



KONZEPTE UND METHODEN

Informationssicherheit

Stand: Juni 2026

Obeco GmbH

Arenberger Str. 230a, 56077 Koblenz



Informationssicherheit

Viele Anwenderinnen und Anwender fragen sich nach dem Sinn und Zweck eines Software-Servicevertrags. Diese Frage beantworten wir im Folgenden exemplarisch am Begriff der Informationssicherheit – denn der Servicevertrag ist letztlich Ihre Informationssicherheit. Wir gehen dabei auf vier Fragen ein: Was ist Informationssicherheit? Warum ist sie notwendig? Wie wird sie sichergestellt? Und wie überprüfen wir sie?

Was ist Informationssicherheit?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert in „IT-Sicherheitsmanagement und IT-Grundschutz“: Informationssicherheit hat den Schutz von Informationen zum Ziel. Die klassischen Grundwerte der IT-Sicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – sind dabei die Grundlagen dieses Schutzes.

Neben vorsätzlichen Handlungen ist diese Sicherheit unter anderem bedroht durch:

- höhere Gewalt (Sturm, Feuer, Erdbeben usw.),
- Fehler nach Software-Updates,
- Änderungen in den Geschäftsprozessen,
- Verarbeitungsfehler im organisatorischen Umfeld.

Warum ist Informationssicherheit notwendig?

Sicherheit ist kein unveränderbarer Zustand, der einmal erreicht wird und sich nie wieder ändert. Jedes Unternehmen ist ständigen, dynamischen Veränderungen unterworfen:

- Änderungen der Geschäftsprozesse,
- neue Infrastruktur- und Organisationsstrukturen.

Neben den unvorhersehbaren Änderungen innerhalb einer Institution können sich außerdem die Rahmenbedingungen ändern:

- gesetzliche oder vertragliche Vorgaben,
- verfügbare Informations- oder Kommunikationstechnik.

Die Unternehmensleitung ist zudem per Gesetz generell verpflichtet, ein internes Kontrollsystem zur Risikofrüherkennung und -abwehr einzuführen und zu betreiben. Es ist daher notwendig, Sicherheit aktiv zu managen, um ein einmal erreichtes Sicherheitsniveau dauerhaft aufrechtzuerhalten und gegebenenfalls zu erhöhen.

Wie wird Informationssicherheit überprüft?

Die Informationssicherheit im Betrieb von Software wird durch die Umsetzung folgender Ziele hergestellt:

- **Richtigkeit:** Das Programm arbeitet ohne Fehler.



- **Vollständigkeit:** Alle Funktionen sind verfügbar und leicht zu erreichen.
- **Performanz:** Die Antwortzeiten sind akzeptabel.
- **Änderbarkeit:** Das Programm ist einfach zu verändern.
- **Zeitgerechtigkeit** der Verarbeitung.
- **Ordnung und Nachvollziehbarkeit** der Abläufe.

Wer gefährdet die Informationssicherheit?

Die Informationssicherheit wird durch Änderungen der Programmumgebung gefährdet. Jedes Computerprogramm ist zumindest den Änderungen der Systemsoftware unterworfen. Mit jeder Veränderung verringert sich die bisher erreichte Informationssicherheit, da nicht bekannt ist, ob sich die neue Umgebung negativ auf das Laufzeitverhalten auswirkt.

Die folgende Übersicht zeigt exemplarisch, wie häufig sich die eingesetzte Systemsoftware ändert – mit Versionszyklus, jährlichem Alterungsverlust sowie der Zahl der Servicepacks, Hotfixes und Patches pro Jahr:

- **Betriebssystem Server:** Versionszyklus 3 Jahre, Alterungsverlust 33 % pro Jahr, 2 Servicepacks und 36 Hotfixes bzw. Patches pro Jahr.
- **SQL-Server:** 3 Jahre, 33 %, 1 Servicepack, 12 Hotfixes/Patches.
- **Betriebssystem Client:** 4 Jahre, 25 %, 1 Servicepack, 36 Hotfixes/Patches.
- **Programmiersprache (Visual Studio):** 3 Jahre, 33 %, 1 Servicepack, 6 Hotfixes/Patches.
- **Erweiterung Oberflächenkomponenten:** 2 Jahre, 50 %, 3 Servicepacks, 3 Hotfixes/Patches.
- **Erweiterung Druckausgabe und Reporting:** 2 Jahre, 50 %, 2 Servicepacks, 12 Hotfixes/Patches.
- **Optional (Imaging, OCR, Workflow, MDE usw.):** 3 Jahre, 33 %, 2 Servicepacks.

In der Summe ergeben sich so rund zehn potenzielle Änderungsereignisse pro Monat – jedes davon kann das Laufzeitverhalten und damit die Informationssicherheit beeinflussen.

Schutzmaßnahmen

Wie reagieren wir auf diese Gefährdung? Wir setzen eine Struktur ein, die die Businesslogik von den Subsystemen trennt. Damit können wir die gewünschte Informationssicherheit gewährleisten. Die Architektur gliedert sich wie folgt:

- **Anwendungslogik:** Sie enthält die Businesslogik des einzelnen Kunden (z. B. Business-Logik A, B und C) und ist von der Programmlogik des Kernels vollständig getrennt.
- **Policom Kernel:** Er umfasst die Basisfunktionalität für die tabellarische Anzeige, Datenerfassung, Datenausgabe, Datenbankzugriffe, Visualisierung, Navigation und das Reporting. Dieses Modul ist für alle Policom-Anwendungen identisch.



- **Subsysteme:** Betriebssystem (z. B. Windows Server, Client), SQL Server, Entwicklungsumgebung (Visual Studio), Oberflächen- und Reporting-Komponenten sowie Erweiterungen wie Imaging, OCR, Archiv, BDE, MDE und PZE.

Der Businesscode ist von den benutzten Subsystemen getrennt. Ändern sich die Subsysteme, werden diese Veränderungen nicht an die Businesslogik weitergegeben, sondern im Kernel abgewickelt.

Policom Change Management

Durch die Trennung der Businesslogik vom Policom-Kernsystem können wir Änderungen in den Subsystemen abfangen, ohne dass der Businesscode geändert werden muss. Die Aufwände entstehen nur einmalig, wodurch sich die Kosten für alle Kunden reduzieren. Die Anpassungen erfolgen in Abhängigkeit von:

- neuen Versionen der eingesetzten Komponenten,
- Änderungen im Kernel aufgrund neuer oder geänderter Funktionalität,
- Erweiterungen der Anwendungslogik gemäß Kundenwunsch.

Diese Änderungen liefern wir zyklisch – monatlich oder quartalsweise – an unsere Kunden aus. Der Ablauf gliedert sich in drei Phasen:

- **Entwicklung:** Auf Basis der aktuellen Version wird eine neue Version erzeugt, die Anpassungen an die Umgebungsänderungen werden programmiert und die geänderte Version in das Testsystem kopiert.
- **Test:** Die Änderungen an den SQL-Server-Objekten werden übernommen; anschließend erfolgen Funktionstest und Freigabe.
- **Produktion:** Es wird ein neues Setup erstellt und beim Kunden installiert, die abschließende Dokumentation wird erstellt. Dabei wird die bisher aktuelle Version zur Vorgängerversion und die neue Version zur aktuellen Version.

Software-Servicevertrag

Der Software-Servicevertrag deckt die Aufwendungen ab, die zur Herstellung der gesetzlich vorgeschriebenen Informationssicherheit entstehen:

- Anpassungen an die geänderte Systemumgebung,
- Erstellung und Verteilung der Updates,
- unsere Hotline, die Ihnen bei Fragen kostenlos zur Verfügung steht.

Da sich Änderungen an einer aktuellen Programmversion einfacher durchführen lassen, ist der Stundensatz für Dienstleistung und Programmierung um 33 % reduziert. So erhalten Sie eine Anwendung, die auch nach Jahren ihres Betriebs die Umsetzung der gesetzlichen Anforderungen an die Informationssicherheit sicherstellt.



Sie haben Fragen zum Software-Servicevertrag oder zur Informationssicherheit? Wir beraten Sie gerne unter 0261-9634466-0 oder info@obecosupport.de.