IT-Sicherheitsanalysen von PLM-Systemen

Maximilian Janik · Kristin Weber

Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt
maximilian.janik@student.fhws.de
kristin.weber@fhws.de

Zusammenfassung

Webbasierte Product Lifecycle Management (PLM) Systeme werden von vielen Unternehmen der Automobilbranche eingesetzt. Es sind meist stark integrierte Systeme, die sensible Produktdaten vorhalten und wichtige Funktionen rund um die Planung und Entwicklung von Produkten abbilden. Da es bei der Einführung von PLM-Systemen hauptsächlich um Effizienzsteigerungen geht, spielen Überlegungen zur IT-Sicherheit meist nur eine untergeordnete Rolle. Diese Arbeit bietet ein Konzept das zeigt, wie Unternehmen bereits produktiv eingesetzte PLM-Systeme nach Schwachstellen untersuchen können. Im Vorfeld wurde das hier vorgestellte Konzept bei einem deutschen Automobilzulieferer angewandt.

1 Motivation

Im Zuge einer Anfang 2015 durchgeführten Bitkom Studie wurden gut 1.000 Führungskräfte, die für das Thema Wirtschaftsschutz verantwortlich sind, gefragt, ob ihr Unternehmen in den vergangenen zwei Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen war. Die Ergebnisse wurden nach Branche sortiert. Der Automobilbau stand dabei mit 68% „Ja“-Antworten an der Spitze [Bitk15]. Auch die IT-Systeme und Anwendungen des als Fallbeispiel dienenden deutschen Automobilzulieferers (vgl. Abschnitt 3.3.1) sind regelmäßigen Angriffen in unterschiedlicher Schwere sowohl von innen als auch von außen ausgesetzt. Die Zuhilfenahme von externen IT-Sicherheitsexperten war dort bereits in schwerwiegenden Fällen notwendig.

PLM-Systeme sind meist stark integrierte Systeme. Sie bilden das Herzstück des Produktlebenszyklus und weisen viele Schnittstellen zu anderen Systemen auf, wie zum Beispiel Office-Programmen, CAD- und ERP-Systemen. Auch Anforderungen von Kunden kommen über das Anforderungsmanagement in das System. In einem hauptsächlich produzierenden Betrieb, in dem das PLM-System einen hohen Durchdringungsgrad hat, fließen nahezu alle produktionsrelevanten Daten durch ebendieses [EiSt13, S. 253].

PLM-Systeme sollten also möglichst sicher sein, um die Unternehmenswerte, wie z.B. Produkt- und Produktionsdaten oder Patente, ausreichend zu schützen. Bevor konkrete Maßnahmen ermittelt werden können, um das System abzusichern, muss zunächst einmal festgestellt werden, wie sicher es bereits ist. Eine IT-Sicherheitsanalyse kann genau das bewerkstelligen.

Praktisch umsetzbare Konzepte, welche die IT-Sicherheit von PLM-Systemen adressieren, sind allerdings kaum zu finden. Hauptsächlich handelt es sich um Literatur, die auf abstrakter Ebene versucht, die unternehmensübergreifende Verteilung von PLM-relevanten Daten sicherer zu

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 202-213.

gestalten [RaBh13] oder sich grundsätzlich um die IT-Sicherheit bei der Zusammenarbeit von Unternehmen kümmert [Heit07]. Ziel dieses Beitrags ist es daher, gängige Konzepte zur Sicherheitsanalyse von IT-Systemen auf deren Eignung für PLM-Systeme zu untersuchen und ein anwendbares Konzept zur IT-Sicherheitsanalyse für PLM-Systeme vorzuschlagen.

2 Grundlagen

Eine IT-Sicherheitsanalyse soll feststellen, ob ein System die Schutzziele der IT-Sicherheit (Integrität, Vertraulichkeit, Verfügbarkeit) erreicht. Das bedeutet, dass es gegen unbefugte Zugriffe und Manipulationen gewappnet ist und dabei auch verfügbar bleibt. Gleichzeitig muss die Analyse feststellen, ob Aktivitäten auf dem System ausreichend protokolliert und genügend Schutz während der Speicherung, Verarbeitung und Übertragung der Daten gewährleistet wird [Kapp13, S. 2]. Im Anschluss an die Analyse, kann die Sicherheit des Systems qualitativ (z.B. „ausreichend“ oder „ungenügend“) oder quantitativ (z.B. 0 bis 10) bewertet werden.

2.1 Product Lifecycle Management im Kontext Sicherheit

Product Lifecycle Management ist ein Ansatz „zur ganzheitlichen, unternehmensweiten Verwaltung und Steuerung aller Produktdaten und Prozesse des gesamten Lebenszyklus – von der Entwicklung und Produktion über den Vertrieb bis hin zur Wartung. Ziel dabei ist es, den Produktentstehungsprozess durch Datenmanagement zu unterstützen und die Entwicklungsproduktivität zu erhöhen.“ [Schu15] Eigner und Stelzer charakterisieren den Produktlebenszyklus noch etwas genauer: „Der Produktlebenszyklus ist ein Kernprozess von Industrieunternehmen. [...] [Er] umfasst die komplette Planung und Entwicklung von Produkten und ihren zugehörigen Betriebsmitteln, Ressourcen, Fertigungs- und Montageprozessen, deren Herstellung sowie Nutzung, Betrieb und Recycling.“ [EiSt13, S. 9] PLM-Systeme spielen eine wesentliche Rolle bei der Umsetzung des PLM-Ansatzes.

Abbildung 1 veranschaulicht, wie ein PLM-System in der IT-Landschaft eines Unternehmens üblicherweise eingebettet ist. Durch diese zentrale Positionierung ist die Sicherheit von PLM-Systemen und der damit verwalteten Daten für Unternehmen essenziell. Hat eines der angebundenen Systeme die Möglichkeit, unerlaubte Aktionen auszuführen und PLM-Daten zu lesen oder gar zu ändern, oder ist das PLM-System selbst angreifbar, sind unter Umständen alle anderen verbundenen Systeme mitbetroffen. Kann zum Beispiel ein CAD-System beliebige Produktdaten im PLM-System löschen und verursachen, dass diese Löschung an die ERP-Systeme weitergereicht wird, kann das erhebliche Probleme bis hin zum Produktionsstopp nach sich ziehen.

Aber nicht nur eine Manipulation der Daten (Verletzung der Integrität) kann immense Auswirkungen haben. Eigner und Stelzer betonen vor allem die Bedeutung des Zugriffsschutzes, also des Schutzes vor rein lesendem Zugriff (Verletzung der Vertraulichkeit, Stichwort Produktpiraterie) [EiSt13, S. 333]. PLM-Systeme speichern und verwalten produktrelevante Dokumente, Informationen zum Entwicklungsstand und die Historie von Produkten. Interner und vor allem externer Zugriff, zum Beispiel durch Partnerunternehmen über das Internet, muss durch Berechtigungen innerhalb der Anwendung stark reguliert werden, um einen unbefugten Informationsabfluss zu vermeiden.

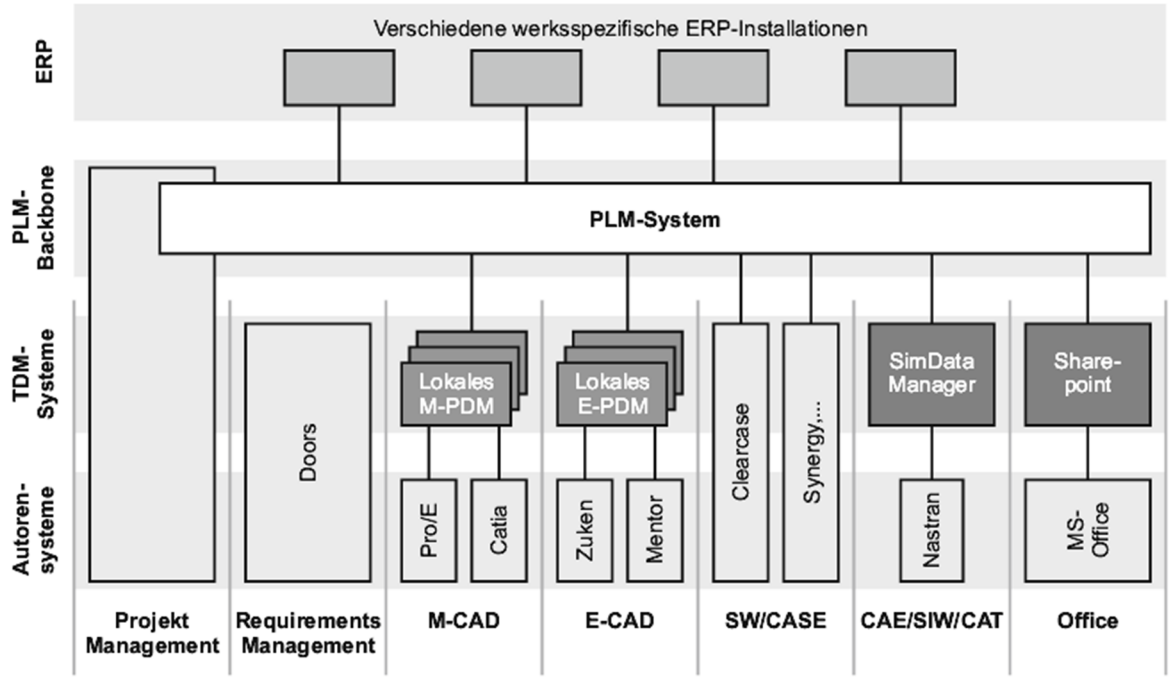

Abb. 1: Typisches vierstufiges Architekturkonzept [EiSt13, S. 43]

Genauso wie die Sicherstellung der Vertraulichkeit und der Integrität, ist die Sicherstellung der Verfügbarkeit von großer Bedeutung. Ein Ausfall des PLM-Systems von nur kurzer Zeit kann aufgrund dessen Einsatzes zur Prozesssteuerung hohe Kosten verursachen. Im Extremfall steht die Produktion aufgrund von fehlenden Daten still. Daher muss gewährleistet werden, dass das System stabil läuft und die verwalteten Daten stets verfügbar bleiben, bestenfalls auch bei einem Anwendungsausfall. [EiSt13, S. 343f]

Die hier betrachteten webbasierten PLM-Systeme basieren grundsätzlich auf der Client-Server-Architektur. Wie genau sie aufgebaut ist, variiert von System zu System. Abbildung 2 zeigt die Architektur des webbasierten PLM-Systems PTC Windchill exemplarisch. Die Architektur besteht aus Clients, wie zum Beispiel einem Webbrowser oder einem CAD-Tool, und einem Webserver, der die Anfragen der Clients annimmt, verarbeitet und an den Application Server weitergibt. Darüber hinaus besteht sie aus Datenhaltungssystemen wie den Vaults, die als externe Dateiablagen dienen, einem Verzeichnisdienst, wie zum Beispiel einem LDAP-Server und einem Datenbankserver. Alle diese Komponenten gilt es abzusichern.

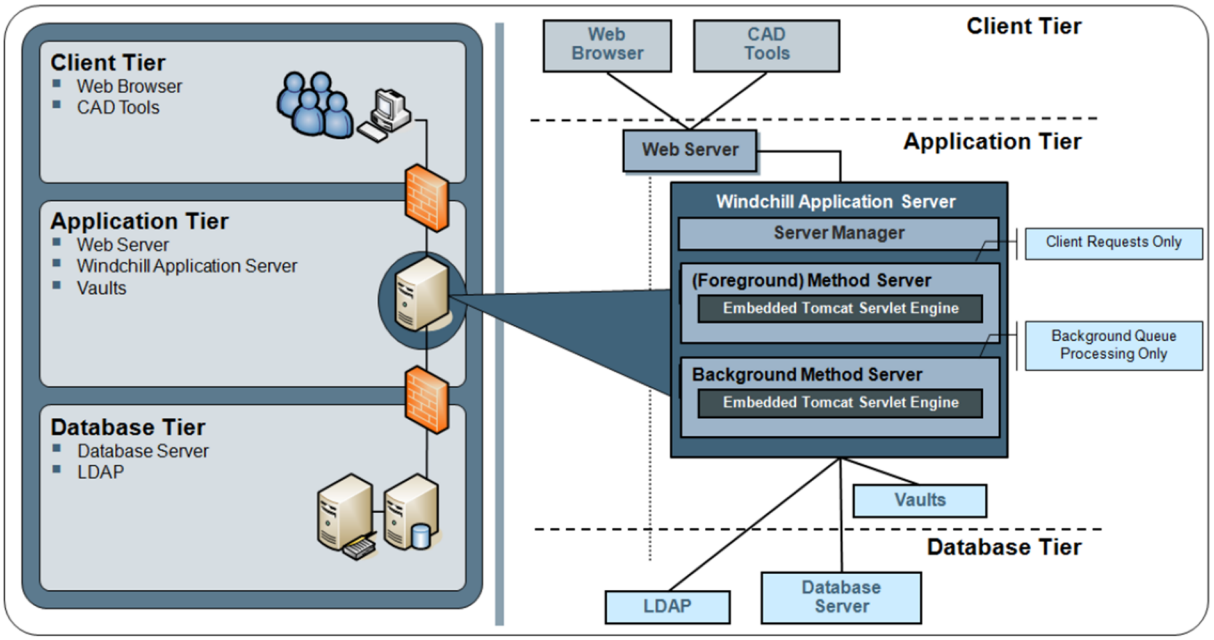

Abb. 2: „Multi-tier"-Architektur von PTC Windchill [PTC14]

2.2 Methoden zur Sicherheitsanalyse von PLM-Systemen

Im Bereich der IT-Sicherheit gibt es viele verschiedene Normen und Standards. Bei der Wahl geeigneter Sicherheitsanalyse-Methoden für PLM-Systeme sollten zunächst nationale Vorgaben berücksichtigt werden. Der Verband der Automobilindustrie (VDA) empfiehlt für den Informationsschutz die direkte Umsetzung der ISO/IEC 27000 Familie [VDA05]. Die ISO/IEC 27000 Familie ist ein internationaler Standard, der sich mit dem Aufbau und der Erhaltung eines Information Security Management Systems (ISMS) beschäftigt [Klip15, S. 38]. Der VDA ergänzt seine Empfehlungen um den Prototypenschutz. Darin werden Richtlinien für den korrekten Umgang mit Prototypen vorgestellt. Da es in diesem Beitrag nicht um den Schutz (z.B. durch Tarnung) von Prototypen geht und auch kein ISMS analysiert werden soll, kommen die Anforderungen der VDA hier nicht zum Tragen.

Die Standards 100-1 bis 100-3 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientieren sich an der ISO/IEC 27000 Familie, um eine möglichst breite Anerkennung der Zertifizierung nach IT-Grundschutz zu gewährleisten [KeKl15, S. 5]. Der IT-Grundschutz Basis-Sicherheitscheck bietet ein systematisches Vorgehen, um das erreichte Sicherheitsniveau eines „Zielobjektes“ – beispielsweise eines PLM-Systems mit seinen Komponenten und Schnittstellen – zu identifizieren und Verbesserungsmöglichkeiten aufzuzeigen [BSI11, S. 62]. Die Common Criteria (CC) stellen den internationalen de-facto Standard zur Bewertung von IT-Sicherheit in Produkten dar und haben sich aus den nationalen Standards vieler Länder heraus entwickelt. Der OWASP-Testing Guide beschäftigt sich speziell mit der Sicherheitsanalyse von Webanwendungen. OWASP[1] (Open Web Application Security Project) ist eines der bekanntesten internationalen Projekte, die sich mit der Sicherheit von Webanwendungen beschäftigen und beeinflusst sogar den Data Security Standard der Payment Card Industry [Ecke14, S. 166f]. Diese drei Methoden werden im Folgenden vorgestellt.

[1] www.owasp.org

Common Criteria

Die „Common Criteria for Information Technology Security Evaluation“, kurz CC, sind übersetzt gemeinsame Kriterien zur Prüfung und Bewertung der Sicherheit von Informationstechnik. Sie sind weltweit anerkannt und haben sich aus verschiedenen nationalen Standards, wie zum Beispiel dem deutschen „Grünbuch“ von 1989, heraus entwickelt. Die erste Version der CC wurde 1996 veröffentlicht. 2006 wurde die Version 2.3 von der ISO als internationaler Standard ISO 15408 anerkannt. [Ecke14, S. 236f]

Die CC sind ein sehr flexibler Standard. Ein zu untersuchendes Zielsystem kann eine Software, eine Firmware, eine Hardware oder eine Kombination daraus sein. Es kann ein fertiges Produkt, ein bereits konfiguriertes und eingesetztes IT-System oder gar nur einen Prototyp darstellen. Man kann frei entscheiden, was Teil der Evaluation sein soll. [CCEB12c, S. 32f]

Die CC unterscheiden grundsätzlich zwischen einer funktionalen Prüfung von IT-Sicherheit und der Prüfung des Vertrauens in die Umsetzung der funktionalen Anforderungen. Anwender bzw. Kunden können aus einer Sammlung an Anforderungen produktunabhängige Schutzprofile anlegen, die genau die Sicherheitsfunktionalität und Vertrauenswürdigkeit fordern, die der jeweiligen Bedrohungslage und dem Wert der zu schützenden Daten angemessen sind. [Ecke14, S. 237f]

OWASP Testing Guide

Der „OWASP Testing Guide“ setzt sich mit der Analyse von Webanwendungen auseinander. Dabei handelt es sich um eines der Flaggschiff-Projekte des OWASP, welches gemeinsam mit dem „Code Review Guide“ und dem „Development Guide“ ein Anleitungspaket bietet, mit dem das OWASP versucht, unsichere Webanwendungen zur Ausnahme zu machen [MeMu15, S. 5]. Der Testing Guide bildet dabei eine Richtlinie, die beschreibt, wie Webanwendungen nicht nur nach der Entwicklung, sondern über den gesamten Software Development Lifecycle (SDLC) hinweg, auf Schwachstellen getestet werden sollten.

IT-Grundschutz Basis-Sicherheitscheck

Die BSI-Standards bieten eine ganze Reihe an Empfehlungen „zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit“ [BSIod]. Der Basis-Sicherheitscheck ist eine Methode, um bereits umgesetzte Maßnahmen zur IT-Sicherheit eines Systems mit den Anforderungen aus den IT-Grundschutz-Katalogen zu vergleichen. Er setzt voraus, dass bereits eine Strukturanalyse des Systems erstellt, eine Schutzbedarfsanalyse und anschließend eine Modellierung nach IT-Grundschutz durchgeführt wurde [BSI08, S. 65f]. Letztere liefert den Prüfplan für einen Soll-Ist-Vergleich [BSI08, S. 61]. Die IT-Grundschutz-Kataloge zeichnen sich durch einen enorm hohen Detailgrad aus. Es gibt zu nahezu jedem allgemeinen Typ von System oder Anwendung Maßnahmen, um sie sicher zu planen, anzuschaffen und zu betreiben.

3 Konzept der IT-Sicherheitsanalyse

3.1 Anforderungen

Das Konzept soll nicht die Installation und Konfiguration eines PLM-Systems begleiten, sondern die bestehende Installation eines PLM-Systems analysieren, welches bereits konfiguriert und seit längerer Zeit betrieblich genutzt wird. Die Analyse ergibt, ob das System primär technisch und optional auch organisatorisch den Standards der IT-Sicherheit entspricht. Die vom

Unternehmen konfigurierten Rollen und Berechtigungen auf Anwendungsebene werden dabei nicht betrachtet.

Nähert man sich der IT-Sicherheit von webbasierten PLM-Systemen aus technischer Sicht, sind primär die üblichen Sicherheitsprobleme von Webanwendungen zu prüfen. Dieser Beitrag geht von einer grundsätzlich sicheren Infrastruktur im Unternehmen aus. Dazu zählt, dass ein Angreifer keine Kontrolle über das Netzwerk hat, d. h. keine Nachrichten lesen, verändern, löschen oder hinzufügen kann. Das Betriebssystem, welches normalerweise nicht Teil einer Sicherheitsanalyse von Webanwendungen ist [Goll11, S. 342], soll hingegen in diesem Beitrag Beachtung finden. Typische Bedrohungen von Webanwendungen, wie zum Beispiel der Session-Diebstahl, SQL-Injection, Cross Site Scripting (XSS) oder Cross Site Request Forgery (CSRF) sollen von der Sicherheitsanalyse ebenso beachtet werden.

Ein PLM-System wird üblicherweise bei der Einführung an die Bedürfnisse des jeweiligen Unternehmens angepasst [EiSt13, S. 408]. Die Kosten für die IT-Sicherheitsanalyse eines solchen Systems müssen einem entsprechenden Nutzen entgegenstehen [Heit07, S. 29]. Ihr Umfang sollte also zum Beispiel je nach Durchdringungsgrad des Systems und Brisanz der gespeicherten Daten angepasst werden. Werden zum Beispiel nur CAD-Dokumente im PLM-System versioniert, während gleichzeitig lokale Kopien vorhanden sind, ist die Analyse der Anbindung wesentlich weniger kritisch, als wenn Entwickler auf das System angewiesen sind, um überhaupt arbeiten zu können.

Das nachfolgend beschriebene Konzept einer IT-Sicherheitsanalyse geht davon aus, dass Unternehmen, die bereits ein PLM-System einsetzen, keine externe Zertifizierung anstreben. Die drei vorgestellten Methoden werden im Konzept so verarbeitet, dass die Schwachstellensuche möglichst effizient, also schnell und kostengünstig, abläuft.

3.2 Eignung der vorgestellten Methoden

Alle drei vorgestellten Methoden, die zur Analyse und Bewertung der IT-Sicherheit eines PLM-Systems dienen sollen, haben ihre Vor- und Nachteile. So bilden die CC einen umfangreichen Standard, um IT-Systeme jeglicher Art zu validieren und bieten feste Sicherheitsstufen an, um die Vertrauenswürdigkeit greifbar zu machen. Die CC werden momentan allerdings hauptsächlich von der Smart Card Industrie oder von Herstellern von IT-Systemen, welche für Einrichtungen der Regierungen arbeiten, verwendet, da diese eine Zertifizierung nach CC fordern [Goll11, S. 247]. Eine solche Zertifizierung ist aufwendig und eine Re-Evaluation wird bei Weiterentwicklungen, Anpassungen oder Schnittstellen verlangt. Die CC erheben keinerlei PLM-spezifische Anforderungen; auch Webanwendungen werden nicht direkt adressiert. Um den Aufwand für eine Analyse nach den CC gering zu halten, könnte man sich für eine geringere Sicherheitsstufe entscheiden. Dadurch würden aber weniger Sicherheitsprobleme gefunden werden und es entstünde keine wirklich belastbare Aussage zur Vertrauenswürdigkeit der Anwendung. [Goll11, S. 248]

Der OWASP Testing Guide ist speziell auf das Testen von Webanwendungen ausgelegt. Der Guide beschreibt spezifische Anforderungen an die Sicherheit von Webanwendungen und Methoden, um diese zu testen. PLM-Systeme betrachtet der Testing Guide nicht explizit; ebenso wenig wie webbasierte Schnittstellen und die Konfiguration von Webservern und Betriebssystemen. Viele der Anforderungen sind nicht auf ein sich bereits im Betrieb befindliches PLM-System anwendbar, sondern beziehen sich auf die Planung und Entwicklung von Anwendungen.

Der IT-Grundschutz Basis-Sicherheitscheck bietet detaillierte Anforderungen für alle Komponenten einer IT-Landschaft. Viele Aspekte eines PLM-Systems, also zum Beispiel Betriebssystem, Webserver, Webanwendung oder Webservice werden beschrieben. Aus den Maßnahmen der IT-Grundschutz-Kataloge müssen nur diejenigen ausgewählt werden, die auf das Szenario passen. Spezielle Anforderungen von PLM-Systemen werden aber nicht exakt abgebildet, was bedeutet, dass weitere Maßnahmen speziell für PLM-Systeme entwickelt und geprüft werden müssten. Aufgrund sehr detaillierter Anforderungen ist der Aufwand zur Prüfung aller relevanten Maßnahmen enorm. Vom Basis-Sicherheitscheck gestellte Anforderungen an die sichere Planung, Beschaffung und Umsetzung der Komponenten sind im Fall eines produktiven PLM-Systems nicht relevant.

Alle drei Methoden sind mit einigem Aufwand verbunden, sofern man sie unverändert durchführen will. Alle drei verlangen zum Beispiel eine Risikoanalyse und erwarten Penetrationstests sowie das Beachten von Policies, die vom Unternehmen aufgestellt wurden. Zusammengenommen enthalten die einzelnen Methoden viele Aspekte, die auf die Sicherheitsanalyse eines PLM-Systems anwendbar sind. Ziel des nächsten Kapitels ist es, diese Aspekte in einem neuen Konzept zu vereinen.

3.3 Ablauf der IT-Sicherheitsanalyse

3.3.1 Überblick und Fallbeispiel

Die IT-Sicherheitsanalyse eines PLM-Systems erfolgt in vier Schritten und kann einmalig, oder periodisch in einem wählbaren Intervall (bspw. jährlich) erfolgen:

1. Informationssammlung: Informationen über das Testobjekt sammeln und Strukturanalyse durchführen
2. Prüfung der Richtlinien: Policies und andere sicherheitsrelevante Dokumente des Unternehmens sowie Dokumentation der Hersteller sichten
3. Prüfung der Eigenentwicklungen: Softwareentwicklungsprozesse auf Sicherheit prüfen
4. Penetrationstest: Penetrationstest auf Basis der gewonnenen Informationen durchführen

Die einzelnen Schritte werden im Folgenden anhand eines anonymisierten Fallbeispiels erläutert. Das Unternehmen ist ein global agierender Automobilzulieferer mit Hauptsitz in Deutschland. Knapp 80 % der jährlich erwirtschafteten Umsätze (über 4 Mrd. EUR) stammen aus Geschäften mit Kunden aus der Automobilbranche. Zu den Kunden gehören hauptsächlich OEMs (Original Equipment Manufacturers) wie zum Beispiel VW, Audi, Citroën oder Land Rover. Das PLM-System des Unternehmens gewann in den letzten Jahren zunehmend an Bedeutung. Es handelt sich um die Standardsoftware Windchill von PTC, die durch eigenentwickelte Schnittstellen und geänderte Workflows an die Bedürfnisse des Unternehmens angepasst wurde. Die Software wird regelmäßig aktualisiert, wobei auch auf Sicherheitsupdates geachtet wird. Die Konfigurationen und Eigenentwicklungen wurden dagegen nie hinsichtlich IT-Sicherheit geprüft.

3.3.2 Informationssammlung

Zunächst werden Informationen über das zu testende System gesammelt. Dazu können hauptsächlich die Techniken des OWASP Testing Guides bezüglich „Information Gathering“ angewandt werden [MeMu15, S. 28ff]. Der Guide bietet beispielsweise Anleitungen um herauszufinden, welche HTTP-Header, Parameter oder Cookies von einer Webanwendung erwartet bzw.

gesetzt werden. Ein Tool, das dafür eingesetzt wird, ist zum Beispiel die Browsererweiterung „Wappalyzer“. Im Fallbeispiel sah das Ergebnis eines solchen Tests wie folgt aus:

„OTG-INFO-002: einfaches Fingerprinting des Webservers ist möglich. Die Serverversion lautet: Apache/x.x.x (Unix) mod_ssl/x.x.x OpenSSL/x.x.x. Sowohl die Art und Version des Webservers konnten ermittelt werden als auch die Version von OpenSSL, welches für den Aufbau von HTTPS-Verbindungen genutzt wird.“

Darauf aufbauend ist eine knappe, technische Strukturanalyse durchzuführen. Diese Strukturanalyse geht von einem Netzplan aus und beschreibt IT-Systeme beginnend auf Betriebssystemebene. Die Strukturanalyse beinhaltet ebenfalls die auf den Systemen laufenden Anwendungen und eventuell genutzte Bibliotheken, sofern sie im Zusammenhang mit dem zu prüfenden PLM-System stehen. Die hier verwendete Strukturanalyse stellt eine vereinfachte Art des Modells, wie sie der BSI IT-Grundschutz vor dem Basis-Sicherheitscheck fordert, dar [BSI08, S. 39ff]. Tabelle 1zeigt einen Ausschnitt aus der Strukturanalyse des Fallbeispiels.

Tab. 1: Ausschnitt aus der tabellarischen Strukturanalyse (Quelle: eigene Darstellung)

Nr.	Titel	Version	Beschreibung
1	Red Hat Enterprise Linux	x.x	Zugrunde liegendes Betriebssystem
2	Ext JS Library	x.x	Javascript Library für interaktive Anwendungen

Die Informationssammlung eröffnet einen groben aber dennoch vollständigen Blick auf das PLM-System und dient den nächsten Schritten als Fundament.

3.3.3 Prüfung der Richtlinien

Im zweiten Schritt sind Sicherheitsrichtlinien und andere relevante Dokumente des Unternehmens zu sichten. Dazu zählen auch sicherheitsrelevante Dokumentationen des Herstellers des PLM-Systems und andere relevante externe Richtlinien, wie sichere Beispielkonfigurationen. Das PLM-System wird anschließend auf Konformität zu diesen Richtlinien geprüft. Die Vorgaben in den Richtlinien sind wie funktionale Anforderungen nach Common Criteria zu behandeln und entsprechend in Sicherheitsziele für das zu prüfende System und Sicherheitsziele für die Einsatzumgebung aufzuteilen [CCEB12, S. 71]. Da die Grundvoraussetzung war, dass die Einsatzumgebung bereits sicher sein soll, sind nur die Sicherheitsziele für das PLM-System auch tatsächlich zu prüfen. Jede signifikante Abweichung ist zu dokumentieren.

Der Automobilzulieferer hat mehrere Richtlinien, die auf das PLM anzuwenden sind. Dazu gehören eine allgemeine Sicherheitsrichtlinie, eine Sicherheitsrichtlinie für Anwender und eine Richtlinie speziell für Linux-Server. Neben diesen Dokumenten wurden auch Dokumente des Herstellers des PLM-Systems auf Hinweise und Empfehlungen durchsucht. So stellte sich zum Beispiel heraus, dass die gewählte Installationsarchitektur nicht vom Hersteller empfohlen wurde. Tabelle 2 zeigt den Ausschnitt einer tabellarischen Aufstellung der Prüfergebnisse aus dem Fallbeispiel.

Diese Übersicht der Verstöße gegen Richtlinien und Empfehlungen dient neben der später zu erstellenden Schwachstellenliste als Leitfaden für Verbesserungen. So gesehen, stellt die Tabelle bereits eine Art Aufgabenliste dar. Sie kann auch als zusätzlicher Input für den Penetrationstest in Schritt vier dienen; insbesondere der Abgleich mit den Empfehlungen der Hersteller der Softwareprodukte.

Tab. 2: Beispiel für Prüfung von Sicherheitsrichtlinien (Quelle: eigene Darstellung)

Nr.	Dokument	Richtlinie	Abweichung
1	Sicherheits-richtlinie	Ein zentraler Server soll für das Logging verwendet werden.	Logs werden nur lokal in Dateien gespeichert.
2	Linux-Richtli-nie	Jeder Administrator soll seinen eigenen Account besitzen.	Der Administrator wird von mehre-ren Nutzern geteilt.

3.3.4 Prüfung der Eigenentwicklungen

Falls das Unternehmen Anpassungen, Schnittstellen oder andere Software selbst entwickelt, die mit dem PLM-System arbeiten, wird das Vorgehen bei der Softwareentwicklung geprüft. Es muss vor allem festgestellt werden, ob Softwareentwicklungsprozesse existieren, die die Sicherheit fördern, z.B. nach OWASP Testing Guide. Der Testing Guide hat zum Ziel, das Testen der Sicherheit über den kompletten Softwarelebenszyklus auszudehnen. Das bedeutet, dass schon während der Planung zur Entwicklung der Anwendung sicherheitsrelevante Fragen gestellt und beantwortet werden müssen.

Im Fallbeispiel lautet eine Bewertung der Eigenentwicklungen zum Beispiel so:

„IT-Sicherheit ist kein fester Bestandteil der Softwareentwicklung. Die Mitarbeiter entwickeln üblicherweise auf einem von mehreren Entwicklungsservern, oft aber auch direkt auf dem Integrationsserver, wenn der Umfang der Entwicklung gering ist. So geschieht es, dass sich Entwicklungen kreuzen und beeinflussen."

Im Anschluss an die Sicherheitsanalyse können die Aufzeichnungen dazu genutzt werden, den Softwareentwicklungsprozess zu verbessern. Auch dabei sollten wieder Anforderungen des OWASP Testing Guides berücksichtigt werden.

3.3.5 Penetrationstest

Zuletzt wird das PLM-System inklusive Betriebssystem einem Penetrationstest unterzogen. Als Input dienen die gewonnenen Informationen aus den vorherigen Schritten. Der Tester kann die in den BSI IT-Grundschutz-Katalogen beschriebene Vorgehensweise für Penetrationstests befolgen [BSI16, S. 4669ff.]. Diese schließt auch Vereinbarungen bezüglich z.B. Verantwortlichkeiten und zu nutzender Technik mit ein und erklärt typische Angriffstechniken wie z.B. Portscanning, DoS oder Social Engineering. Alle gefundenen Schwachstellen sind zu dokumentieren. Dazu gehört auch eine Einschätzung der Gefährdung, die durch die gefundenen Schwachstellen ausgeht, bewertet z.B. nach dem CVSS[2] (Common Vulnerability Scoring System). Aus den Einzelwerten kann der Durchschnitt berechnet werden, um die Gesamtbedrohungslage darzustellen. Wann immer möglich, sollten auch Code Reviews durchgeführt werden. Black Box Testing sollte hingegen so weit wie möglich vermieden werden.

Als Anregung zu den Tests können die vorgesehenen Maßnahmen aus den IT-Grundschutz-Katalog-Bausteinen „B 1.10 Standardsoftware", „B 3.101 Allgemeiner Server", der entsprechende spezifische Baustein, zum Beispiel „B 3.102 Server unter Unix", „B 5.4 Webserver", „B 5.7 Datenbanken", „B 5.21 Webanwendungen" und „B 5.24 Web-Services" auf ihre Umsetzung hin geprüft werden [s. BSI16]. Die Prüffragen der Kataloge können dafür hilfreich sein. Methodisch können die Anleitungen des OWASP Testing Guide verwendet werden, um die

[2] Ein System um den Schweregrad von gefundenen Schwachstellen zu bewerten.

einzelnen Aspekte zu testen. Automatisierte Tools können genutzt werden, um Schwachstellen zu finden.[3] Ein solches Tool ist zum Beispiel der „OWASP Zed Attack Proxy“. Grundsätzlich können zusätzlich funktionale Anforderungen oder auch Anforderungen an die Vertrauenswürdigkeit aus den CC geprüft werden, sofern sie passend sind, zum Beispiel Anforderungen an die Protokollierung von sicherheitsrelevanten Ereignissen.

Bei der IT-Sicherheitsanalyse des PLM-Systems des Automobilzulieferers wurden über 30 technische oder organisatorische Schwachstellen aufgedeckt. Tabelle 3 zeigt am Fallbeispiel die Dokumentation einer Schwachstelle. Die meisten dieser Schwachstellen wurden durch händisches Probieren aufgedeckt. Beispielsweise wurde durch das simple Eingeben von HTML und Javascript in Eingabefelder eine schwerwiegende persistente XSS-Lücke in einer eigenentwickelten Anpassung des Systems entdeckt. Andere Schwachstellen kamen durch Gespräche mit Mitarbeitern ans Tageslicht. Wiederum andere – vor allem bei Anpassungen und Schnittstellen – durch eine intensive Prüfung des Quellcodes und der Konfiguration. Oftmals half auch eine genaue Betrachtung von Dateiberechtigungen wichtiger Dateien. Grundsätzlich ist es wichtig, im Rahmen der Informationssammlung so viel wie möglich über das System in Erfahrung zu bringen und auch nach bekannten Schwachstellen der Softwarekomponenten in Schwachstellendatenbanken (z.B. https://nvd.nist.gov) zu suchen.

Tab. 3: Beispiel für Schwachstellendokumentation (Quelle: eigene Darstellung)

# 1	Tomcat-Error-Seiten zeigen zu viele Informationen	CVSS: 4,3
Problem: Tomcat-Error-Seiten zeigen zu viele Informationen, z.B. Art des Fehlers, Kompletter Serverseitiger Pfad der betroffenen Datei, detaillierte Beschreibung, Tomcat Version.		
Mögliche Fehlerbehebung: Tomcat-Fehlerseite anpassen um sensible Informationen zu verstecken.		

Nach Abschluss der Sicherheitsanalyse des PLM-Systems kann das Unternehmen anhand der Ergebnisse Maßnahmen ableiten, um das System sicherer zu machen. Die erstellte Schwachstellenliste ist dafür ein guter Ansatzpunkt. Die Durchführung der vier Schritte der hier beschriebenen IT-Sicherheitsanalyse durch eine Person hat insgesamt nur ca. drei Wochen gedauert. Dabei wurden Kontakte zu den Abteilungen PLM, IT, Informationssicherheit und Teilemanagement hergestellt um alle notwendigen Informationen zu beziehen.

4 Fazit

Als Branche mit den meisten Datendiebstählen und Wirtschaftsspionage- und Sabotageschäden, braucht die Automobilbranche sichere PLM-Lösungen, die Produkte und ihre Lebenszyklen schützen können. Die IT-Sicherheitsanalyse eines PLM-Systems birgt jedoch einige Herausforderungen. Neben dem Standard-Produkt, zum Beispiel Windchill, existieren in Unternehmen ganz unterschiedliche Konfigurationen, Anpassungen und Schnittstellen mit unterschiedlicher Integrationstiefe. Aber nicht nur die Technik unterscheidet sich, auch organisatorisch ist jedes Unternehmen anders. Die drei vorgestellten Methoden Common Criteria, OWASP Testing Guide und IT-Grundschutz Basis-Sicherheitscheck sind grundsätzlich eigenständig dazu geeignet, ein PLM-System zu analysieren. Jede Methode hat Vor- und Nachteile. Alle drei Methoden fordern in gewisser Weise mehr als für eine IT-Sicherheitsanalyse eines

[3] Der OWASP Testing Guide rät allerdings eher davon ab, automatisierte Tools zu nutzen. Diese Tools testen nur generisch und nicht spezifisch die vorliegende Anwendung oder Konfiguration. Gleichzeitig liefern sie oft viele potentielle Schwachstellen, die bei genauerer Betrachtung doch keine sind [MeMu15, S. 6].

PLM-Systems von Nöten wäre. Jedoch enthält jede Methode Elemente, deren Beachtung für diesen Zweck lohnenswert ist.

Das erstellte Konzept bietet auf Basis dieser drei Methoden eine möglichst effektiv umsetzbare Grundlage zur internen Analyse eines PLM-Systems und versucht gleichzeitig, die Ressourcen eines Unternehmens nicht zu stark zu beanspruchen. Das Konzept hat sich in der Anwendung bei einem Automobilzulieferer als geeignet herausgestellt: Es führte innerhalb weniger Wochen zu einer Schwachstellenliste, die nun als Leitfaden für die Verbesserung der Sicherheit des PLM-Systems dient. Erstmals wurde durch die Analyse auch erkannt und festgehalten, dass das System teilweise gegen unternehmenseigene Sicherheitsrichtlinien verstößt und der Prozess zur Entwicklung von Anpassungen Sicherheitsaspekte nicht korrekt bedachte.

Es bleibt zu hoffen, dass zukünftig mehr Literatur, die IT-Sicherheit und PLM vereint, veröffentlicht wird. Das Konzept ist ein erster Vorstoß in diese Richtung, welches als Grundlage für weitere Arbeiten dienen kann.

Literatur

[Bitk15] „Computerkriminalität nach Branche in Deutschland 2015 | Umfrage“, Statista, 2015. http://de.statista.com/statistik/daten/studie/164303/umfrage/computerkriminalitaet-nach-branche-in-deutschland/. [Zugegriffen: 01/2016].

[BSI08] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-2, IT-Grundschutz Vorgehensweise“, 2008.

[BSI11] Bundesamt für Sicherheit in der Informationstechnik, „Webkurs IT-Grundschutz IT-Grundschutz im Selbststudium“, 2011. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/gskurs_pdf.pdf?__blob=publicationFile&v=1

[CCEB12c] Common Criteria Editorial Board, „Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components“. 2012.

[BSI16] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, 15. Ergänzungslieferung, 2016.

[BSIod] Bundesamt für Sicherheit in der Informationstechnik, „BSI - IT-Grundschutz - IT-Grundschutz-Standards“. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html. [Zugegriffen: 01/2016].

[Ecke14] C. Eckert, IT-Sicherheit: Konzepte, Verfahren, Protokolle, 9. Aufl. Oldenbourg: De Gruyter, 2014.

[EiSt13] M. Eigner und R. Stelzer, Product Lifecycle Management: ein Leitfaden für Product Development und Life Cycle Management, 2., neu bearb. Aufl. Dordrecht: Springer, 2013.

[FIRST1] FIRST.Org, Inc., „CVSS v3.0 User Guide (v1.4)“.

[Goll11] D. Gollmann, Computer security, 3rd ed. Chichester, West Sussex: Wiley, 2011.

[Heis16] heise online, „IT-Sicherheitsgesetz: Wer was wann zu melden hat“, heise online. http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-Wer-was-wann-zu-melden-hat-3096885.html. [Zugegriffen: 02/2016].

[Heit07] M. Heitmann: IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, 1. Auflage, Wiesbaden, Dt. Uni.-Verl, 2007.

[Kapp13] M. Kappes: Netzwerk- und Datensicherheit: eine praktische Einführung, 2. Auflage, Wiesbaden, Springer Vieweg, 2013.

[KeKl15] H. Kersten, G. Klett: Der IT Security Manager Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden. Wiesbaden, Springer Vieweg, 2015.

[Klip15] S. Klipper: Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010, 2. Auflage, Springer Vieweg, 2015.

[MeMu15] M. Meucci und A. Muller: Testing Guide 4.0 - Release. The OWASP Foundation, 2015.

[PTC14] PTC: „Windchill Architecture Overview“. 2014.

[RaBh13] R. Ranchal und B. Bhargava: „Protecting PLM Data Throughout Their Lifecycle“, in Quality, Reliability, Security and Robustness in Heterogeneous Networks, Greater Noida, India, 2013.

[Schu15] Schuh, Prof. Dr. Günther: „PLM (Product Lifecycle Management) — Enzyklopaedie der Wirtschaftsinformatik“, 2015. [Online]. http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/informationssysteme/Sektorspezifische-Anwendungssysteme/Product-Life-Cycle-Management. [Zugegriffen: 06/2016].

[VDA05] VDA (Hrsg.):„Rahmenanforderungen zur Produktsicherheit in der deutschen Automobilindustrie (Prototypenschutz)“, 2005.