TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

System Security Engineering für Manager

Entwicklung sicherer Systeme und sicherer Software

T.E.S.S.®
TeleTrusT Engineer System Security

Autoren

Birgitte Baardseth, isits AG International School of IT Security
Thomas Bleier, AIT Austrian Institute of Technology
Patrick Michaelis, AC – The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff
Marieke Petersohn, TeleTrusT – Bundesverband IT-Sicherheit e.V.
Markus Robin, SEC Consult Deutschland Unternehmensberatung
Christoph Weinmann, Secorvo Security Consulting

Diese Publikation wurde im TeleTrusT - Bundesverband IT-Sicherheit e.V. erarbeitet.

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
http://www.teletrust.de

Herstellung:

DATEV eG, Nürnberg

2. Auflage

1 Motivation

IT-Systeme umgeben uns auf Schritt und Tritt. Wo vor einigen Jahren noch menschliche Akteure oder analoge Maschinen dominierten, findet man heute digitale Steuerungen, Software-Anwendungen, Kleinstrechner, Apps, etc. Maschinen kommunizieren heute mit Maschinen, "Industrie 4.0" soll in die Fabriken Einzug halten, mächtige Webanwendungen beherrschen das World Wide Web, das Internet der Dinge wird sprachlich schon zum Internet of Everything und wir sprechen von Cyber Physical Systems.

Doch warum sollte Sicherheit in all diesen Systemen und Applikationen eine Rolle spielen? Und wenn Sicherheit eine Rolle spielen sollte, welches Niveau an Sicherheit ist mindestens notwendig? Und warum betrifft das Thema jedes Unternehmen, das (IT-)Systeme nutzt, kauft oder verkauft?

Betrachten wir exemplarisch einen Vorfall aus dem Jahr 2013. Der deutsche Hersteller einer hochmodernen Heizanlage hatte sein Produkt mit einer Webanwendung für den Anwender und die Servicetechniker ausgestattet. Diese zusätzliche Funktionalität auf dem Weg zur "smarten" Heizung stellte sich jedoch im Betrieb als mögliche Schwachstelle für den Angriff durch kriminelle Computerhacker dar. Denn in der Software verbarg sich ein Sicherheitsproblem, das relativ einfach den Zugang zu den Klartext-Passwörtern der Anlage für den Fernzugriff erlaubte. Ein Hacker mit entsprechenden IT-Kenntnissen hätte dann die Heizanlage an- und ausschalten oder die Sollwerttemperaturen verändern können.

Von den Medien werden solche Sicherheitsmängel mit Interesse aufgenommen, verbreitet und durchaus auch dramatisiert. Daher sollten schon allein wegen des möglichen Vertrauensverlustes beim Endkunden solche Schwachstellen vermieden werden.

Doch was geschieht, wenn Konsumenten ein Schaden durch nachweisbar unsichere Systeme und Anwendungen entsteht? Wird eine Produkthaftung schlagend oder ist ein Rückruf notwendig? Welche Konsequenzen hat der Ausfall eines Systems bei Ihren B2B-Kunden durch Hacker-Angriffe auf Ihren Umsatz und Ihren Vorsprung auf den Mitbewerb? Akzeptieren Ihre Kunden die Auslieferung von Systemen und Anwendungen, die nicht nachweisbar sicher sind? Welche unsicheren Systeme können in Ihrem Unternehmen zu einer Betriebsunterbrechung führen? Wie weit sind Ihre Sublieferanten mit der Härtung der gelieferten IT-Systeme und Software?

In der Praxis gibt es gravierende Unterschiede zwischen der (implizit von Lieferanten) versprochenen Sicherheit und der realen Sicherheitsreife. Neben der steigenden Sensibilität beim Unternehmenskunden fordern auch gesetzliche Mindeststandards Sicherheit von Systemen und Software.

Die Entwicklung sicherer Systeme und Software wird in Zukunft immer mehr ein Qualitätskriterium werden. Nicht nur werden die Systeme dadurch per se sicherer, sondern der Gesamtprozess und die Gesamtqualität der Produktentwicklung werden gestärkt.

TeleTrusT ermöglicht mit dem T.E.S.S. (TeleTrusT Engineer for System Security) den Nachweis spezieller Qualifikation für die Gestaltung von sicheren Systemen. Der erste wichtige Schritt für die nachhaltige Verankerung der Sicherheit und Entwicklung in Ihrem Unternehmen. Nutzen Sie den Wettbewerbsvorteil durch sichere Systeme schon jetzt.

2 Begriffsbestimmung

System Security Engineering ist eine spezielle Disziplin des System Engineering und nutzt dessen hohen Erfahrungsschatz. System Security Engineering ermöglicht es, Systeme zu bauen, die trotz bösartiger Angriffe ihre Aufgaben erfüllen können[1]. Dazu ist es notwendig, über einen systematischen, ingenieurwissenschaftlichen Ansatz bewährte Prinzipien und Konzepte aus dem Security Engineering im gesamten Lebenszyklus von Systemen einzusetzen, damit diese trotz anhaltender Bedrohungen und Störungen dem notwendigen Schutzbedarf gerecht werden.

Ein **System** besteht aus mehreren **Komponenten**, die über **Schnittstellen** miteinander interagieren. Die Sicherheitseigenschaften des Gesamtsystems ergeben sich aus den Sicherheitseigenschaften der Einzelkomponenten, aller Schnittstellen und der Interaktion aller Komponenten. Die Komponenten haben sehr unterschiedliche Ausprägungen, z.B. Hardware, Software, Personen, Prozesse usw.

Der **Lebenszyklus** von Systemen erstreckt sich von der Konzeption über die Entwicklung und Inbetriebnahme der Systeme bis hin zur Stilllegung von Systemen. Sicherheitsbetrachtungen müssen diesen gesamten Lebenszyklus mit einbeziehen, da

[1] Anderson, R.: Security Engineering, 2nd. Ed

beispielsweise bei der Entwicklung eingebaute Sicherheitsmechanismen möglicherweise bei der Inbetriebnahme auch aktiviert und im Betrieb überwacht werden müssen.

Systeme können einen unterschiedlichen **Schutzbedarf** aufweisen. Dieser ist nicht nur vom System selbst, sondern insbesondere von den Anforderungen, die z. B. externe Stakeholder an das System stellen, abhängig. Die wichtigsten Kategorien für den Schutzbedarf eines Systems sind die **Vertraulichkeit**, die **Integrität** und die **Verfügbarkeit** des Systems. Daneben gibt es noch abgeleitete Schutzziele wie die Authentifizierbarkeit von Akteuren, die Nachvollziehbarkeit bzw. Nicht-Abstreitbarkeit von Aktivitäten oder die Autorisierung der Nutzer eines Systems.

Da nicht beliebig viele Sicherheitsmaßnahmen und beliebig hohe Sicherheitsniveaus umgesetzt werden können, ist eine **Risikoanalyse** ein wesentliches Element jeder Sicherheitsbetrachtung. Aufgrund möglicher **Verwundbarkeiten** bzw. potenzieller Schwachstellen eines Systems und der **Bedrohungen**, die diesem System entgegenstehen erfolgt eine Priorisierung der Maßnahmen zur Sicherstellung eines adäquaten Sicherheitsniveaus.

Bewährte **Design-Prinzipien** aus dem Security-Engineering sind beispielsweise[2] die Verwendung von sicheren Standardeinstellungen (Fail-safe defaults), die Reduktion von Komplexität (Economy of mechanism), die Aufteilung von Zugriffsprivilegien (Separation of privilege), die vollständige Zugriffskontrolle (Complete mediation), nicht darauf zu vertrauen, dass die Funktion von Sicherheitsmechanismen nicht bekannt wird (Open design), die Reduktion auf die unbedingt notwendigen Zugriffsprivilegien (Least privilege), der Verzicht auf die gemeinsame Verwendung von Sicherheitsmechanismen für unterschiedliche Aufgaben (Least common mechanism) und die Sicherstellung der psychologischen Akzeptanz von Sicherheitsmechanismen (Psychological acceptability).

[2] Saltzer, J and Schroeder, M: The Protection of Information in Computer Systems

3 Wie sicher ist der System-Engineering-Prozess bei Ihnen?

Der erste Schritt zur Entwicklung sicherer Systeme sind konzeptionelle Überlegungen. Im Folgenden finden Sie Anregungen, um den Status Quo in Ihrem Unternehmen herauszufinden. Betrachten Sie ein System, das Sie entwickeln oder beschaffen wollen und beantworten Sie folgende Fragen:

1. In welche Phasen des Lebenszyklus des zu entwickelnden Systems haben Sie Sicherheitsaspekte integriert?

Konzeption	Entwicklung	Produktion	Betrieb	Stilllegung
☐	☐	☐	☐	☐

2. Welche Komponenten/Schnittstellen werden in Ihrem aktuellen Systemmodell bezüglich ihrer Sicherheitsrelevanz betrachtet?
(Markieren Sie die zutreffende Ausprägung)

	0 %	25%	50%	75%	100%
Interne Komponenten/Schnittstellen					
Externe Komponenten/Schnittstellen					
Eigenentwickelte Komponenten/Schnittstellen					
Zugekaufte/Open-Source-Komponenten/Schnittstellen					
Alle Komponenten/Schnittstellen					

3. Für welche Komponenten und Schnittstellen existiert ein aktuelles Bedrohungsmodell?

	0 %	25%	50%	75%	100%
Interne Komponenten/Schnittstellen					
Externe Komponenten/Schnittstellen					
Eigenentwickelte Komponenten/Schnittstellen					
Zugekaufte/Open-Source-Komponenten/Schnittstellen					
Alle Komponenten/Schnittstellen					

4. Für welche Phase des Lebenszyklus sind in Ihrem System sicherheitsrelevante Anforderungen unverzichtbar?

Konzeption	Entwicklung	Produktion	Betrieb	Stilllegung
☐	☐	☐	☐	☐

5. Wie weisen Sie die Sicherheit Ihres Systems nach und woher ziehen Sie diese Informationen?

	0 %	25%	50%	75%	100%
Interne Komponenten/Schnittstellen					
Externe Komponenten/Schnittstellen					
Weiß nicht					

Statusinformation durch:

- ☐ Evaluationen/ Audits
- ☐ Prozessdefinitionen
- ☐ Testergebnisse
- ☐ Andere:

6. Wie viele Ihrer Mitarbeiter haben sich nachweislich im letzten Jahr im Bereich System Security Engineering weitergebildet?

<30%	<50%	<70%	100%	Weiß nicht
☐	☐	☐	☐	☐

Weitere Notizen:

4 Empfehlungen

Zur 1. Frage **Lebenszyklus**: Sicherheit ist ein integrierter Bestandteil des gesamten Lebenszyklus. Auch Betrieb und Stilllegung besitzen ganz spezifische Sicherheitsanforderungen mit Schussfolgerungen. Wenn Sie alle Phasen angekreuzt haben, sind Sie gut beraten.

Zur 2. Frage **Sicherheitsrelevanz**: Eine vollständige Betrachtung aller Komponenten und Schnittstellen bezüglich ihrer Sicherheitsrelevanz ist anzustreben. Dabei ist es entscheidend zu wissen, welche Komponenten mit welchen sicherheitsrelevanten Annahmen verwendet werden. Alle Annahmen sind zu validieren. Beispiel: Die Entwickler von SSL-Applikationen nutzen SSL-Bibliotheken unter der impliziten Annahme, dass sie fehlerfrei sind. Dies ist eine Fehlannahme. Die fehlende Validierung eröffnet Angriffsmöglichkeiten, die regelmäßig genutzt werden.

Zur 3. Frage **Bedrohungsanalyse**: Alle Systemelemente müssen einem Sicherheits-Risikomanagement unterworfen werden, um zuverlässig Aussagen über ihre Sicherheitsrelevanz machen zu können. Zum Sicherheits-Risikomanagement gehören Schutzbedarfsanalyse, Bedrohungsanalyse und Schwachstellenanalyse, kombiniert mit der Anforderungsanalyse

Zur 4. Frage **Anforderungsanalyse**: Für ein sicheres System ist es wichtig die sicherheitsrelevanten Anforderungen in allen Phasen des Lebenszyklus zu definieren. Wir können so das System effektiver schützen und deutlich Kosten sparen. Die Betriebsphase ist die längste und kostenintensivste Phase eines Systems. Hier ist die Feststellung der sicherheitsrelevanten Anforderungen besonders wichtig. In der Realität wird sich aber nur sehr selten darum gekümmert.

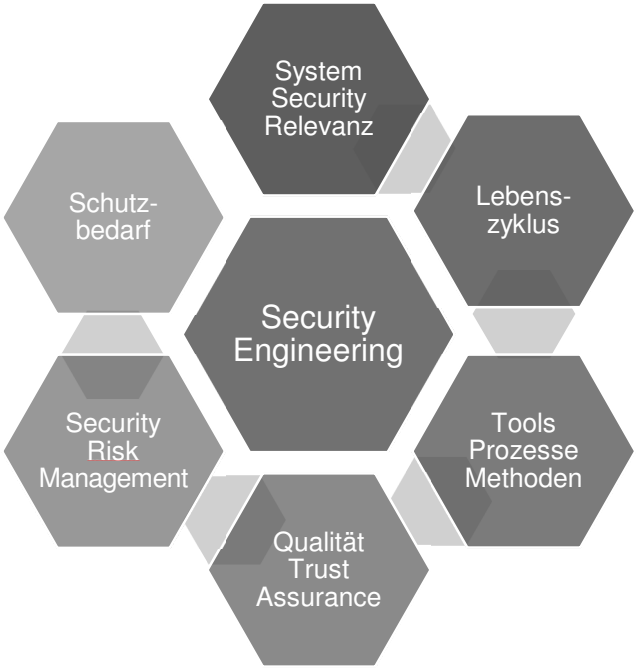
Zur 5. Frage **Assurance und Vertrauen**: Sowohl formalisierte Entwicklungsprozesse (z. B. Secure Development Lifecycle) für alle sicherheitsrelevanten Systemelemente entsprechend der Risikobetrachtung als auch umfängliches Testen und Evaluieren ermöglichen Aussagen über die Sicherheitsqualität eines Systems. Diese Aussagen sind die Basis für Assurance und Vertrauen in das System. Assurance bedeutet: System Security Engineering bringt messbaren Schutz, der imstande ist, den beabsichtigten Schutz zu garantieren, trotz Fehlern, Defekten, Katastrophen und vorsätzlichen Angriffen.

Zur 6. Frage **Weiterbildung**: Sicherheit wird nicht nur von Sicherheitsexperten eingebaut, sondern jede Ebene von der Entwicklung bis zum Betrieb ist an der Implementierung der Sicherheit beteiligt (z. B. auch Architekten, SW-Entwickler, HW-Entwickler, Tester, Projektmanager). Eine gute Zusammenarbeit ist wichtig für den Erfolg, wie auch die angemessene Weiterbildung aller Beteiligten.

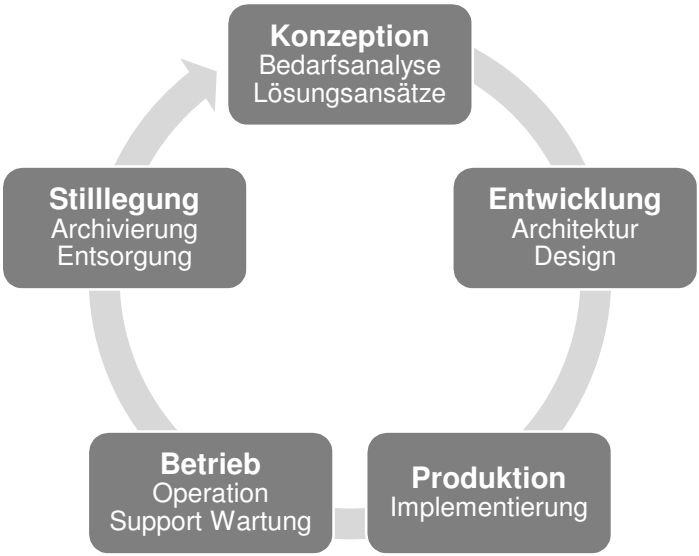
5 Fazit

Wird System Security Engineering in einem Entwicklungsprozess kontinuierlich eingesetzt, kann ein effizienterer Schutz des Systems erreicht werden bei gleichzeitiger Kostensenkung in der Gesamtkalkulation. Ein wichtiger Faktor dafür ist der Überblick über das gesamte System mit allen Komponenten und Schnittstellen, der durch die ganzheitliche Sicht auf das System entsteht. Dies ermöglicht es ein Security Risk Management mit einem strukturierten Threat & Vulnerability Assessment über das gesamte System zu etablieren. Der Schutzbedarf kann umfassend festgestellt werden und dient als Motor, um die Umsetzung von Sicherheitsmaßnahmen voranzutreiben. Mit gezielten Maßnahmen wird Sicherheit in die Prozesse des gesamten Lebenszyklus eines Systems integriert. Es wird ein System-Design geschaffen, das begründetes Vertrauen in ein System erzeugt, obwohl es Bedrohungen und Störungen ausgesetzt ist. Dies schließlich ist eine gute Grundlage für eine stabile hohe Kundenzufriedenheit.

Weitere hilfreiche Informationen finden Sie auf www.teletrust.de/tess.



Konzept des System Security Engineering



Der System-Lebenszyklus

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Engineer for System Security" (T.E.S.S.) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de


TeleTrusT
Pioneers in IT security.