ONLINE SICHERHEIT.AT

Auditprogramm

Bei der Kontrolle der tatsächlich getroffenen Sicherheitsmaßnahmen sind insbesondere interne und externe Sicherheitsaudits und Sicherheitsanalysen (Penetrationstests und Source Code-Analysen) zu unverzichtbaren Maßnahmen geworden.

Audits und Sicherheitsanalysen decken nicht nur Konformitätsabweichungen zu geltenden Rechtsvorschriften und internen Regelungen oder kritische Sicherheitsschwachstellen auf. Sie identifizieren zudem Optimierungspotenzial und mögliche Verbesserungsmaßnahmen zur Erhöhung des Sicherheitsniveaus. Sie dienen daher als wertvolle Instrumente, um die Rentabilität und Wirksamkeit des Informationssicherheits-Managements nachhaltig zu steigern.

Abnahmekriterien

Die Festlegung von sicherheitsrelevanten Abnahmekriterien dient der Durchführung und Protokollierung von Abnahmetests.

Secure Coding-Standards und Source Code-Analysen

Durch die Festlegung und Schulung von Secure Coding-Standards sollen Sicherheitsschwachstellen im Programm-Quellcode von IT-Anwendungen weitgehend vermieden werden. Die Durchführung von Source Code-Analysen ermöglicht die Prüfung der Einhaltung von Secure Coding-Standards sowie die Identifizierung von (etwaig) bestehenden Sicherheitsschwachstellen.

Penetrationstests

Die Durchführung von Penetrationstests ermöglicht neben der Identifizierung von bestehenden Sicherheitsschwachstellen im Programm-Quellcode auch die Erkennung von Design- und Architekturschwachstellen, von veralteten Versionen der eingesetzten Softwareprodukte und von vorliegenden Systemkonfigurationsfehlern.

System-, Produkt- und Prozessaudits

Die Durchführung von System-, Produkt- und Prozessaudits dient der Prüfung der Aktualität, Vollständigkeit, Konformität, Einhaltung und Wirksamkeit des Informationssicherheits-Managementsystems, der dokumentierten Sicherheitsrichtlinien sowie der festgelegten und umgesetzten Sicherheitsmaßnahmen.

Weitere Informationen

Folgende Normen, Standards und Sicherheitshandbücher unterstützen bei der Implementierung und dem Betrieb eines Auditprogramms:

- **ISO/IEC 27007 –** Leitfaden für ISMS-Audits
- **ISO/IEC TR 27008 –** Leitfaden für die Überprüfung von Sicherheitsmaßnahmen
- **Österreichisches Informationssicherheitshandbuch –** Etablierung eines umfassenden Informationssicherheits-Managementsystems (ISMS) in Behörden
- **Standards (Checklisten) zur Internet-Sicherheit (ISi-Reihe)** des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI)

> rechtlicher Hinweis

< zurück

Datum der Veröffentlichung: 12.11.2012

Für den Inhalt verantwortlich:

- A-SIT Zentrum für sichere Informationstechnologie – Austria

---