Wert auf Koexistenz und Interoperabilität gelegt werden.

Usabitlity

Hier spielen mehrere Faktoren eine Rolle, neben einer guten Bedienbarkeit und Erlernbarkeit auch vermeintlich “softe” Faktoren wie die Ästhetik der Benutzeroberfläche.

Zuverlässigkeit

Ein wichtiger Bestandteil ist die Verlässlichkeit der Software, die Verfügbarkeit, Fehlertoleranz und Wiederherstellbarkeit gewährleistet.

Sicherheit

Software sollte immer den höchsten Ansprüchen an Datenschutz, Integrität und Sicherheit genügen.

Portabilität

Software sollte immer den höchsten Ansprüchen an Datenschutz, Integrität und Sicherheit genügen.

Betriebssicherheit ist ein Submerkmal des Qualitätsmerkmals Zuverlässigkeit

Die Betriebssicherheit ist ein Qualitätskriterium, das sich auf die Fähigkeit einer Software bezieht, unter normalen Betriebsbedingungen stabil und zuverlässig zu funktionieren. Zu den Faktoren, die die Betriebssicherheit beeinflussen können, gehören die Stabilität der Plattform, auf der die Software ausgeführt wird, sowie die Fähigkeit der Software, auf unerwartete Situationen zu reagieren, wie z. B. Netzwerkfehler oder fehlerhafte Eingaben.

Datensicherheit ist als Submerkmal des Qualitätsmerkmals Sicherheit

Die Datensicherheit ist ein weiteres wichtiges Qualitätskriterium, das sich auf den Schutz von Daten bezieht, die von der Software verarbeitet werden. Dies kann den Schutz vor unerlaubtem Zugriff auf sensible Daten, die Integrität der Daten und die Vertraulichkeit der Daten umfassen. Zu den Faktoren, die die Datensicherheit beeinflussen können, gehören die Implementierung von Verschlüsselungstechnologien, die Durchführung von Sicherheitsaudits und das Vermeiden von Schwachstellen in der Software, die Angreifern Zugriff auf Daten ermöglichen könnten.

Aufgabe 2) Wo in der Software-Produktion treten Safety- und wo Security-Fehler auf? Orientieren Sie sich am SDL.

Antwort

Safety-Fehler können in der Regel während des gesamten Software-Entwicklungslebenszyklus (SDLC) auftreten, aber insbesondere in den Phasen der Anforderungsanalyse, Architekturdesign, Implementierung und Tests. Hier sind einige Beispiele für potenzielle Safety-Fehler in jeder Phase:

-Anforderungsanalyse (*Phase One*): Fehlerhafte oder unvollständige Anforderungen können zu Fehlern bei der Umsetzung von Sicherheitsanforderungen führen, z.B. wenn bestimmte Szenarien nicht berücksichtigt werden. -Architekturdesign (*Phase Two*): Sicherheitsrelevante Entscheidungen im Design können Fehler verursachen, z.B. wenn Schwachstellen bei der Datenverarbeitung oder bei der Authentifizierung und Autorisierung eingebaut werden. -Implementierung (*Phase Three*): Fehler bei der Implementierung können zu unsicheren Codierungspraktiken führen, die die Sicherheit beeinträchtigen können, z.B. wenn keine ausreichenden Validierungen für Eingaben durchgeführt werden. -Tests: Unzureichende Tests können Sicherheitslücken aufdecken oder übersehen, was zu einer schlechteren Qualität und einer höheren Unsicherheit führt.

Security-Fehler treten typischerweise auf, wenn die Sicherheit nicht richtig in die SDLC integriert wird oder wenn sich Sicherheitsprobleme im Code einschleichen, der durch den Entwicklungsprozess geht. Der Security Development Lifecycle (SDL) ist ein Entwicklungsansatz, der sich auf die Integration von Sicherheit in den gesamten Software-Entwicklungslebenszyklus konzentriert, um sicherzustellen, dass Software sicher entwickelt wird. Hier sind einige Beispiele für potenzielle Security-Fehler in jeder Phase des SDL:

-Planungs- und Anforderungsphase *(*Phase One*): Es können Sicherheitsanforderungen übersehen werden, wenn sie nicht explizit berücksichtigt werden. -Designphase (*Phase Two*): Es können Designentscheidungen getroffen werden, die die Sicherheit beeinträchtigen, z.B. wenn Sicherheitsfunktionen nicht ausreichend berücksichtigt werden. -Implementierungsphase (*Phase Three*): Es können Schwachstellen im Code eingebaut werden, z.B. wenn keine sichere Codierungspraktiken angewendet werden. -Testphase (*Phase Four*): Unzureichende Tests können Sicherheitslücken aufdecken oder übersehen, was zu einer schlechteren Qualität und einer höheren Unsicherheit führt. -Bereitstellungs- und Wartungsphase (*Phase Five*): Es können Sicherheitsprobleme entstehen, wenn Sicherheitsanforderungen nicht berücksichtigt oder aktualisiert werden, z.B. wenn veraltete Software verwendet wird. [^2]

Aufgabe 3) Charakterisieren Sie die Produktpflege eines typischen Herstellers. Warum ist es nicht einfach, die Kernmodule zu überarbeiten?

Antwort

Die Produktpflege ist ein wesentlicher Bestandteil des Software-Entwicklungsprozesses und bezieht sich auf die Aktivitäten, die erforderlich sind, um ein Produkt nach dessen Veröffentlichung auf dem Markt zu warten, zu aktualisieren und zu verbessern. Ein typischer Hersteller pflegt ein Produkt in der Regel, um folgende Ziele zu erreichen:

-Behebung von Fehlern und Sicherheitslücken: Produktpflege beinhaltet die regelmäßige Überprüfung und Korrektur von Fehlern und Schwachstellen im Produkt, um sicherzustellen, dass es sicher und zuverlässig bleibt. -Aktualisierung und Verbesserung: Die Produktpflege umfasst auch die Integration neuer Funktionen und Verbesserungen, um das Produkt auf dem neuesten Stand der Technik zu halten und den Kundenanforderungen gerecht zu werden. -Unterstützung: Produktpflege umfasst auch den technischen Support und die Kundenbetreuung, um sicherzustellen, dass Kunden bei Fragen oder Problemen Unterstützung erhalten.

Es ist nicht einfach, die Kernmodule zu überarbeiten, weil diese Module in der Regel tief in die Architektur und den Code des Produkts integriert sind. Änderungen an diesen Kernmodulen können zu Auswirkungen auf andere Module und auf die Gesamtfunktionalität des Produkts führen. Daher erfordert die Überarbeitung von Kernmodulen oft eine umfassende Analyse und Planung, um sicherzustellen, dass Änderungen ordnungsgemäß umgesetzt und getestet werden, um mögliche negative Auswirkungen auf das Produkt zu minimieren.

Darüber hinaus können Änderungen an Kernmodulen auch eine umfassende Neuzertifizierung oder Validierung des Produkts erforderlich machen, um sicherzustellen, dass es den geltenden Vorschriften und Standards entspricht. Dies kann zu zusätzlichen Kosten und Zeitverzögerungen führen.

Zusammenfassend lässt sich sagen, dass die Produktpflege eine wichtige Aufgabe für Hersteller ist, um die Qualität und Zuverlässigkeit ihrer Produkte sicherzustellen und den Kundenbedürfnissen gerecht zu werden. Die Überarbeitung von Kernmodulen erfordert jedoch eine sorgfältige Analyse und Planung, um potenzielle Auswirkungen auf das Gesamtsystem zu minimieren.

Aufgabe 4) Überarbeiten Sie Ihre Dokumentation des Rollenspiels Kosten der Sicherheit: Was würden Sie nun anders formulieren?

Siehe: https://hetzlefetz.github.io/uni-sicherheitsmanagement/chat/dist/index.html

Aufgabe 5) Vertiefen Sie die Auflistung der zu erwartenden Gefährdung Ihres Use Cases hinsichtlich Geschäftsmodell, Asset, Bedrohung und Einsatzumgebung.

Antwort aus Vertiefung 1b Aufgabe c)

- Branche, Zielgruppe: Kunsthandel, (Wohlabende) Gehobene Klientel
- Mitarbeiterzahl: KMU, ~ 50 Mitarbeiter
- Umsatz: Mehrere hundert Mio €
- Anzahl und mittlerer Preis jährlich verkaufter Produkte: 5-100 Gemälde/Gegenstände, weltweit.

Mögliche Risiken:

- Entwendung der Kundenliste
- Nichtdurchfürbarkeit der Auktion
- Defacement der Seite

Mögliche Angreifer:

- Konkurrenten könnten versuchen Kunden abzugraben.
- Finanzamt könnte versuchen Kundendaten einzusehen.
- Bei umstrittener Kunst könnten Aktivisten versuchen die Seite unbenutzbar zu machen.

Vertiefung

Geschäftsmodell

-Entwendung der Kundenliste: Der Diebstahl der Kundenliste kann zu einem erheblichen Verlust des Geschäftsmodells führen, da diese Kunden in dieser Branche oft Wiederholungskäufer sind. Auch könnte die Konkurrenz diese Liste nutzen, um Kunden abzuwerben oder den Ruf des Unternehmens schaden. -Nichtdurchführbarkeit der Auktion: Wenn die Auktion nicht wie geplant stattfinden kann, werden wertvolle Verkaufschancen verloren gehen, was sich direkt auf den Umsatz und die Reputsation auswirkt. -Defacement der Seite: Ein Angriff auf die Website, der zu einer Änderung oder Beschädigung der Website führt, kann das Vertrauen der Kunden beeinträchtigen und zu einem erheblichen Verlust von Kunden und Einkommen führen.

Asset

-Kundenliste: Die Kundenliste ist ein wichtiges Asset des Kunsthandels, da sie eine Liste von wertvollen Kunden enthält, die potenzielle Käufer von Kunstwerken sein könnten. -Auktionsplattform: Die Auktionsplattform ist ein wichtiges Asset, da sie die primäre Verkaufsplattform für die Kunstwerke ist - interesant für Kunden, die nicht das lokale Geschäft aufsuchen können. -Webseite: Die Webseite ist ein wichtiges Asset, da sie das Unternehmen repräsentiert und als primäre Informationsquelle für Kunden dient.

Bedrohung

-Konkurrenten: Konkurrenten könnten versuchen, Kunden abzuwerben, indem sie auf Informationen zugreifen, die sie nicht haben sollten. Darüber hinaus könnten sie gezielte Werbeaktionen durchführen, um Kunden abzuwerben. -Finanzamt: Das Finanzamt könnte versuchen, auf die Kundenliste zuzugreifen, um z.B. Informationen über Steuerzahlungen und ähnliches zu erhalten. -Aktivisten: Aktivisten, die sich gegen umstrittene Kunstwerke aussprechen, könnten versuchen, die Website unbenutzbar zu machen, um ihren Standpunkt zu verdeutlichen.

Einsatzumgebung

-Gehobene Klientel: Die Zielgruppe des Kunsthandels ist eine gehobene Klientel, die hohe Erwartungen an den Service und die Qualität haben. Ein Verlust des Vertrauens kann erhebliche Auswirkungen auf das Geschäft haben, in diesen Kreisen ist der Ruf einer Unternehmung bedeutsam und wird schnell über Mundpropaganda verbreitet. -Weltweit: Der Kunsthandel findet weltweit statt, was bedeutet, dass das Unternehmen mit verschiedenen gesetzlichen Vorschriften, Sprachbarrieren und kulturellen Unterschieden konfrontiert sein kann.

Quellen

^1: An ISO 25010 Based Quality Model for ERP Systems, Emmanuel Peters, George Kwamina Aggrey ^2: Security Development Lifecycle, Michael Kranawetter