



OPS.1.1: Kern-IT-Betrieb / Kernaufgaben

OPS.1.1.6: Software-Tests und -Freigaben

1 Beschreibung

1.1 Einleitung

Der Einsatz von IT in Institutionen setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei funktioniert, da die Einzelergebnisse in den meisten Fällen nicht mehr kontrolliert werden können. Deswegen muss Software jeglicher Art schon vor Inbetriebnahme im Rahmen von Software-Tests überprüft werden. In diesen Tests muss nachgewiesen werden, dass die Software die erforderlichen Funktionen zuverlässig bereitstellt und darüber hinaus keine unerwünschten Nebeneffekte aufweist. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Organisationseinheit wird die grundsätzliche Erlaubnis erteilt, die Software produktiv in der Institution zu nutzen. Gleichzeitig übernimmt diese Organisationseinheit damit auch die Verantwortung für das IT-Verfahren, das durch die Software unterstützt wird.

Software kann an unterschiedlichen Stellen ihres Lebenszyklus getestet werden. So können Software-Tests bereits bei der Entwicklung, vor der Freigabe für den Produktivbetrieb oder im Zuge des Patch- und Änderungsmanagements notwendig werden. Dies betrifft sowohl Individualsoftware als auch standardisierte Software. Eine besondere Rolle nehmen hierbei Regressionstests ein, denn selbst wenn nur kleinere Aspekte der Software geändert werden, besteht die Möglichkeit, dass sich dies auf ganz andere Aspekte und Funktionen der Software auswirkt. Regressionstests überprüfen Software genau auf diese Auswirkungen hin.

Dieser Baustein beschreibt den Test- und Freigabeprozess für jegliche Art von Software. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann.

1.2 Zielsetzung

Mit der Umsetzung dieses Bausteins sorgt die Institution dafür, dass die eingesetzte Software den technischen und organisatorischen Anforderungen sowie dem vorliegenden Schutzbedarf der gesamten Institution oder einzelner Organisationseinheiten entspricht. Ein wesentlicher Teilaspekt ist dabei, dass sicherheitskritische Software auf bestehende Schwachstellen systematisch und methodisch überprüft wird.

1.3 Abgrenzung und Modellierung

Der Baustein OPS.1.1.6 *Software-Tests und Freigaben* ist auf den Informationsverbund einmal

anzuwenden.

Während der Baustein CON.8 *Softwareentwicklung* auf den Softwareentwicklungsprozess und die darin enthaltenen Software-Tests, die während des Entwicklungsprozesses notwendig sind, eingeht, beschreibt dieser Baustein die speziellen Anforderungen, die an ein Test- und Freigabemanagement gestellt werden. Dabei bezieht sich dieses Test- und Freigabemanagement nicht ausschließlich auf selbst oder im Kundenauftrag entwickelte Software, sondern auch auf das Testen und die Freigabe von jeglicher Software, wie sie in APP.6 *Allgemeine Software* beschrieben wird, sowie alle weiteren Softwareprodukten der Schicht APP *Anwendungen*.

Software-Tests können auch Bestandteil des Patch- oder Änderungsmanagements oder der Software-Entwicklung werden. Entsprechende Anforderungen sind im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* sowie CON.8 *Software-Entwicklung* näher spezifiziert.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.6 *Software-Tests und -Freigaben* von besonderer Bedeutung.

2.1 Software-Tests mit Produktivdaten

Werden Software-Tests mit Produktivdaten durchgeführt, können hierdurch Sicherheitsprobleme entstehen. Insbesondere vertrauliche Produktivdaten könnten dabei von unbefugten Mitarbeitern oder Dritten eingesehen werden, die mit dem jeweiligen Software-Test beauftragt wurden. Wird mit den „originalen“ Produktivdaten getestet und nicht mit Kopien der Daten, könnten diese ungewollt geändert oder gelöscht werden.

Durch Software-Tests im Produktivbetrieb könnte der gesamte Betrieb massiv gestört werden. Denn Fehlfunktionen der zu testenden Software können sich auch auf andere Anwendungen und IT-Systeme auswirken, die dadurch ebenfalls gestört werden. Hinzu kommt, dass Software-Tester bewusst die Software im Grenzbereich testen und damit beabsichtigen, mögliche Fehler aufzudecken. Dies erhöht wiederum die Gefahr, dass der gesamte Betrieb gestört wird.

2.2 Fehlendes oder unzureichendes Testverfahren

Wird neue Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, können Fehler in der Software unerkannt bleiben. Ebenso ist es möglich, dass dadurch erforderliche und einzuhaltende Installationsparameter nicht erkannt oder nicht beachtet werden.

Diese Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Testverfahren resultieren, können den IT-Betrieb der Institution erheblich gefährden. So können beispielsweise wichtige Daten verloren gehen, wenn ein Update eines Datenbankmanagementsystems ohne vorherigen Test eingespielt wird.

2.3 Fehlendes oder unzureichendes Freigabeverfahren

Ein fehlendes oder unzureichendes Freigabeverfahren kann dazu führen, dass Software eingesetzt wird, die von der Fachseite nicht abgenommen wurde. Auf diese Weise kann die Software Funktionen umfassen, die sie nicht enthalten sollte, oder benötigte Funktionen können fehlen. Außerdem kann die Software zu anderen Anwendungen inkompatibel sein.

2.4 Fehlende oder unzureichende Dokumentation der Tests und Testergebnisse

Software kann in der Regel freigegeben werden, sobald alle Tests durchgeführt wurden und keine Abweichungen gefunden wurden. Sollte die Dokumentation der Software-Tests jedoch unvollständig sein, ist nachträglich nicht erkennbar, was getestet wurde. Wurden erkannte Softwarefehler oder fehlende Funktionen ungenügend dokumentiert und damit bei der Freigabe nicht berücksichtigt,

können durch diese Abweichungen die zu verarbeitenden Produktivdaten ungewollt gelöscht oder verändert werden. Außerdem können andere IT-Systeme und Anwendungen gestört werden.

2.5 Fehlende oder unzureichende Dokumentation der Freigabekriterien

Wenn Freigabekriterien nicht klar kommuniziert werden, kann dies dazu führen, dass Software voreilig freigegeben wird oder keine Freigabe erfolgt, obwohl diese erteilt werden könnte. Dadurch könnten zum einen Versionen mit unerkannten Softwarefehlern freigegeben werden, die den Produktivbetrieb stören können. Zum anderen kann eine fehlende oder unzureichende Dokumentation der Freigabekriterien dazu führen, dass sich Projekte verzögern und dadurch finanzielle Schäden entstehen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.6 *Software-Tests und -Freigaben* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Tester, Fachverantwortliche, Datenschutzbeauftragter, Personalabteilung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein OPS.1.1.6 *Software-Tests und -Freigaben* vorrangig erfüllt werden:

OPS.1.1.6.A1 Planung der Software-Tests (B)

Die Rahmenbedingungen für Software-Tests MÜSSEN vor den Tests innerhalb der Institution entsprechend der Schutzbedarfe, Organisationseinheiten, technischen Möglichkeiten und Test-Umgebungen festgelegt sein. Die Software MUSS auf Basis der Anforderungen des Anforderungskatalogs zu der Software getestet werden. Liegt auch ein Pflichtenheft vor, dann MUSS dieses zusätzlich berücksichtigt werden.

Die Testfälle MÜSSEN so ausgewählt werden, sodass diese möglichst repräsentativ alle Funktionen der Software überprüfen. Zusätzlich SOLLTEN auch Negativ-Tests berücksichtigt werden, die überprüfen, ob die Software keine ungewollten Funktionen enthält.

Die Testumgebung MUSS so ausgewählt werden, sodass diese möglichst repräsentativ alle in der Institution eingesetzten Gerätemodelle und Betriebssystemumgebungen abdeckt. Es SOLLTE dabei getestet werden, ob die Software mit den eingesetzten Betriebssystemen in den vorliegenden Konfigurationen kompatibel und funktionsfähig ist.

OPS.1.1.6.A2 Durchführung von funktionalen Software-Tests [Tester] (B)

Mit funktionalen Software-Tests MUSS die ordnungsgemäße und vollständige Funktion der Software überprüft werden. Die funktionalen Software-Tests MÜSSEN so durchgeführt werden, dass sie den Produktivbetrieb nicht beeinflussen.

OPS.1.1.6.A3 Auswertung der Testergebnisse [Tester] (B)

Die Ergebnisse der Software-Tests MÜSSEN ausgewertet werden. Es SOLLTE ein Soll-Ist-Vergleich mit definierten Vorgaben durchgeführt werden. Die Auswertung MUSS dokumentiert werden.

OPS.1.1.6.A4 Freigabe der Software [Fachverantwortliche] (B)

Die fachlich zuständige Organisationseinheit MUSS die Software freigeben, sobald die Software-Tests erfolgreich durchgeführt wurden. Die Freigabe MUSS in Form einer Freigabeerklärung dokumentiert werden.

Die freigebende Organisationseinheit MUSS überprüfen, ob die Software gemäß den Anforderungen getestet wurde. Die Ergebnisse der Software-Tests MÜSSEN mit den vorher festgelegten Erwartungen übereinstimmen. Auch MUSS überprüft werden, ob die rechtlichen und organisatorischen Vorgaben eingehalten wurden.

OPS.1.1.6.A5 Durchführung von Software-Tests für nicht funktionale Anforderungen [Tester] (B)

Es MÜSSEN Software-Tests durchgeführt werden, die überprüfen, ob alle wesentlichen nichtfunktionalen Anforderungen erfüllt werden. Insbesondere MÜSSEN sicherheitsspezifische Software-Tests durchgeführt werden, wenn die Anwendung sicherheitskritische Funktionen mitbringt. Die durchgeführten Testfälle, sowie die Testergebnisse, MÜSSEN dokumentiert werden.

OPS.1.1.6.A11 Verwendung von anonymisierten oder pseudonymisierten Testdaten [Datenschutzbeauftragter, Tester] (B)

Wenn Produktivdaten für Software-Test verwendet werden, die schützenswerte Informationen enthalten, dann MÜSSEN diese angemessen während der Software-Tests geschützt werden. Enthalten diese Daten personenbezogene Informationen, dann MÜSSEN diese Daten anonymisiert werden. Wenn ein Personenbezug von den Testdaten abgeleitet werden könnte, MUSS der Datenschutzbeauftragte und unter Umständen die Personalvertretung hinzugezogen werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein OPS.1.1.6 *Software-Tests und -Freigaben*. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.6.A6 Geordnete Einweisung der Software-Tester [Fachverantwortliche] (S)

Die Software-Tester SOLLTEN über die durchzuführenden Testarten und die zu testenden Bereiche einer Software vom IT-Betrieb informiert werden. Darüber hinaus SOLLTEN die Software-Tester über die Anwendungsfälle und mögliche weitere Anforderungen der Software informiert werden.

OPS.1.1.6.A7 Personalauswahl der Software-Tester [Personalabteilung, Fachverantwortliche] (S)

Bei der Auswahl der Software-Tester SOLLTEN gesonderte Auswahlkriterien berücksichtigt werden. Die Software-Tester SOLLTEN die erforderliche berufliche Qualifikation haben.

Wird Individualsoftware auf Quellcode-Ebene überprüft, dann SOLLTEN die Tester über ausreichendes Fachwissen über die zu testenden Programmiersprache und der Entwicklungsumgebung verfügen. Der Quellcode SOLLTE NICHT ausschließlich von Testern überprüft werden, die an der Erstellung des Quellcodes beteiligt waren.

OPS.1.1.6.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.6.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.6.A10 Erstellung eines Abnahmeplans (S)

In einem Abnahmeplan SOLLTEN die durchzuführenden Testarten, Testfälle und die erwarteten Ergebnisse dokumentiert sein. Außerdem SOLLTE der Abnahmeplan die Freigabekriterien beinhalten. Es SOLLTE eine Vorgehensweise für die Situation festgelegt werden, wenn eine Freigabe abgelehnt wird.

OPS.1.1.6.A12 Durchführung von Regressionstests [Tester] (S)

Wenn Software verändert wurde, SOLLTEN Regressionstests durchgeführt werden. Hierbei SOLLTE überprüft werden, ob bisherige bestehende Sicherheitsmechanismen und -einstellungen durch das Update ungewollt verändert wurden. Regressionstests SOLLTEN vollständig durchgeführt werden und hierbei auch Erweiterungen sowie Hilfsmittel umfassen. Werden Testfälle ausgelassen, SOLLTE dies begründet und dokumentiert werden. Die durchgeführten Testfälle und die Testergebnisse SOLLTEN dokumentiert werden.

OPS.1.1.6.A13 Trennung der Testumgebung von der Produktivumgebung (S)

Software SOLLTE nur in einer hierfür vorgesehenen Testumgebung getestet werden. Die Testumgebung SOLLTE von der Produktivumgebung getrennt betrieben werden. Die in der Testumgebung verwendeten Architekturen und Mechanismen SOLLTEN dokumentiert werden. Es SOLLTEN Verfahren dokumentiert werden, wie mit der Testumgebung nach Abschluss des Software-Tests zu verfahren ist.

OPS.1.1.6.A15 Überprüfung der Installation und zugehörigen Dokumentation [Tester] (S)

Die Installation der Software SOLLTE entsprechend der Regelungen zur Installation und Konfiguration von Software (siehe Baustein APP.6 *Allgemeine Software*) überprüft werden. Falls vorhanden, SOLLTE zusätzlich die Installations- und Konfigurationsdokumentation geprüft werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein OPS.1.1.6 *Software-Tests und -Freigaben* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

OPS.1.1.6.A14 Durchführung von Penetrationstests [Tester] (H)

Für Anwendungen beziehungsweise IT-Systeme mit erhöhtem Schutzbedarf SOLLTEN Penetrationstests als Testmethode durchgeführt werden. Ein Konzept für Penetrationstests SOLLTE erstellt werden. Im Konzept für Penetrationstests SOLLTEN neben den zu verwendenden Testmethoden auch die Erfolgskriterien dokumentiert werden.

Der Penetrationstest SOLLTE nach den Rahmenbedingungen des Penetrationstest-Konzepts erfolgen. Die durch den Penetrationstest aufgefundenen Sicherheitslücken SOLLTEN klassifiziert und dokumentiert sein.

OPS.1.1.6.A16 Sicherheitsüberprüfung der Tester (H)

Sofern Tester auf besonders schützenswerte Informationen zugreifen müssen, SOLLTE die Institution Nachweise über ihre Integrität und Reputation einholen. Handelt es sich dabei um klassifizierte Verschlusssachen, SOLLTEN sich die Software-Tester einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) unterziehen. Hierzu SOLLTE der ISB den Geheimschutzbeauftragten bzw. Sicherheitsbevollmächtigten der Institution einbeziehen.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Annex A.14 „System Acquisition, Development and maintenance“ Anforderungen an die sichere

System-Entwicklung, die auch einen Test- und Freigabeprozess erfordert, sowie direkt an Testdaten selbst. Darüber hinaus hat die ISO die Norm ISO/IEC 29119-2:2013 „Software and systems engineering - Software testing - Part 2: Test processes, International Organization for Standardization“ veröffentlicht, die ausführlich Anforderungen an Software-Tests behandelt.

Das BSI hat die Studie „Durchführungskonzept für Penetrationstests“, die als Grundlage für Penetrationstests verwendet werden kann, sowie den BSI-Leitfaden zur Entwicklung sicherer Webanwendungen, der auch Software-Tests inkludiert, veröffentlicht.

Das Information Security Forum (ISF) führt in „The Standard of Good Practice for Information Security“ Aspekte zum Testen und Freigeben zu allen relevanten Anforderungen (Areas) aus.

Das National Institute of Standards and Technology stellt Richtlinien zum Testen von Software in der NIST Publication 800-53 in der SA 11 Developer Security Testing and Evaluation zur Verfügung.

Das Buch „The Art of Software Testing“ von Glenford J. Myers, Corey Sandler, Tom Badgett, kann für Software-Tests konsultiert werden.

Das Common Vulnerability Scoring System kann als Scoring-System zur Klassifikation des Schweregrades einer Sicherheitslücke verwendet werden und somit die Ergebnisse von Software-Tests in Bezug auf die Informationssicherheit darstellen.

5 Anlage: Kreuzreferenztablelle zu elementaren Gefährdungen

Die Kreuzreferenztablelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein OPS.1.1.6 *Software-Tests und -Freigaben* von Bedeutung.

- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.32 Missbrauch von Berechtigungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.41 Sabotage
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen