Technische Universität Braunschweig

Stabsstelle CISO

Stabsstelle CISO
Software Entwicklung

Robert Strötgen auf der Grundlage der Ausarbeitung durch Michael Weissing, 8.11.2023

Softwareentwicklung mit den Vorgaben des BSI

Summary:

- Wer Softwareentwicklung nach Best Practice macht, ist auf dem besten Weg.
- Die folgende Präsentation nimmt noch den einen und anderen Punkt aus der IT-Sicherheit (BSI Grundschutzkompendium) hinzu

Basismaßnahmen

Vorgehensweise

- Für den Software-Entwicklungsprozess ist ein Gesamtverantwortlicher zu benennen, sowie Rollen und Verantwortlichkeiten für alle Aktivitäten im Rahmen der Software-Entwicklung festzulegen.
- Für jedes Entwicklungsprojekt ist ein Sicherheitsverantwortlicher zu benennen
- Es ist ein geeignetes Vorgehensmodell zur Software-Entwicklung seitens des Projektteams festzulegen. Die relevanten Sicherheitsanforderungen sind zu dokumentieren.

BSI Grundschutz-Einteilungen

Schutzniveau

- Das BSI Grundschutzkompendium unterscheidet bei den geforderten Maßnahmen zwischen
  - Basismaßnahmen (erreicht nur ein Niveau unterhalb des Grundschutzniveaus, nicht zertifizierbar)
  - Standardmaßnahmen (Grundschutzniveau für normalen Schutzbedarf, zertifizierbar)
  - Erweiterte Maßnahmen (nötig bei erhöhtem Schutzbedarf, zertifizierbar)
- Wir betrachten hier nur den Basisschutz und die Standardmaßnahmen.

Basismaßnahmen

Vorgehensweise

- Sofern ein Wechsel des Vorgehensmodells während des Projektes notwendig ist, müssen die Gründe dokumentiert und alle Beteiligten hierüber informiert werden. Der entwickelte oder geänderte Quellcode muss auf Fehler gesichtet und auf Kompatibilität mit allen genutzten Lizenzmodelle überprüft werden. Dies gilt insbesondere bei der Einbindung externer Komponenten und deren Schwachstellen Prüfung

Basismaßnahmen

Sicheres Design

- Grundsätzlich sind alle Eingabedaten/Formulardaten vor der Weiterverarbeitung zu prüfen und zu validieren.
- Bei Client-Server-Anwendungen sind die Daten grundsätzlich auf dem Server zu validieren.
- Die Software ist so zu konfigurieren, dass ein sicherer Betrieb bereits im Standard der Software gewährleistet ist (dies ist auch in der EU-DSGVO vorgeschrieben).
- Bei Fehlern oder Ausfall von Komponenten der Software oder des darunter liegenden IT-Systems dürfen keine vertraulichen Daten preisgegeben werden.
- **Der Betrieb der Software muss mit möglichst geringen Benutzerprivilegien nach dem Need-to-Know-Prinzip möglich sein**
- Das Software und Systemdesign muss für Dritte nachvollziehbar dokumentiert werden

Basismaßnahmen

Testen

- Sofern auf externe Bibliotheken zurückgegriffen wird, sind diese aus vertrauenswürdigen Quellen zu beziehen. Bevor die externen Bibliotheken verwendet werden, sind diese durch geeignete Methoden auf deren Integrität (bspw. die genutzte Lizenz, **veröffentliche Sicherheitsprobleme** und deren Zeitraum bis zur Behebung sowie die stetige Weiterentwicklung) zu prüfen.
- Vor der Freigabe neuer oder geänderter Softwareversionen sind angemessene Tests durchzuführen, bei denen die Funktionalität und Sicherheit der Software auf dem Zielsystem geprüft wird. Alle kritischen Grenzwerte für die Funktionalität und Sicherheit sind zu testen. Des Weiteren sind für die entwickelte Software Code Reviews und eine automatische statische Code-Analyse durchzuführen. Verwendete externe Bibliotheken sind ebenfalls in den Code Reviews zu integrieren.

Basismaßnahmen

Patches und Updates

- Seitens der Entwickler muss sichergestellt sein, dass sicherheitskritische Patches und Updates zeitnah durch die Entwickler bereitgestellt und die Verantwortlichen diese einspielen. Dies gilt ebenfalls auch für verwendete externe Bibliotheken.
- Für die Installations-, Update- oder Patchdateien sind vom Entwickler digitale Signaturen bereitzustellen.

Basismaßnahmen

Compliance

Alle Compliance-Anforderungen:

- die internen Sicherheitsvorgaben,
- die internen Datenschutzvorgaben,
- die internen Notfallmanagementvorgaben,
- die rechtlichen Anforderungen
- und die spezifischen Sicherheitsanforderungen

sind bei der Software-Entwicklung **zu ermitteln** und zu berücksichtigen.

Basismaßnahmen

Versionsverwaltung

Das Entwicklungsprojekt (der Quellcode des Projektes) ist über eine geeignete Versionsverwaltung zu verwalten

Geregelt werden muss:

- Zugriff auf das Versionverwaltungstool
- Wann ist eine Änderung eine eigene Version
- Alle Änderungen am Quellcode müssen rückgängig gemacht werden können

Standardmaßnahmen

Schulung

Schulung des Projektteams zu

- Datenschutz
- Informationssicherheit
- Notfallmanagementaspekten

Standardmaßnahmen

Entwicklungsumgebung

- Die Test- und Entwicklungsumgebungen müssen getrennt von der Produktionsumgebung betrieben werden
- Verteilte und remote Arbeitsplätze der Software-Entwicklung dürfen nur über eine kryptographisch abgesicherte Verbindung miteinander kommunizieren