

Grundschutzbaustein

Sichere System-Entwicklung

EUROSEC GmbH Chiffriertechnik & Sicherheit

Autor: Dr. Thilo Zieschang, EUROSEC

Tel: 06173 / 60850, www.eurosec.com

© EUROSEC GmbH Chiffriertechnik & Sicherheit, 2005

Der Baustein im Kurzüberblick

Vorbemerkung: die Darstellung orientiert sich am Sachstand Oktober 2005. Der Baustein befindet sich in der Reviewphase und wird noch Änderungen erfahren vor der endgültigen Veröffentlichung. Die nachfolgende Darstellung dient lediglich zur Vorab-Information.

Worum es geht

- Grundsatzbaustein zum Thema Sichere System-Entwicklung
- 15 Maßnahmen, die den gesamten Entwicklungsprozess adressieren
- Schwerpunkt weniger auf technischer (z.B. Programmiersprachen-)Ebene, sondern auf Prozessen, Workflows, Zuständigkeiten etc.
- Naturgemäß eher generische Maßnahmen, bedingt durch beschränkten Gesamtumfang

Zielgruppe

- Baustein spricht nicht nur Entwickler an, sondern Fachverantwortliche für Sicherheit sowie Entwicklungsleiter
- Keine speziellen technische Vorkenntnisse in sicherer System-Entwicklung erforderlich zur Umsetzung der Maßnahmen
- Baustein spricht von „System-Entwicklung“ statt von Softwareentwicklung, da Hardware-orientierte Entwicklungen die selben formulierten Maßnahmen berücksichtigen können und müssen

Status des Bausteins

- Erstellung in der Hauptsache zu Jahresbeginn 2005, danach ausgedehnte Reviewphase
- Stabile Version liegt derzeit vor und wird für die Veröffentlichung vorbereitet
- Voraussichtliche Veröffentlichung in elektronischer Vorab-Version auf BSI-Webseiten: Januar 2006
- Voraussichtliche Aufnahme als Ergänzungslieferung in das Grundschutzhandbuch: voraussichtlich zweite Jahreshälfte 2006

| | | | | | |
|---|---|---|---|---|---|
| 3 | 4 | 5 | 6 | 7 | 8 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 4 | 5 | 6 | 7 | 8 |
| | | 1 | | | |
| | | 2 | | | |
| 2 | 3 | 3 | 3 | 3 | 3 |
| | | 4 | | | |
| | | 5 | | | |
| 3 | 4 | 5 | 6 | 7 | 8 |
| 6 | 6 | 6 | 6 | 6 | 6 |
| | | 7 | | | |
| | | 8 | | | |
| 9 | 9 | 9 | 9 | 9 | 9 |
| 3 | 4 | 5 | 6 | 7 | 8 |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 4 | 5 | 6 | 7 | 8 |
| | | 1 | | | |
| | | 2 | | | |
| 2 | 3 | 3 | 3 | 3 | 3 |
| | | 4 | | | |
| | | 5 | | | |
| 3 | 4 | 5 | 6 | 7 | 8 |
| 6 | 6 | 6 | 6 | 6 | 6 |
| | | 7 | | | |
| | | 8 | | | |

Die Maßnahmen im Überblick

(Details folgen anschließend)

Liste der Maßnahmen (1)

- Maßnahme 1: Initialisierung einer Systemumgebung
- Maßnahme 2: Erstellung eines Anforderungskatalogs für die Systementwicklung
- Maßnahme 3: Projektmanagement bei der Systementwicklung
- Maßnahme 4: Vergabe der Systementwicklung
- Maßnahme 5: Dokumentation bei Systementwicklung
- Maßnahme 6: Schulung der Entwickler
- Maßnahme 7: Architekturentwurf / Design / Grobkonzept / Feinkonzept
- Maßnahme 8: Designspezifikation erstellen und mit Anforderungsspezifikation abgleichen

Liste der Maßnahmen (2)

- Maßnahme 9: Aufbau einer geeigneten Entwicklungsumgebung
- Maßnahme 10: Implementierung: Häufige Implementierungsfehler vermeiden
- Maßnahme 11: Aufbau einer geeigneten Testumgebung für die Systemumgebung, Tests
- Maßnahme 12: Auslieferung und Betrieb
- Maßnahme 13: Notfallvorsorge
- Maßnahme 14: Datenschutzgerechte Systementwicklung
- Maßnahme 15: Makro-Software-Entwicklung durch Endbenutzer

Maßnahme 1: Initialisierung einer Systemumgebung

- Erste Idee, Produkt-Konzeption, Einsatzbedingungen
- Wie beeinflusst das Produkt die Sicherheit existierender Systeme oder Netze
- Beschaffung externer Hard- und Software organisieren
- Vertrauenswürdigkeit von Herstellern und Entwicklern
- Gesamt-Vorgehensmodell zur System-Entwicklung
- Freigabe durch IT-Sicherheitsmanagement

Maßnahme2: Erstellung eines Anforderungskatalogs für die Systementwicklung

Bevor mit Sicherheitsarchitektur, -design oder gar Implementierung von Systemen begonnen werden kann, muss geklärt werden, welche Anforderungen bei der konkreten Entwicklung überhaupt erforderlich sind und im weiteren Verlauf beachtet werden müssen.

- Anforderungen identifizierter Einsatzszenarien analysieren
- Anforderungen externer Rahmenwerke
- Sicherheitsanforderungen von Anwendern/Auftraggebern berücksichtigen
- Alle ermittelten Anforderungen adäquat formulieren in Anforderungsspezifikation
- Restrisiken identifizieren und Ersatz- bzw. Ergänzungsmaßnahmen vorsehen

Maßnahme 3: Projektmanagement bei der Systementwicklung

- Planung und Steuerung eines System-Entwicklungsprojektes
- Projektmanagement
- Festlegung der Verantwortlichkeiten bei der Systementwicklung
- Auswahl einer geeigneten Entwicklungsmethode
- Wahl einer geeigneten Programmiersprache
- Auswahl von Entwicklungsumgebung und CASE Tools
- Auswahl weiterer Tools, z.B. Versionsmanagement
- Ergebnis-Input und -Output für alle Phasen festlegen
- Prozesse für Genehmigung, Bewertung, Dokumentation, Entscheidung

Maßnahme 3: Projektmanagement bei der Systementwicklung (2)

- Abnahme-Prozeduren und -Anforderungen festlegen
- Abnahmekriterien für erfolgreiche Tests formulieren
- Kontinuierliche Qualitätsverbesserung organisieren
- Fehler-Management
- Patch-Management Unterstützung
- Versionsverwaltung
- Sicherheitswarnungen gewährleisten
- Nachbesserungsprozess festlegen

Maßnahme 4: Vergabe der Systementwicklung

- Geeignete Auswahl / Vertrauenswürdigkeit von Herstellern und Entwicklern
- Vertragsrelevante Sicherheitsaspekte bei System-Entwicklungen
- Funktionale Eigenschaften vertraglich zusichern lassen
- Lizenzvereinbarungen beachten
- Patentrechte Dritter klären
- Gewährleistung und Haftung
- Reaktionszeiten
- Qualität und Verfügbarkeit von Sicherheitsinformationen
- Behandlung vertraulicher Informationen und geistigen Eigentums
- Abwesenheit von Hintertüren zusichern lassen
- Auditierbarkeit
- Entwicklungsumgebung
- Hinterlegung des Quellcodes
- Sicherheitsmaßnahmen bei extern durchgeführten Entwicklungsvorhaben

Maßnahme 5: Dokumentation bei Systementwicklung

- Produktdokumentation
- Dokumentation des Entwicklungsprozesses
- Code-Kommentierung

Maßnahme 6: Schulung der Entwickler

- Sensibilisierung aller Beteiligten für Sicherheitsbelange
- Die Schulungsmaßnahmen sollten unter anderem auch häufige Schwachstellen und Angriffsmöglichkeiten darstellen und praktikable Gegenmaßnahmen skizzieren. Die Schulung sollte inhaltlich Bezug nehmen auf die jeweils zu verwendenden Technologien, Programmiersprachen, Entwicklungswerkzeuge und -umgebungen.
- Schulungsmaterial kann in vielerlei Formen erstellt werden, so beispielsweise folgende:
 - Vortragsfolien-Satz
 - Online-Hilfe
 - Online-Tutorial
 - BeispielInstallation“ mit sinnvollen Beispielinhalten

Maßnahme:7 Architekturentwurf / Design / Grobkonzept / Feinkonzept

Im Rahmen der vorzunehmenden Arbeitsschritte Architekturentwurf, Design, Grobkonzept und Feinkonzept sollten stets die wichtigsten Sicherheitsziele Berücksichtigung finden. Es lassen sich verschiedene fundamentale Sicherheitsziele identifizieren, die insbesondere in der Designphase eines zu entwickelnden Systems entsprechend zu berücksichtigen sind. Diese Sicherheitsziele bringen zum Ausdruck, „was“ erreicht werden soll. Im Anschluss wird dann beschrieben, „wie“ dies erreicht werden soll. Für diesen Zweck werden einige fundamentale (Sicherheits-) Designziele formuliert.

- Sicherheitsziele
 - Identifizierung und Authentisierung
 - Zugriffskontrolle und Autorisierung
 - Beweissicherung und Nachvollziehbarkeit
 - Übertragungssicherung
 - Datenablagensicherung
 - Robustheit
- Weitere Ziele sind Integrität und Verfügbarkeit. Näheres hierzu findet sich in Folgeabschnitten

Maßnahme:7 (Fortsetzung) (Sicherheits-) Designziele

Die im folgenden aufgelisteten Designkriterien helfen dabei, die gewünschten Sicherheitsziele zu erreichen. Sie sind generisch formuliert und lassen sich daher praktisch immer anwenden.

- Einfachheit anstreben
- Anwendbarkeit / Usability
- Höchstmögliche Akzeptanz anstreben
- Wirtschaftlichsten Mechanismus anwenden
- Vollständige Offenlegung der Funktionsweise voraussetzen
- Sparsam mit Vertrauensbeziehungen agieren
- Protokollierung ermöglichen
- Fehlererkennung und -behebbarkeit anstreben
- Sicheren Zustand im Fehlerfall gewährleisten
- Datenintegrität sicherstellen
- Standardmäßige Abweisung praktizieren
- Patch- bzw. Updatefähigkeit unterstützen
- Geringst mögliche Privilegien zugestehen
- Bereichstrennung in Compartments erwägen
- Komplette Rechteprüfung durchführen
- Geringstmögliche gemeinsame Mechanismen und Ressourcen anstreben
- Verfügbarkeitsanforderungen im Design berücksichtigen

Maßnahme 8: Designspezifikation erstellen und mit Anforderungsspezifikation abgleichen

- Anforderungen, Planung, Vorgehensweise etc. sollten stets schriftlich dokumentiert werden
- Besonders in der Designphase ermöglicht dies einen systematischen Abgleich der Designspezifikation mit der zuvor erstellten Anforderungsspezifikation
- Zu diesem Zeitpunkt fallen etwaige Defizite am ehesten auf und erforderliche Änderungen an Funktionalität, Architektur o.ä. können noch berücksichtigt werden

Maßnahme 9: Aufbau einer geeigneten Entwicklungsumgebung

- Beschaffung externer Hard- und Software für die Entwicklungsumgebung
- Sicherheit der Entwickler-Arbeitsplätze / Saubere Trennung von Produktiv- und Testsystem

Für Entwickler-Arbeitsplätze gelten oftmals andere (Sicherheits-) Richtlinien als für Arbeitsplätze anderer Mitarbeiter. Für diese sind gleichwertige Sicherheitsvorkehrungen zu treffen. So muss beispielsweise ein funktionierendes, zeitnahes Backup vorhanden sein und unberechtigter Zugriff auf Code-Bestandteile muss verhindert werden.

Maßnahme 10: Implementierung: Häufige Implementierungsfehler vermeiden

Es ist unmöglich, alle oder auch nur die meisten Implementierungsfehler an dieser Stelle zu kategorisieren und aufzulisten. Dennoch werden nachfolgend einige häufige Quellen für Softwareschwachstellen benannt

- Buffer Overflows und verwandte Probleme
- Daten-Validierung (Input und Output)
- Debug Informationen vor Auslieferung aus Code entfernen
- Code Obfuscation erwägen
- Durchgriff auf Betriebssystem bzw. Shell und Absetzen unerwünschter Kommandos verhindern
- Austauschbarkeit von Kryptoalgorithmen unterstützen

Maßnahme 11: Aufbau einer geeigneten Testumgebung für die Systemumgebung, Tests

Systematisches Testen begleitet den gesamten System-Entwicklungszyklus, unabhängig von der praktizierten Entwicklungsmethode. Bereits die Anforderungs- und Designspezifikation kann (und soll) Tests unterzogen werden, wenngleich diese meist in Form einfacher Reviews erfolgen. Während der Implementierungsphase muss auf unterschiedlichen Ebenen getestet werden, insbesondere nicht erst „am Ende“.

Vor Beginn der Tests müssen zugehörige Prozesse aufgesetzt, die passende Testumgebung aufgebaut, und Ressourcen eingeplant werden. Dabei muss folgendes berücksichtigt werden:

- Testpläne müssen erstellt werden mit Vorgaben, was zu welchen Zeitpunkten in welcher Intensität mit welchem Qualitätsziel getestet werden muss. Die im Anforderungskatalog spezifizierte Sicherheitsfunktionalität sollte selbstverständlich zum Bestandteil der Testpläne gemacht werden.
- Codebestandteile, die neu bzw. modifiziert in die Codebasis eingestellt werden, müssen vorgegebene Tests durchlaufen, bestimmten Anforderungen genügen, und einer definierten (und praktikablen) Abnahmeprozedur unterliegen.

Maßnahme 11: (Fortsetzung)

- Jedes Stück Code muss eindeutig einer namentlich zu benennenden Person zugeordnet werden, die für zugehörige Tests und Qualität verantwortlich zeichnet.
- Die Gesamtheit der Codebestandteile muss von hierfür Verantwortlichen dahingehend getestet werden, welche neuen Probleme oder Schwächen sich im Zusammenspiel der getesteten Einzelkomponenten ergeben. Hierbei [\[TZ1\]](#) sollten insbesondere auch Schnittstellen zu anderen Systemen getestet werden, ferner sollten Performance- und Kapazitätstests durchgeführt werden. Die Tests sollten nicht nur die gewünschten bzw. geplanten Bedingungen, sondern auch plausible „Ausnahmesituationen“ berücksichtigen.
- Spezielle Testsysteme und Testumgebungen müssen bereitgestellt werden. Die Arbeitsstationen der Entwickler sind hierfür in den wenigsten Fällen ausreichend. Spätere Einsatzumgebungen müssen detailgetreu nachempfunden werden.
- Die Software muss auf allen für den Betrieb freigegebenen Plattformen getestet werden, insbesondere auch auf veralteten (aber noch unterstützten) Versionen (zum Beispiel alle Browsertypen (auch mit restriktiven Sicherheitseinstellungen) bei Webanwendungen, verschiedene Betriebssystemausprägungen und Releases mit/ohne Service Packs, und vieles mehr).
- Angebundene Systeme wie Datenbanken, Webserver, Applikationsserver, Autorisierungsserver, etc. müssen in unterschiedlichen Ausprägungen getestet werden.
- Vor Auslieferung muss anhand einer (gegebenenfalls nachgestellten) typischen Einsatzumgebung ein Penetrationstest stattfinden, der nach Möglichkeit von externen Spezialisten ausgeführt werden sollte.

Maßnahme 12: Auslieferung und Betrieb

- Eine frisch installierte Software, an der noch keine Konfigurationsanpassungen vorgenommen wurden, sollte ein akzeptables Sicherheitsniveau vorweisen. Diese Forderung bezeichnet man gelegentlich auch als „Secure by default“.
- Zusätzlich zu einem hinreichend sicheren Auslieferungszustand sollte auch eine Standardkonfiguration propagiert werden, die normalem Schutzbedarf gerecht wird. Diese Standardkonfiguration sollte idealerweise mit wenigen, angeleiteten Schritten aus dem Auslieferungszustand heraus zu erreichen sein, ohne sich zuvor ausgiebig mit beigefügter Dokumentation beschäftigen zu müssen.
- Ferner müssen in der beigefügten Dokumentation (und gegebenenfalls zusätzlich Online) Möglichkeiten beschrieben werden, wie eine Standardinstallation auf die eigenen Sicherheitsbedürfnisse hin angepasst werden kann. Sofern für den späteren Betrieb nur einige wenige, standardisierte Einsatzszenarien zu erwarten sind, so empfiehlt sich die Bereitstellung von Konfigurations-Templates und/oder -Beispielen, die auf diese Einsatzszenarien individuell zugeschnitten sind.

Maßnahme 13: Notfallvorsorge

- Datensicherung und Rekonstruktion:
 - Auf „normalen“ IT-Systemen (Arbeitsplatzrechner und Server) existieren in der Regel gut funktionierende Backup- und Recovery Mechanismen. Entwicklungssysteme sind jedoch in manchen Fällen nicht an das „reguläre“ Unternehmensnetz nebst Backup angeschlossen und bedürfen daher einer gesonderten Backup-Maßnahme. Diese muss frühzeitig geplant und regelmäßig auf Einhaltung und Funktionstüchtigkeit hin überprüft werden. In jedem Fall sollte eine Eingliederung in das reguläre Backup geprüft und präferiert werden.
- Aufbewahrung funktionstüchtiger früherer Entwicklungsumgebungen:
 - Diese Maßnahme erlaubt nicht nur die spätere Änderung (beispielsweise Fehlerbehebung) früherer Versionsstände. Bei auftretenden Problemen kann im Bedarfsfall auch die Korrektheit und Manipulationsfreiheit ausgelieferter Systeme überprüft werden.

Maßnahme 14: Datenschutzgerechte System-Entwicklung

Bei der Softwareentwicklung sollten die folgenden Entwicklungsprinzipien beachtet werden:

- Datensparsamkeit
- Transparenz sowie
- Kontrollmöglichkeiten für Benutzer.

Dabei bedeutet Datensparsamkeit, dass

- Datenschutz-Interessen bereits bei der Entwicklung neuer Systeme berücksichtigt werden,
- keine unnötigen (personenbezogenen) Daten erhoben werden,
- IT-Systeme so konzipiert werden, dass den späteren Benutzern eine anonyme oder pseudonyme Nutzung möglich ist,
- während der Nutzung angefallene (personenbezogene) Daten sobald wie möglich vernichtet werden. Wenn die Daten noch erforderlich sind, aber ein Personenbezug unverzichtbar ist, sollten sie möglichst anonymisiert oder pseudonymisiert werden.

Maßnahme 15: Makro-Software-Entwicklung durch Endbenutzer

Viele der bei Büroarbeitsplätzen eingesetzten Standardprogramme ermöglichen es den Benutzern, selbst Programme zu entwickeln, z. B. um sich Routinetätigkeiten zu erleichtern. Ein typisches Beispiel dazu ist die Makroprogrammierung unter Microsoft Word oder Access. Es ist zu bedenken,

- dass die Makro- bzw. Programmierer im allgemeinen keine geschulten Programmierer sind,
 - dass die Sicherheitsrichtlinien des Hauses beachtet werden sollten,
 - wie andere Benutzer davon profitieren können (und wer dann die Benutzerbetreuung übernimmt) und
 - wie die meist spontan erstellten Programme gepflegt und dokumentiert werden.
- ➔ Folglich müssen geeignete Regelungen erfolgen und die Anwender hierüber informiert werden.