

Dokumentation Freigabeverfahren

E-Mail Marketing Manager - Emma

Programmversion: 3.5

Stand: Dezember 2016

arxes-tolina GmbH
Siemensdamm 62
13627 Berlin
Tel.: +49(30)264745-0
vertrieb@arxes-tolina.de

1. Kompetenz

Das Freigabeverfahren wurde durch uns, die Firma arxes-tolina GmbH durchgeführt. Unter der Marke tolina entwickeln wir seit vielen Jahren erfolgreich Softwareprodukte für Banken und Sparkassen. Diese Produkte werden einem Freigabeverfahren nach OPDV unterzogen, woraus eine weitreichende Erfahrung in der Qualitätssicherung von Softwareprodukten resultiert, die in das vorliegende Freigabeverfahren eingeflossen ist.

2. Testobjekt

Gegenstand der Programmfreigabe ist die von der Sparkassen Finanz-Portal GmbH angebotene Online-Anwendung E-Mail Marketing Manager, Emma. Die Anwendung basiert auf der E-Mail Marketing Lösung der Firma mailingwork GmbH

3. Testumgebung

Die Tests wurden innerhalb der produktiven Online-Anwendung mit Hilfe eines Test-Zugangs vorgenommen.

4. Risikobewertung

Bei dem Programm Emma handelt es sich um Anwendung zur Unterstützung des Marketings und damit nicht um eine bankfachliche Anwendung im engeren Sinne.

Bei der Risikobewertung wird davon ausgegangen, dass die Entwicklung des Programms mit berufsmäßiger Sorgfalt erfolgte.

Die Schutzbedarfsfeststellung hat das Ziel, die Anforderungen hinsichtlich der Grundwerte der Informationssicherheit (Verfügbarkeit, Vertraulichkeit und Integrität) zu identifizieren und zu dokumentieren.

Vertraulichkeit

In dem Programm werden kundenbezogene Daten verarbeitet. Dies sind insbesondere Benutzerprofile mit Namen, Geburtsdaten, Firmenzugehörigkeit und E-Mail-Adressen und die Zuordnung zu Abonnentenlisten, Zielgruppen und Interessen.

Ein möglicher Missbrauch personenbezogener Daten hätte nur geringfügige Auswirkungen für den Betroffenen. Der Schutzbedarf wird daher als normal eingestuft.

Integrität

Eine absichtliche oder unabsichtliche ungerechtfertigte Modifikation der Abonentendaten würde dazu führen, dass ein Kunde oder Interessent keine oder nicht passende oder ungewollte Informationen erhalten würde. Davon wären nur geringe Ansehens- oder Vertrauensbeeinträchtigung zu erwarten.

Höher zu bewerten wäre ein möglicher Imageverlust, falls über das E-Mail Marketing Programm falsche oder Imageschädigende Inhalte verbreitet werden. Denkbar wären z.B. auch Phishing-Aktionen, wo die Abonnenten über offiziell erscheinende E-Mails zur Preisgabe von vertraulichen Daten aufgefordert werden. Der Schutzbedarf hinsichtlich der Integrität lässt sich daher als hoch einstufen.

Verfügbarkeit

Die Anwendung wird nicht als zeitkritisch eingeschätzt. Eine Beeinträchtigung würde von allen Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit des IT-Systems beträgt mehr als 48 Stunden.

Bei Nicht-Verfügbarkeit wäre eine geringe, bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung zu erwarten. Der Schutzbedarf wird daher als normal eingestuft.

Es sind damit insgesamt die Voraussetzungen für die Einstufung mit hohem Schutzbedarf gegeben.

5. Testverfahren

Mit der aktuellen Fassung der Stellungnahme 1/2015 des Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung (OPDV) wird die Verwendung von „Standards und Anforderungen an die Qualitätssicherung“ nahegelegt.

Die vorgenommenen Tests orientieren sich an der Normenreihe DIN ISO/IEC 250xx „Software-Engineering – Qualitätskriterien und Bewertung von Softwareprodukten (SQuaRE)“. Es wurden insbesondere die folgenden Qualitätskriterien untersucht: **Richtigkeit, Bedienbarkeit, Sicherheit, Reife, Stabilität und Verständlichkeit.**

Die folgenden Tests und Beurteilungen wurden dafür genutzt:

Testverfahren	Beschreibung
Funktionaltests	• Durchführung von Tests zu fachlichen Abläufen
Sicherheitstest	• Prüfung der gesicherten Verbindung (https) und der zugehörigen Zertifikate. • Beurteilung der IT-Sicherheit und der Maßnahmen zum Datenschutz.
Bedienbarkeitstest Oberflächentest	• Test der Bedienbarkeit und Funktionsfähigkeit der Benutzeroberfläche
Dokumentationstest	• Test auf Übereinstimmung von Dokumentation und Programm
Robustheitstests	• Test auf Falscheingaben, Abbruch von Arbeitsschritten, nachträgliche Korrekturen usw.

Die Erfüllung der Anforderungen zur Betrachtung der aufgeführten Qualitätskriterien durch die Testverfahren wird bestätigt.

Aufgrund der Risikobewertung wird ein Schwerpunkt auf die Beurteilung der IT-Sicherheit gelegt.

6. Testdokumentation

Die durchgeführten Funktionaltests wurden im Rahmen der OPDV-Programmfreigabe dokumentiert.

Die Ergebnisse aller durchgeführten Tests und Beurteilungen sind in einem separaten Dokument „02 Testergebnisse“ zusammengefasst worden.

7. Ausblick

Die Anwendung wird fortlaufend weiterentwickelt.

Der Hersteller der Software-Lösung stellt eine detaillierte Änderungs-Historie bereit, anhand derer klar nachvollziehbar ist, welche Änderungen vorgenommen wurden. Für die Beurteilung künftiger Versionen kann diese Änderungs-Historie herangezogen werden. Je nach Art und Umfang der Änderungen kann die Software auch ohne erneute Freigabe weiter eingesetzt werden. Wir empfehlen jedoch eine erneute Programm-Freigabe bei größeren Änderungen oder nach einem längeren Zeitraum vorzunehmen.