MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

IT-Security Status Evaluation
Entwicklung und Implementierung eines Modells mit Tool-Unterstützung

verfasst von / submitted by

Gönül Yigitsoy, BSc.

angestrebter akademischer Grad/in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur (Dipl.-Ing.)

Wien, 2018/ Vienna 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student records sheet:	A 066 926
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet	Masterstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.Prof. Dipl.-Ing. Dr. Dr. Gerald Quirchmayr

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, 24. Oktober 2018 Gönül Yigitsoy

Zusammenfassung

Im Rahmen dieser Arbeit wird ein Modell entwickelt, das den IT-Sicherheitsstatus eines Systems bewertet. Dabei werden Sicherheitskennzahlen basierend auf ISO-Standards entwickelt. Im Verlauf der Arbeit wird ein Überblick über das ISO Messmodell und über die Balanced Scorecard gegeben und für die Durchführung der Bewertung entsprechend modelliert. Abschließend runden die prototypische Implementierung und dessen Test die Arbeit ab. Die Bewertung des IT-Sicherheitsstatus von Systemen ist ein wichtiger Punkt in einem Unternehmen. Daher investieren diese immer mehr in die Sicherheit, um den Schutz vor Angriffen durch Hacker oder durch Schadprogramme zu gewährleisten. Aus diesem Grund ist eine regelmäßige Durchführung von Sicherheitsanalysen und Sicherheitsbewertungen von großer Bedeutung. In diesem Zusammenhang ist für die Bewertung der Sicherheitslage eines Unternehmens ein Framework erforderlich, das auf Best Practices und auf Standards basiert. Besonders hervorzuheben ist in diesem Kontext die Definition von Sicherheitskennzahlen. In der vorliegenden Arbeit wird zunächst ein Überblick über das Information Security Management System und über den Plan-Do-Check-Act Zyklus gegeben. Des Weiteren werden die Security Metrics und die Balanced Scorecard detailliert beschrieben. Die Zielsetzung dieser Arbeit ist es, mit Hilfe der definierten Sicherheitskennzahlen, den IT-Sicherheitsstatus eines Unternehmens zu messen und zu bewerten. Anhand von Sicherheitskennzahlen wird der Status der IT-Sicherheit im Unternehmen ermittelt. In dieser Arbeit werden Kennzahlen entwickelt, um die Zugriffskontrolle und die Sucheingaben im System zu bewerten. Dazu wird ein Plugin entwickelt und implementiert, das die Sicherheitsbewertung eines Systems automatisch durchführt. Dabei werden alle Login-Daten und Sucheingaben in einem bestimmten Zeitraum analysiert und bewertet. Um die IT-Sicherheitsbewertung durchführen zu können, ist auch ein Indikator erforderlich. Dieser wird vom Unternehmen bestimmt. Anhand der Bewertungsergebnisse wird ein Überblick über den IT-Sicherheitsstatus des Systems gegeben. Aufgrund dieser Ergebnisse kann das Unternehmen entscheiden, welche Maßnahmen bezüglich der Sicherheit im System getroffen werden müssen. Außerdem kann das Unternehmen detaillierte Informationen über Benutzernamen, Zeitpunkt und IP-Adresse aufrufen. Im Rahmen dieser Arbeit wird die Modellentwicklung, die Prototyp-Implementierung und die Testdurchführung ausführlich erklärt. Abschließend werden die Testergebnisse diskutiert.

Abstract

As part of this work, a model has been developed that evaluates the IT security status of a system. Security metrics are developed based on ISO standards. In the course of this work, an overview of the ISO measurement model and of the balanced scorecard is given and modeled accordingly for the performance of the evaluation. Finally, the prototype implementation and its test complete the work. Evaluating the security status of systems is an important issue in organizations. As a result, organizations are investing more and more in security to protect themselves against attacks by hackers or malware. For this reason, regular security analyses and security evaluations are important. In this context, assessing a company's security level requires a framework based on best practices and on standards. In this context the definition of security metrics is particularly highlighted. In the present work, an overview of the Information Security Management System and the Plan-Do-Check-Act cycle is given. There will also be a detailed description of the Security Metrics and the Balanced Scorecard. The objective of this thesis is to measure and evaluate the IT security status of a company with the aid of the defined security metrics. Security metrics are used to determine the status of IT security in the enterprise. In this work, metrics are developed to assess access control and search input in the system. For this purpose, a plugin is developed and implemented, which carries out the safety assessment of a system automatically. All login data and search entries are analyzed and evaluated within a certain period of time. To perform the IT security assessment, an indicator is also required. This is determined by the company. The evaluation results provide an overview of the IT security status of the system. Based on these findings, the company can decide what security measures to take to improve the system. In addition, the company can call up detailed information about user name, time and IP address. In the context of this work the model development, the prototype implementation and the test execution are explained in detail. Finally, the test results are discussed.

Inhaltsverzeichnis

1 Einleitung

Die IT-Sicherheit ist ein essentielles Thema in einem Unternehmen. Die Messung der Sicherheit wird durch die steigende Komplexität der Systeme schwieriger. Aus diesem Grund gibt es einen Bedarf an methodischen Ansätzen um den Sicherheitsstatus und die Performance der Systeme bewerten zu können. Das Unternehmen kann bessere Entscheidungen bezüglich der Sicherheit treffen, wenn das Sicherheitsniveau des Systems bekannt ist. Daraus resultiert, dass die Security Metrics in diesem Zusammenhang eine wichtige Rolle spielen. Mit Hilfe von Security Metrics kann die Sicherheit des Systems bewertet werden. Jedoch gibt es keine einheitlich akzeptierten Ansätze hinsichtlich der Messung der Sicherheit. Daher ist die Definition von Security Metrics ein Themengebiet in der Forschung, das zunehmend an Interesse gewinnt. [Savola, 2009]

Die Verwaltung und Gewährleistung der IT-Sicherheit in Unternehmen ist eine komplizierte und kostenintensive Aufgabe. Zu diesen Aufgaben zählen zum Beispiel die sichere Konfiguration diverser Softwarekomponenten und die Sicherheitsüberwachung. Die Erfüllung der erforderlichen Sicherheitsanforderungen ist mit großer Zeit- und Arbeitsaufwand verbunden. Der Grund dafür ist, dass in Unternehmen automatisierte Methoden fehlen um diese Sicherheitsanforderungen erfüllen zu können. [Montesino and Fenz, 2011]

Die IT-Sicherheit spielt in vielen Unternehmen eine wichtige Rolle, dementsprechend werden Maßnahmen getroffen, um die Sicherheit im System sicherzustellen. Im Gegensatz zu den getroffenen Maßnahmen können aber auch Mängel identifiziert werden, die eine Gefahr für die Sicherheit im Unternehmen darstellen können. Dies kann die Leistungsfähigkeit der Unternehmen negativ beeinflussen. Das Management muss daher in der Lage sein den Sicherheitszustand der Organisation zu bewerten. Die Bewertung des Sicherheitsstatus erfolgt anhand von Sicherheitskennzahlen. Um die Bewertung durchführen zu können, ist ein Tool notwendig, das die gesamte Sicherheitslage eines Unternehmens überprüfen und bewerten kann. Damit ist es dann möglich ein besseres Verständnis über diverse Sicherheitsprozesse zu haben und diesbezüglich Entscheidung zu treffen. [Chaula et al., 2004] Das Ziel dieser Arbeit ist daher ein Modell für die Bewertung des IT-Sicherheitsstatus eines Systems zu entwickeln und zu implementieren.

Die vorliegende Arbeit gliedert sich in zehn Kapitel: Das erste Kapitel beinhaltet die Motivation und die Zielsetzung sowie eine Literaturanalyse. Eine detaillierte Problembeschreibung schließt das erste Kapitel ab. Das zweite Kapitel beschäftigt sich mit dem Thema IT-Security Status Evaluation. Hier werden vor allem Security Evaluation Architecture, Information Security Management System und Plan-Do-Check-Act thematisiert. Im Fokus des dritten Kapitels stehen Security Metrics. Zunächst wird die Entwicklung der Sicherheitsmetriken beschrieben und das Messmodell ISO/IEC 27004 dargestellt. Anschließend wird im vierten Kapitel die Balanced Scorecard erklärt. Hier wird näher auf die Perspektiven von IT-Security Balanced Scorecard eingegangen und auf die Merkmale der Sicherheitsleistungsmessung. Im fünften Kapitel wird die Modellentwicklung beschrieben. Darauf aufbauend erfolgt im sechsten Kapitel eine detaillierte Beschreibung der prototypischen Implementierung. Schließlich werden im Kapitel sieben und acht die Testergebnisse dokumentiert und im neunten Kapitel die Testergebnisse diskutiert. Im zehnten Kapitel wird die Arbeit mit der Conclusio abgeschlossen.

1.1 Motivation und Zielsetzung

Die kontinuierliche Entwicklung der Technologie und der IT-Systeme hat zur Folge, dass IT-Sicherheit und Datenschutz in Unternehmen oberste Priorität haben. [DSG, 2018] Die Unternehmen sind durch diverse Bedrohungen aus dem Internet gefährdet. Angriffe wie Denial of Service (DoS) und viele andere Angriffe können ernsthafte Schäden anrichten. Daraus resultiert, dass die Unternehmen laufend angemessene Sicherheitsanalysen, Überwachungen und Bewertungen der IT-Sicherheit durchführen müssen. In diesem Fall sind übliche Analysen mit einem Antivirenprogamm nicht ausreichend. Es besteht ein Bedarf an einem Framework, welches verschiedene Messmodelle, Standards und Sicherheitskennzahlen integriert. In dieser Hinsicht stellt sich die Frage, welche Sicherheitsfaktoren überhaupt gemessen und wie sie bewertet werden können. [Farn et al., 2004]
Diese Arbeit beschäftigt sich mit der Bewertung des IT-Sicherheitsstatus eines Systems. Dazu wird ein Modell entwickelt, implementiert und getestet. Die Motivation liegt darin, anhand von Sicherheitskennzahlen die IT-Sicherheit eines Systems zu bewerten.

Das Ziel dieser Arbeit ist die Entwicklung und die Implementierung

eines Modells mit Tool-Unterstützung sowie die Evaluation des Informationssicherheitsstatus eines Systems. Die Evaluation der IT-Sicherheit des Systems erfolgt unter Berücksichtigung der existierenden Normen, Standards und Best Practices. Dazu zählen Cobit (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), CC (Common Criteria), ISO/IEC-Standards, NIST SP 800-55 u.a. [Isselhorst, 2016] [Chew et al., 2008]
Im Rahmen dieser Arbeit entwickelten Kennzahlen werden in die IT-Balanced-Scorecard implementiert, um Informationen über den Sicherheitslevel des Unternehmens zu erhalten. Der Schwerpunkt dieser Arbeit ist ein IT-Sicherheitsbewertungs-Prototyp für eine Organisation zu entwickeln. Der entwickelte Prototyp wird anschließend in Kooperation mit der Plus Mobile e.U. getestet.

1.2 Literaturanalyse

In der vorliegenden Arbeit wurde eine Literaturanalyse durchgeführt, um den aktuellen Forschungsstand zu erfassen. Die durchgeführte Literaturrecherche zeigt, dass viele Bücher und Artikel zu diesem Thema veröffentlicht wurden. Da das Thema IT-Sicherheit ein weit verbreitetes Forschungsgebiet ist, musste die Recherche auf die IT-Sicherheitsevaluation eines Systems eingeschränkt werden. Um weitere Untersuchungen zu ermöglichen, wurde das Thema in die folgenden Konzepte eingeteilt:

- IT-Security Management
- IT-Risks Management
- IT-Security Standards/Best Practices
- IT-Security Metrics
- IT-Security Balanced Scorecard

Im Zusammenhang zu dem Thema gibt es auch viel Literatur über Frameworks für die Implementierung der IT-Sicherheit in einem Unternehmen. Außerdem gibt es Veröffentlichungen über modellbasierte Methoden der Sicherheitsanalyse. Jedoch gibt es derzeit kein umfassendes, integriertes Bewertungstool oder ein Bewertungsmodell zur Bewertung der gesamten IT-Sicherheitslage einer Organisation.

Die im Rahmen der Literaturrecherche gewonnenen Informationen werden in Verbindung mit Best Practices, Standards und Sicherheitskennzahlen

verwendet, um einen Prototyp zur Bewertung der Sicherheitslage eines Systems zu entwickeln und ein Hintergrundwissen über die Informationssicherheit zu vermitteln. Darüber hinaus wird die Arbeit einen Überblick über die Herausforderungen und über die verschiedenen Aspekte der Informationssicherheit geben. Als letztes werden die unterschiedlichen Messmodelle analysiert.

1.3 Problembeschreibung

Die IT-Sicherheitsanalyse in einem Unternehmen wird mit der zunehmenden Entwicklung der Systeme komplexer. Um beurteilen zu können, wie sicher das System einer Organisation ist, ist es unerlässlich den aktuellen Sicherheitsstatus der Organisation zu messen und zu bewerten. Die Herausforderung bei der Bewertung des IT-Sicherheitsstatus einer Organisation ist die Definition von Sicherheitskennzahlen. Die Problematik liegt darin, dass die Kennzahlen quantifizierbare Informationen wie Prozentsatz, Durchschnittswerte oder absolute Zahlen sein müssen um Formeln für die Analyse anwenden zu können. Daher müssen die Sicherheitskennzahlen messbar sein, um die IT-Sicherheit abzudecken. Unter Berücksichtigung dieser Bedingung, besteht das Problem darin, standardisierte quantitative IT-Sicherheitsmessgrößen für eine effiziente Bewertung der IT-Sicherheitslage festzulegen. [Kahraman, 2005]

Die rasante Entwicklung der Informationstechnologie und des Internets ermöglicht es Informationen jederzeit und an jedem Ort abzurufen. Neben dem legalen Informationserwerb gibt es aber auch den illegalen Erwerb. Zum Beispiel können die Angreifer die Sicherheitslücke im System eines Unternehmens umgehen und somit die Systeme angreifen. Dabei kann es sich sowohl um externe aber auch um interne Angriffe handeln. Zum Beispiel kann es sich um Bedrohungen wie Denial of Service (DoS) handeln oder aber auch um andere, die einen großen Schaden im System verursachen können. Aus diesem Grund ist das Thema Informationssicherheit für alle Organisationen ein essentielles Kerngebiet. [Farn et al., 2004]

Seit Unternehmen ihre Geschäftsprozesse auf das Internet und mobile Anwendungen verlagert haben, sind sie vielen ernsthaften und unterschätzten Sicherheitsrisiken ausgesetzt. Aus diesem Grund besteht die Notwendigkeit, dass Organisationen angemessene Sicherheitskennzahlen definieren und regelmäßig eine entsprechende

Überwachung und Sicherheitsbewertung durchführen. [Pereira and Santos, 2014]

Daher ist es von großer Bedeutung die IT-Sicherheit im Unternehmen dementsprechend zu verwalten und zu implementieren. Für die Verwaltung und Wartung von IT-Services sind diverse Standards, Tools, Frameworks und Best Practices vorhanden, die in Managementsysteme integriert werden können. Jedoch reichen sie nicht für ein effizientes IT-Managementsystem aus. Aus diesem Grund ist es wichtig ein umfassendes Framework zu entwickeln, welches verschiedene Frameworks und Standards integriert. Ein Vorteil von so einem umfassenden Framework ist, dass es in allen Organisationen verwendet werden kann. [Sahibudin et al., 2008]

Außerdem müssen Metriken definiert werden, um die Effizienz der implementierten Kontrollen zu bewerten, aber auch um die Sicherheitsinvestitionen zu rechtfertigen. Mit Hilfe von Metriken können für Entscheidungsträger entscheidungsrelevante Informationen zur Verwaltung ihrer organisatorischen Ressourcen bereitgestellt werden um ihren täglichen Betrieb sicherzustellen. [Pereira and Santos, 2014]

Die Implementierung von Sicherheitskontrollen in Unternehmen ist entscheidend, hängt jedoch mit den Geschäftszielen des Unternehmens zusammen. Die Entwicklung eines Risikomanagementprozesses beispielsweise, der Aufgaben wie Risk Assesment, Implementierung von Richtlinien und Kontrollen, Monitoring und Evaluierung umfasst, ermöglicht die Analyse der Auswirkungen im Fall eines Sicherheitsvorfalls. [Pereira and Santos, 2014]

Anhand einer Sicherheitsrisikobewertung kann das Unternehmen Informationen über die Risikofaktoren erhalten, die die organisatorischen Abläufe beeinträchtigen können und somit auch einen Einfluss auf die Ergebnisse ihrer Prozesse haben können. [Pereira and Santos, 2014]

Diese Informationen sind zum Beispiel: „Identifizierung von Bedrohungen; Schätzung der Wahrscheinlichkeit des Auftretens einer Bedrohung; Identifikation von organisatorischen kritischen Ressourcen, die betroffen sein können, sowie deren Wert; Schätzung der Auswirkungen; Bewertung kostenwirksamer Maßnahmen zur Minderung der Risiken; Dokumentierung der Ergebnisse und des Implementierungsplans für die

resultierenden Kontrollen.“ [Pereira and Santos, 2014]

Um das Risiko auf ein akzeptables Maß zu minimieren, müssen diejenigen Sicherheitskontrollen bei der Implementierung von Richtlinien und Kontrollen berücksichtigt werden, die die Risikominimierung beeinflussen. Zum Beispiel werden anhand von Kontrollen wie Training und Schulung, den Mitarbeitern Informationen über die Risikomanagementpolitik im Unternehmen gegeben. Auf diese Weise kann das Know-how der Mitarbeiter gefördert und somit zur Verringerung des Risikos im Unternehmen beigetragen werden. [Pereira and Santos, 2014]

Andere Kontrollen wie technische Kontrollen sind mit hohen Investitionen verbunden. In diesem Zusammenhang ist die Überwachung und Bewertung von Risikofaktoren kostenintensiv, was die kontinuierliche Implementierung von Kontrollen bestimmt. Mit Hilfe dieser Kontrollen kann bewertet werden, ob das Risiko erhöht oder verringert wurde. Jedoch ist in diesem Fall die Risikobewertung nicht so einfach, da die erforderlichen Daten für die Bewertung begrenzt sind. Der Grund dafür ist, dass in der Praxis die Ursachen und die Auswirkung des Risikos sich immer ändern. [Pereira and Santos, 2014]

Ein grundsätzliches Problem ist, wie bei jedem anderen Prozess, dass die Sicherheit im Unternehmen nicht verwaltet werden kann, wenn sie nicht gemessen werden kann. Deshalb sind die Metriken sehr wichtig, um den aktuellen Sicherheitsstatus zu bewerten. Des Weiteren stehen die Unternehmen unter zunehmendem Compliance-Druck, sodass sie verpflichtet sind ihre Datenbestände vor Angriffen zu schützen. Die Sicherheitsmetriken geben den Unternehmen die Möglichkeit die Bedrohungen, die Schwachstellen und die Risiken anhand quantitativer oder qualitativer Kriterien zu priorisieren. [Patriciu et al., 2006]

Viele Bewertungsmethoden konzentrieren sich auf die Ergebnisse der Sicherheitsbewertungen von IT-Systemen und auf die Prüfung der Prozesse und Kontrollen. Jedoch sind diese Methoden nicht ausreichend erfolgreich, da die Wahrscheinlichkeit zu hoch ist, neue Sicherheitslücken zu identifizieren. Die Gefahr besteht darin, dass je kürzer das Intervall ist, desto mehr nützen die Angreifer den Exploit aus, nachdem die Sicherheitslücke öffentlich bekannt gegeben wurde. In diesem Fall würden eine Echtzeit-Sicherheitsüberwachung und die Definition von guten

Sicherheitskennzahlen dazu beitragen den Status der IT-Sicherheit zu ermitteln und die Sicherheitsrisiken für die neuen Schwachstellen zu minimieren. [Patriciu et al., 2006]

Ein weiteres Problem ist, dass in den Organisationen die Bewertungen der Sicherheit von Informationssystemen von separaten Teams durchgeführt werden, da verschiedene Benutzer des Systems auch unterschiedliche Besorgnisse über die Sicherheitsaspekte von IT-Systemen haben. Dies führt dazu, dass die technischen Kennzahlen unabhängig definiert, gesammelt und analysiert werden. [Patriciu et al., 2006]

Zu diesen Kennzahlen zählen beispielsweise die Anzahl der Sicherheitslücken in Netzwerk-Scans, die Anzahl abgefangener infizierter E-Mails und die Erkennungsrate für Sicherheitsfehler in einer neuen Softwareanwendung. Aus diesem Grund können subjektive Interpretationen zu Messfehlern führen. Deswegen ist ein automatisierter Messprozess erforderlich, um die IT-Sicherheit im System bewerten zu können [Patriciu et al., 2006]

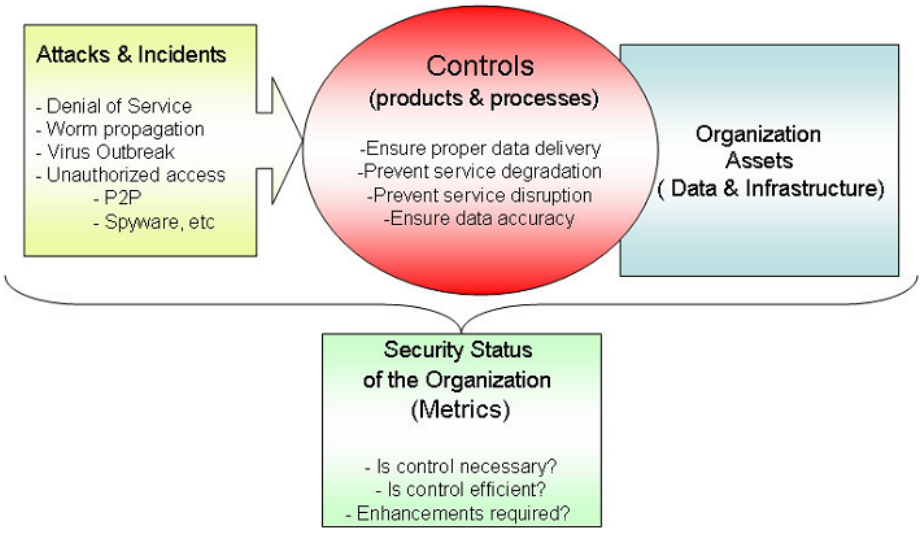

Abb. 1: Netzwerk- und Systemsicherheit basierend auf Metriken [Patriciu et al., 2006]

Die Abbildung 1 zeigt den Sicherheitsstatus eines Systems in einer grafischen Darstellung.
Alle arten von Angriffen, Viren aber auch Sicherheitsverletzungen können die IT-Infrastruktur des Unternehmens schädigen. Jedoch stehen Kontrollen wie zum Beispiel Firewalls zur Verfügung, die die physischen und logischen Ressourcen der Organisation schützen. Unter Berücksichtigung all dieser Aspekte kann der Sicherheitsstatus der Organisation bestimmt werden. Anhand dieses Sicherheitsstatus können angemessene Maßnahmen gegen die potenziellen Risiken getroffen werden. Darüber hinaus kann mit Hilfe von Sicherheitsstatusevaluationen die erforderliche Investition in Sicherheitskontrollen spezifiziert und bewertet werden. [Weiß et al., 2005]

Es gibt einige Ansätze, die sich auf die Sicherheitsbewertung von Organisationen konzentrieren. Die wichtigsten sind: Best-practice Ansätze, IT-Grundschutzhandbuch, Schwachstellenanalyse (Vulnerability analysis), Penetrationstest, Risikomanagement. [Weiß et al., 2005]

Die vorliegende Arbeit konzentriert sich auf die IT-Sicherheitsbewertung in Unternehmen. Dazu werden unterschiedliche Standpunkte betrachtet und erklärt. Im folgenden Kapitel wird zunächst die IT-Security Status Evaluation beschrieben.

2 IT-Security Status Evaluation

In diesem Kapitel wird ein allgemeiner Überblick über die IT-Sicherheitsstatusbewertung (IT-Security Status Evaluation) gegeben. Vor allem wird das Sicherheitsbewertungssystem (Security Evaluation System) näher beschrieben. Im Abschnitt 2.1 wird die Information Security Architecture und im Abschnitt 2.2 das Information Security Management System dargestellt. Anschließend erfolgt eine detaillierte Beschreibung des Plan-Do-Check-Act Zyklus.

Für die Messung der IT-Sicherheit gibt es verschiedene Möglichkeiten, wie Best Practices, Standards und Methoden. Einer der bekanntesten Ansätze ist die Common Criteria and Common Evaluation Methodology. Weitere Beispiele sind ISO-Standards, ITIL, Cobit und NIST SP 800-33. [BSI, 2018] [Chew et al., 2008] [Isselhorst, 2016]

Die Messung, Analyse und Bewertung der Sicherheit einer Organisation besteht aus mehreren Prozessen. In erster Linie liegt der Fokus bei der IT-Sicherheitsevaluierung darauf die Sicherheitsfaktoren zu identifizieren. Dies erfolgt, indem die Risiken durch Risikoanalysen transparent gemacht werden. Anschließend werden die entsprechenden Sicherheitsmaßnahmen definiert, schlussendlich erfolgen dann die Umsetzung und die Bewertung der Sicherheitsmaßnahmen. [BKA, 2014]

In der Abbildung 2 ist zu sehen, welche Prozesse bei dieser Arbeit durchgeführt wurden.

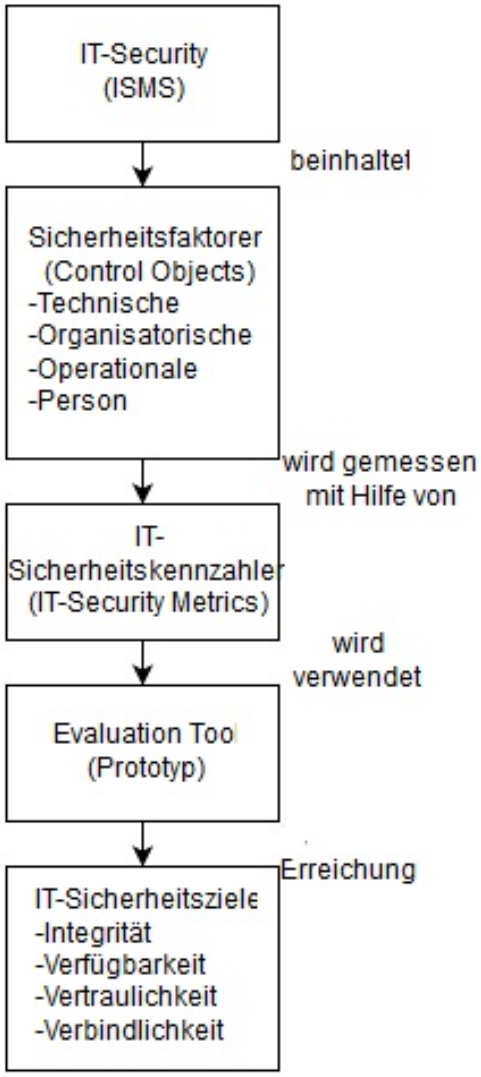

Abb. 2: Prozessschritte(eigene Darstellung)

Der Prozess IT-Security Metrics wird im dritten Kapitel erklärt. Die Entwicklung und die Implementierung des

IT-Sicherheitsbewertungssystems werden im Kapitel 5 und im Kapitel 6 beschrieben.
Das Ziel ist es einen Überblick über den aktuellen Status im Hinblick auf die Sicherheit des Systems zu geben und die IT-Sicherheitsziele, nämlich die Integrität, die Verfügbarkeit, die Vertraulichkeit und die Verbindlichkeit, zu gewährleisten. [BKA, 2014]

Für die Sicherheitsbewertung in einer Organisation sind verschiedene Arten von Tests und Analysen notwendig, jedoch ist es unmöglich alle Tests und Analysen manuell durchzuführen. Daher ist ein Werkzeug zur Automatisierung der Tests und Analysen erforderlich. Es gibt bereits einige Schwachstellenanalyse Tools die in der Praxis verwendet werden. Diese bieten aber nur netzwerk- und hostbasierten Scan-Funktionen. [Lee et al., 2001]

Lee et al. (2001) beschreiben das Security Evaluation System und analysieren welche Anforderungen das Security Evaluation System erfüllen muss, um die Sicherheitsbewertung zu automatisieren. [Lee et al., 2001]

Ein Sicherheitsevaluationssystem (Security Evaluation System) besteht aus verschiedenen Komponenten und dient dazu die Sicherheit des gesamten Systems der Unternehmen bzw. den „aktuellen Sicherheitsstatus“ des Systems zu bewerten. [Lee et al., 2001] Anhand der Bewertungsergebnisse kann der Sicherheitsmanager Entscheidungen bezüglich der Maßnahmen treffen. Zum Beispiel kann er entscheiden, wie die Konfiguration des Netzwerks geändert werden soll, um die Sicherheitslücke zu umgehen und somit den Angriff auf das Netz zu verhindern. Mit anderen Worten ausgedrückt, es ermöglicht im Vorfeld eine Strategie zur Verhinderung von Angriffen zu entwickeln. [Lee et al., 2001]

In diesem Zusammenhang stellen Lee et al. (2001) fest, dass ein Security Evaluation System folgende Anforderungen erfüllen muss. [Lee et al., 2001]

- Das Security Evaluation System muss die Sicherheitsbewertung des Unternehmens unterstützen. Die Leistung des Security Evaluation System sollte nicht verringert werden, auch dann nicht, wenn die Größe des Unternehmensnetzwerkes zunimmt. [Lee et al., 2001]

- Das Sicherheitsbewertungssystem muss Funktionen wie zum Beispiel Analyse der Schwachstellen eines Hosts und Überprüfung auf mögliche Konfigurationsfehler im System haben. Darüber hinaus muss es auch die Hinweise von Angriffen verfolgen können. [Lee et al., 2001]
- Eine weitere Anforderung ist die Durchführung von Sicherheitschecks und Sicherheitsanalysen einzelner Subnetze. Des Weiteren muss es eine Funktion zur Erzeugung von Sicherheitsbewertungsberichten bieten. [Lee et al., 2001]
- Außerdem muss es überprüfen, ob die verschiedenen Komponenten des Unternehmensnetzwerks die Sicherheitsrichtlinien, die im Security Policy Server vorhanden sind, befolgen oder nicht.
- Das Sicherheitsbewertungssystem muss einen Überblick über den Sicherheitsstatus des gesamten Netzwerks bereitstellen. [Lee et al., 2001]
- Darüber hinaus muss das Bewertungssystem über Schwachstellen Recovery-Funktionalitäten verfügen sowie regelmäßig neue Informationen aus Verzeichnisdiensten erhalten und diese bei der Bewertung der Sicherheit anwenden. [Lee et al., 2001]

Im nächsten Kapitel wird die Sicherheitsarchitektur analysiert und die wichtige Rolle im Unternehmen erläutert.

2.1 Security Evaluation Architecture

Das Internet bietet Unternehmen auf der ganzen Welt in einer vernetzten und informationsreichen Umgebung zu arbeiten. Jedoch bringen diese globalen technologischen Infrastrukturen nicht nur neue Geschäftsmöglichkeiten, sondern sind auch für neue komplexe Schwachstellen verantwortlich. Aus diesem Grund ist die IT-Sicherheit und eine klar definierte und dokumentierte IT-Sicherheitsarchitektur für viele im Unternehmen eine essentielle Voraussetzung für die Durchführung ihrer Geschäftsprozesse. Allerdings ist die Implementierung der Informationssicherheit nicht nur ein komplizierter Prozess, sondern ist auch zeitaufwändig und mit hohe Kosten verbunden. [Eloff and Eloff, 2005]
Eine gut strukturierte und ganzheitliche Methode ist notwendig, um alle Aspekte der Informationssicherheit behandeln zu können. Aus diesem Grund wird als ganzheitlicher Ansatz das Konzept der Information Security Architecture (ISA) eingeführt. Jedoch gibt es keine standardisierte Information Security Architecture. Es gibt viele Security Management Ansätze, viele von ihnen konzentrieren sich auf

Code-of-Practices wie zum Beispiel Cobit und ISO 17799. [Eloff and Eloff, 2005]
Der ISO/IEC 17799 Standard wurde überarbeitet und in ISO/IEC 27002 umbenannt. [ISO, 2018] Der Standard ISO 27002 und das international anerkannte Framework Cobit weisen darauf hin, dass Informationssicherheit ein multidisziplinäres Konzept ist, das sich horizontal über die Organisation erstreckt. [Eloff and Eloff, 2005] Jedoch stellt die Verwaltung eines multidisziplinären Konzepts eine große Herausforderung für die Organisationen dar. Das Problem ist, dass eine Vielzahl von Security Controls in einer synchronisierten und gut verwalteten Art und Weise implementiert werden müssen. Des Weiteren ist eine ISA ein Managementprozess, der in den laufenden Geschäftsbetrieb einer Organisation eingebunden ist. Sie besteht aus verschiedenen Methoden, um die wichtigsten Sicherheitsaspekte, wie zum Beispiel die Authentifizierung, die Vertraulichkeit, die Integrität und die Verbindlichkeit, zu erreichen und aufrechtzuhalten. [Eloff and Eloff, 2005]

In der Abbildung 3 wird einer Security Evaluation System Architektur und die Komponente dargestellt.

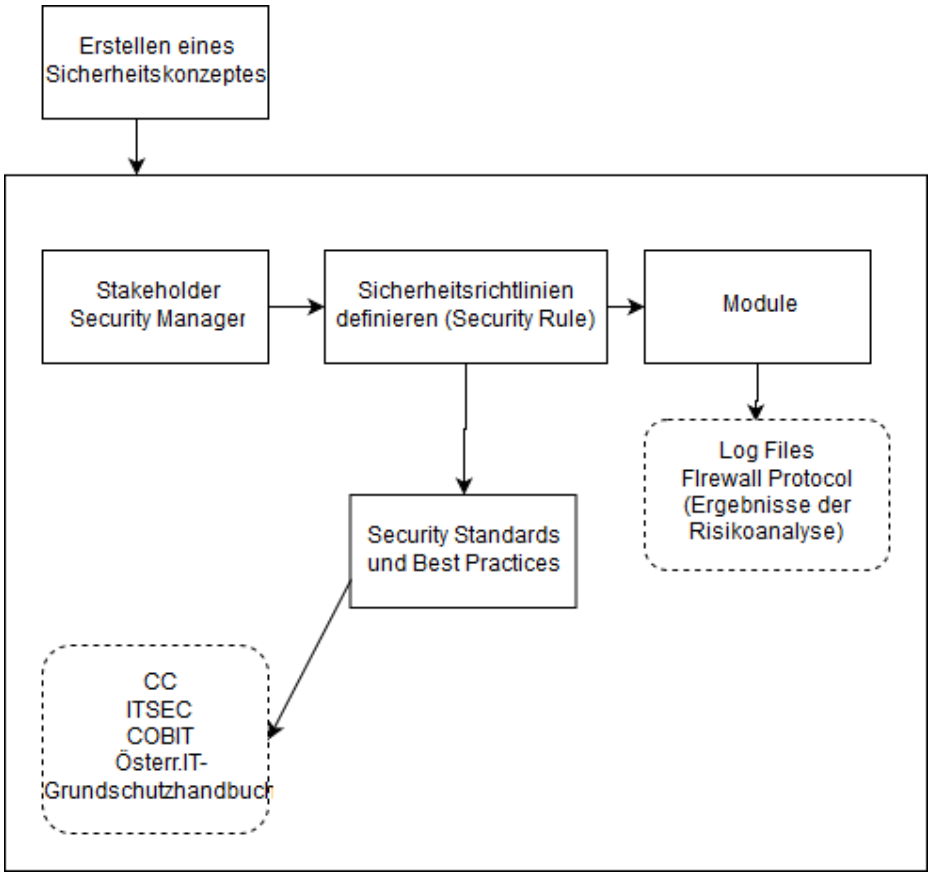

Abb. 3: Security Evaluation System Architektur (eigene Darstellung)

In dieser vorliegenden Arbeit werden mit Hilfe von Security Standards und Best Practices zuerst Sicherheitskennzahlen definiert, um den Sicherheitsstatus des Unternehmens Plus Mobile zu bewerten. Dazu wird analysiert, welche Daten es gibt und welche messbar sind. Diese Informationen sind zum Beispiel in Modulen wie Log Files und Firewall Protocol vorhanden.

Im den nächsten Abschnitten wird ein Überblick über das Information

Security Management System gegeben und die Plan-Do-Check-Act Zyklus untersucht.

2.2 Information Security Management System (ISMS)

Ein Information Security Management System (ISMS) ist ein systematischer Ansatz, um Geschäftsziele zu erreichen. Es bietet den Grundstein für die Einrichtung, Implementierung, Durchführung, Überwachung, Überprüfung, Wartung und Verbesserung der Informationssicherheit in einer Organisation. ISMS besteht aus den Richtlinien, Verfahren, Strategien und damit verbundenen Aktivitäten, die zusammen verwaltet werden müssen, um die Informationsressourcen der Organisation zu schützen. Als Basis werden die Risikobewertung und die Risikoakzeptanz der Organisation in Betracht gezogen, die darauf ausgerichtet sind, Risiken wirksam zu behandeln und zu steuern. [ISO/IEC27000, 2014]

Im ISMS werden auch Richtlinien zu den Verfahren und zu den Dokumentationskategorien festgelegt. Diese sind für die Kontrolle dieser Dokumentation erforderlich. Die gespeicherten Dokumentationen enthalten Informationen über die Managementstruktur, über das Implementierungsverfahren der Kontrollen, einschließlich der dazu gehörenden Maßnahmen und Informationen über die Managementprozeduren der ISMS. [Eloff and von Solms, 2000]

Es gibt diverse Sicherheitsmodelle, die bei der Umsetzung eines Security Management Systems und bei der Implementierung von Sicherheitskontrollen unterstützen. Das am häufigsten referenzierte Sicherheitsmodell ist der „Code of Practice for Information Security Management“. [Whitman and Mattord, 2005] Dieser Verhaltenskodex, der ursprünglich als British Standard BS7799 veröffentlicht wurde, wurde als internationales Standard Framework für Informationssicherheit von der International Organization for Standardization (ISO) und von der International Electrotechnical Commission (IEC) als ISO/IEC 17799 angenommen. Der Standard wurde überarbeitet und in ISO 27002 umbenannt, um es an das Dokument ISO 27001 anzugleichen. [Whitman and Mattord, 2005]
Der ISO/IEC 27002 gibt einen Überblick über die verschiedenen Sicherheitsbereiche und stellt Informationen zu den Sicherheitskontrollen bereit. Der ISO/IEC 27001 bietet Informationen zur Implementierung von ISO/IEC 27002 und zum Aufbau eines Information Security

Management System (ISMS). Des Weiteren bietet ISO/IEC 27001 Implementierungsdetails zur Verwendung eines Plan-Do-Check-Act Zyklus. [Whitman and Mattord, 2005]

2.3 Plan-Do-Check-Act

Die Normreihe ISO 27000 bezieht sich auf den bekannten Plan-Do-Check-Act Zyklus von Deming, der die Notwendigkeit der Prozessorientierung sowie die Integration der Betriebsplanung und die ständige Überprüfung der planungskonformen Umsetzung unterstreicht. [Disterer, 2013]
Die Planungsphase eines ISMS definiert die Anforderungen für den Schutz der Informationssysteme. Des Weiteren werden Risiken identifiziert und bewertet. Dementsprechend werden geeignete Verfahren und Maßnahmen zur Risikoreduzierung getroffen. Die Implementierung dieser Verfahren und Maßnahmen werden während der Durchführung und während des Betriebs umgesetzt. Darüber hinaus werden durch die kontinuierliche Überwachung der Operationen Berichte generiert. Die Informationen in dem Bericht können zu Verbesserungen und zur Weiterentwicklung des ISMS verwendet werden. Die Maßnahmen sollten im Zuge der kontinuierlichen Verbesserung überprüft, verbessert und Sicherheitsrisiken ermittelt und bewertet werden, um die Wirksamkeit und Effizienz des ISMS kontinuierlich zu steigern. Der Schwerpunkt der ISO 27001 ist die Planung, Implementierung, der Betrieb, die kontinuierliche Überwachung und Verbesserung eines prozessorientierten ISMS. Die Umsetzung des ISMS folgt nach dem Konzept des Plan-Do-Check-Act (PDCA) Zyklus. [Disterer, 2013]

Im folgenden Absatz werden die einzelnen Phasen des Plan-Do-Check-Act Zyklus erklärt.

PLAN: Beim Plan werden ISMS-Richtlinien, -Ziele, -Prozesse und –Verfahren festgelegt, die für das Risikomanagement und für die Verbesserung der Informationssicherheit wichtig sind. [Allen, 2006]

DO: In der Phase Do werden die festgelegten Richtlinien, Prozesse und Verfahren implementiert und ausgeführt. [Allen, 2006]

CHECK: In CHECK wird in erster Linie die Prozessleistung gegenüber der ISMS-Richtlinie und den Zielen beurteilt und auch gemessen. Anschließend werden die Ergebnisse dem Management zur Überprüfung

gemeldet. [Allen, 2006]

ACT: In der letzten Phase werden korrigierende und präventive Maßnahmen vorgenommen. Diese basieren auf den Ergebnissen der Sicherheitsbewertung, um eine laufende Verbesserung des Systems zu erreichen. [Allen, 2006]

Die wichtigsten Plan-Do-Check-Act Prozess-Schritte werden in dem Buch von Whitman und Mattord [Whitman and Mattord, 2005] wie folgt definiert.

Die Plan-Phase geht der Frage nach, welchen Entscheidungen bzw. welchen Voraussetzungen gefolgt werden muss, um die Sicherheit im System zu gewährleisten. [Allen, 2006]
Folgende Voraussetzungen sind zum Beispiel in der Plan-Phase:

PLAN

- Anwendungsbereich der ISMS festlegen
- ISMS- und Informationssicherheitsrichtlinie definieren
- Risiken identifizieren und bewerten
- Identifizierung und Bewertung von Optionen für die Behandlung des Risikos
- Maßnahmenziele und Maßnahmen wählen
- Vorbereitung eines Statement of Applicability (SOA)
  [Whitman and Mattord, 2005]

In der nächsten Phase findet die Ausführung der Schritte statt.

DO

- Risikobehandlungsplan formulieren
- Risikobehandlungsplan umsetzen
- Mitarbeiter bezüglich der ISMS schulen
- ISMS verwalten
- Sicherheitsstörfälle erkennen und managen
- Maßnahmen und Maßnahmenziele umsetzen
  [Whitman and Mattord, 2005]

In der Check-Phase wird überprüft, ob die durchgeführten Schritte auch funktioniert haben. Durch die nachfolgenden Punkte kann dies kontrolliert werden.

CHECK

- Überwachungsverfahren durchführen
- Die Effektivität des ISMS regelmäßig überprüfen
- Akzeptables Risiko überprüfen
- Interne ISMS-Audits durchführen
- Regelmäßiges Management von ISMS überprüfen
- Aktionen und Ereignisse, die Auswirkungen auf ISMS haben erfassen [Whitman and Mattord, 2005]

In der letzten Phase werden Maßnahmen getroffen, um weiterhin die Sicherheit im System zu gewährleisten.

ACT

- Identifizierte Verbesserungen umsetzen
- Korrekturen und Maßnahmen treffen
- Lessons learned anwenden
- Ergebnisse an Mitarbeiter kommunizieren
- Verbesserung der aktiven Ziele sicherstellen [Whitman and Mattord, 2005]

In der Abbildung 4 ist ein PDCA-Zyklus mit Sicherheitsprozess in einzelnen Schritten zu sehen.

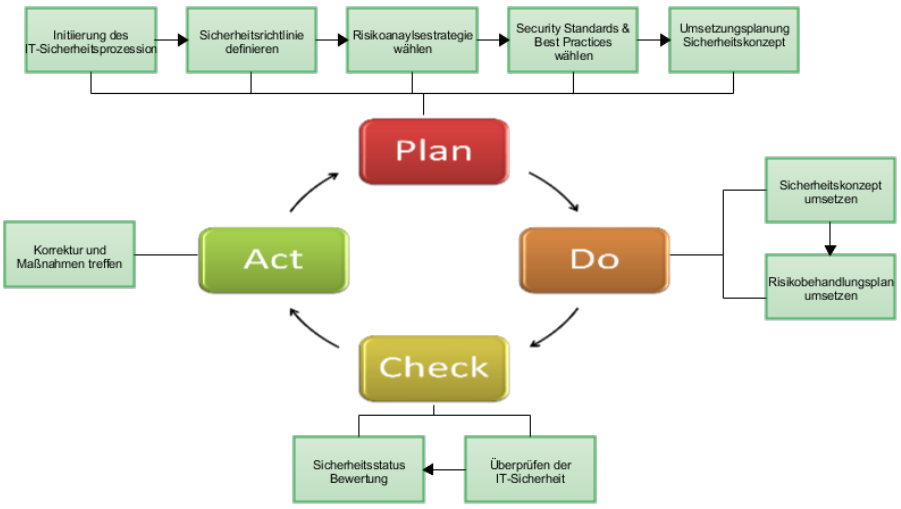

Abb. 4: Plan-Do-Check-Act Zyklus (eigene Darstellung)

Der Fokus in dieser Arbeit liegt auf der Check-Phase. Diese Phase umfasst die Überprüfung der IT-Sicherheit eines Systems sowie die Bewertung des Sicherheitsstatus.

Die Ausführung des IT-Sicherheitsprozesses erfolgt durch die Initiierung. In erster Hinsicht definiert das Management die Sicherheitsziele sowie die grundlegenden Anforderungen. Bei der Definition der Ziele muss beachtet werden, dass dadurch die Risiken nur auf einen annehmbaren Umfang minimiert werden können. Dies ist wichtig, damit weiterhin die Ziele erreicht werden können. Als nächstes wird die Sicherheitsrichtlinie definiert bzw. eingeführt. Bei der Entscheidung müssen die definierten bzw. vorgegebenen Ziele berücksichtigt werden. [Siebenhandl, 2011]

Im nächsten Schritt wird die Risikoanalysestrategie gewählt. Die Ermittlung von existierenden Bedrohungen erfolgt in Form von Risikoanalysen. Es wird ein Risikobehandlungsplan ermittelt. Die Ergebnisse der Risikoanalyse werden bei der Evaluierung des Sicherheitsstatus in Betracht gezogen. [BKA, 2014]

Im folgenden Schritt erfolgt die Auswahl der Security Standards und Best Practices. In der Phase der Umsetzungsplanung des Sicherheitskonzepts werden die ausgewählten Bestandteile aus den vorhandenen Best Practices und Standards umgesetzt. Darüber hinaus werden die Sicherheitsanforderungen berücksichtigt, wie zum Beispiel die Minimierung der Risikofaktoren, die Einführung der Sicherheitsrichtlinie und der IT-Compliance, Berücksichtigung neuer Bedrohungen sowie von Schwachstellen. [Siebenhandl, 2011]

In der Phase Sicherheitskonzept wird überprüft, ob die Kriterien der Standards und Best Practices verwirklicht wurden. Des Weiteren werden die Mitarbeiter über die Sicherheitsrichtlinie informiert. Darüber hinaus werden Mitarbeiterschulungen und Awareness Trainings durchgeführt, damit die Mitarbeiter mit dem Thema Sicherheit vertraut werden. [Siebenhandl, 2011]

Bei der Überprüfung der IT-Sicherheit geht es darum zu kontrollieren, ob die festgelegten Ziele, Anforderungen und Maßnahmen durchgeführt wurden. Dabei richtet sich das Management an bestehende Standards und Best Practices. Anschließend erfolgt die Sicherheitsstatusbewertung. In der letzten Phase werden Korrekturen bzw. Maßnahmen durchgeführt. Wenn die Ergebnisse der Sicherheitsbewertung nicht zufriedenstellend sind, müssen Anpassungen vorgenommen und weitere Evaluierungen durchgeführt werden. [Siebenhandl, 2011]

Das nächste Kapitel befasst sich mit dem wichtigsten Thema der IT-Sicherheitsbewertung. Im folgenden Kapitel wird ein Überblick über die Security Metrics gegeben, anschließend wird die Entwicklung der Sicherheitskennzahlen durchgeführt.

3 Security Metrics

Das folgende Kapitel beschäftigt sich mit Security Metrics. Hier werden zunächst die Security Metrics beschrieben und darauf aufbauend wird der Evaluationsprozess erläutert. Danach wird näher auf die Entwicklung der Kennzahlen eingegangen. Die entwickelten Kennzahlen werden als Kennzahlensteckbrief dargestellt. Außerdem folgt eine Darstellung des Messprozesses basierend auf dem Messmodell ISO/IEC 27004. [ISO/IEC27004, 2016]

Der Bedarf an Security Metrics ist von großer Bedeutung für die Analyse des aktuellen Sicherheitsstatus einer Organisation. Die Unternehmen haben die Möglichkeit mit Hilfe von Security Metrics Informationen über die Bedrohungen, die Schwachstellen und über die Risiken im System zu erhalten. Anhand von IT-Sicherheitskennzahlen wird die Wirkung der Ziele, die für die IT-Sicherheit in der Organisation definiert wurden, überprüft. Des Weiteren wird auch die Implementierung von Sicherheitsrichtlinien geprüft. IT-Sicherheitskennzahlen können für diverse Domänen innerhalb einer Organisation definiert werden. Dabei ist zu beachten, dass die Sicherheitskennzahlen zielorientiert sein sollten. [Patriciu et al., 2006]

Internationale Standards wie zum Beispiel ISO/IEC 27001 helfen dabei, die Sicherheitsdomäne zu bestimmen, die bei der Verbesserung des Informationssicherheitsmanagements zu beachten sind. Somit können sie dazu beitragen die entsprechenden Sicherheitskennzahlen für die Organisationen zu analysieren. [Tashi and Ghernaouti, 2007]
Es wird viel mehr technische IT-Sicherheitskennzahlen wie zum Beispiel „Intrusion Detection Metrics“ verwendet, um den Sicherheitsstatus der Organisation zu bewerten. Jedoch reicht diese Art von Sicherheitskennzahlen nicht aus, um die Gesamtsicherheit einer Organisation zu messen. Daher sind nicht nur technische, sondern auch „Management-Kennzahlen“ erforderlich, um alle Sicherheitsbereiche zu umfassen. Darüber hinaus müssen einige Parameter und Messmethoden definiert werden, um das Sicherheitsniveau der Organisation bewerten zu können. [Tashi and Ghernaouti, 2007]

Der Internationale Standard ISO/IEC 27004 unterstützt den Unternehmen indem er Hinweise zur Entwicklung und Nutzung von Sicherheitsmaßnahmen im Zusammenhang mit der Informationssicherheit

gibt. Der Standard hilft dabei auch die Anforderungen von ISO / IEC 27001 zu erfüllen. [ISO/IEC27004, 2016]

Der Evaluationsprozess der Informationssicherheit und der Effektivität von ISMS beginnt zuerst mit der Überwachung und Messung. Die Organisation muss zunächst bestimmen, was sie bei der Bewertung der Informationssicherheit erreichen möchte, um zu bestimmen, was überwacht und gemessen werden soll. Die Überwachung des Systems ist entscheidend für den Status eines Systems oder eines Prozesses. [ISO/IEC27004, 2016] Zu den Systemen oder Prozessen, die überwacht werden können zählen zum Beispiel:

- Implementation des ISMS Prozesses
- Incident Management
- Access Control
- Firewall und Event Logging
- Risk Assessment Prozess
  [ISO/IEC27004, 2016]

Durch die Überwachung werden Daten erzeugt, die zur Unterstützung anderer Maßnahmen verwendet werden können. Diese Daten sind zum Beispiel Event Logs, Benutzerinterviews, Ausbildungsstatistiken usw. Des Weiteren ermöglicht die Überwachung dem Unternehmen festzustellen, ob ein Risiko eingetreten ist und dementsprechend können Maßnahmen getroffen werden. [ISO/IEC27004, 2016]
Im Gegensatz zur Überwachung ist die Messung eine Tätigkeit, mit Hilfe dessen ein Wert oder der Status der Leistung ermittelt wird. Auf diese Weise können Verbesserungsanforderungen identifiziert werden. Alle ISMS-Prozesse und Kontrollen können gemessen werden. Als Beispiel für die Messung ist, dass eine Organisation feststellen kann, ob alle Personen, die eine Schulung brauchen, diese auch erhalten haben. Dies kann zum Beispiel anhand der Anzahl der trainierten Personen gemessen werden. [ISO/IEC27004, 2016]

Die Aktivitäten Überwachung, Messung, Analyse und Auswertung sind ein Prozess, der aus folgenden Schritten besteht [ISO/IEC27004, 2016]:

- Identifizieren von Informationsbedürfnissen
- Maßnahmen schaffen und pflegen
- Verfahren festlegen
- Überwachen und messen
- Ergebnisse analysieren
- Informationssicherheit und die Effektivität des ISMS bewerten. [ISO/IEC27004, 2016]

Die Abbildung 5 stellt den Prozessablauf grafisch dar.

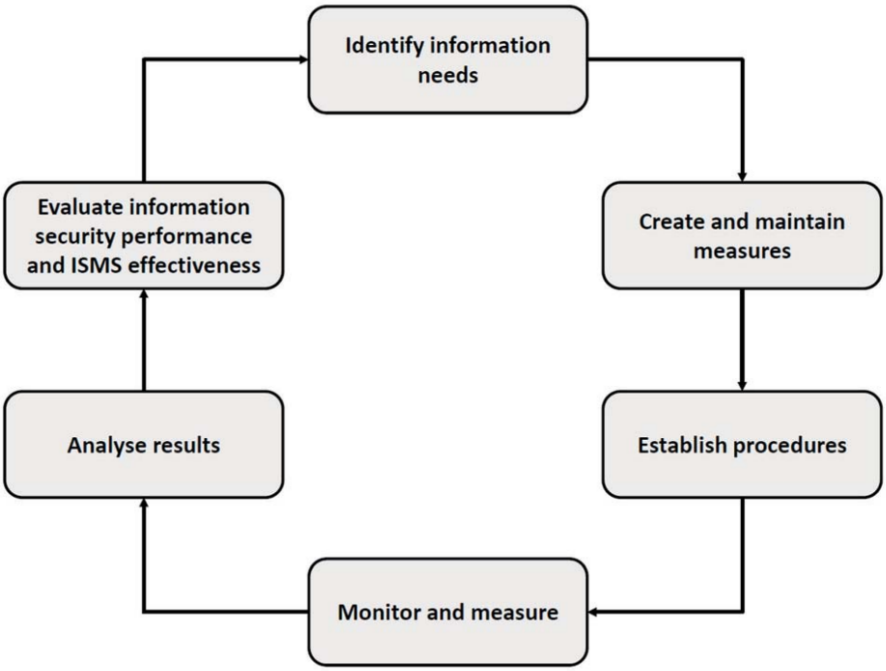

Abb. 5: Monitoring, measurement, analysis and evaluation process [ISO/IEC27004, 2016]

In Bezug auf die Leistung der Informationssicherheit sind auch die Security Controls der Organisation von Bedeutung. Einige Sicherheitskontrollen, die in IT-Security Frameworks wichtig sind, werden unten aufgezählt. [Montesino and Fenz, 2011]

- Zugriffskontrolle
- Control against malicious code
- Backups
- Audit logging
- Control of technical vulnerability
- Network controls
- Key management
- Incident Assessment
  [Montesino and Fenz, 2011]

Jedoch sind nicht alle Security Controls in allen Domänen automatisierbar. Manche Sicherheitskontrollen können nur teilweise automatisiert werden. Es hängt von folgenden Kriterien ab, ob die Sicherheitskontrollen teilweise oder vollständig automatisiert werden können. [Montesino and Fenz, 2011]
Das erste Kriterium ist, dass die Ausführung und Überwachung der Sicherheitskontrollen nur automatisch lesbare, messbare und weiter bearbeitbare Ressourcen voraussetzt. Zum Beispiel kann die Sicherheitskontrolle ‚Awareness Training' nicht automatisiert werden, da das Training für die Mitarbeiter in einer Organisation ist. Das heißt, dass beim Training Menschen beteiligt sind und nicht automatisch gemessen werden kann. Das nächste Kriterium ist, dass die Sicherheitskontrolle teilweise oder vollständig durch eine Sicherheitssoftware automatisiert werden kann. [Montesino and Fenz, 2011]

Auf der folgenden Abbildung 6 ist zu sehen wie viele Security Controls automatisierbar sind.

Domain	Information Security Controls			
	Controls that can be automated	*Total controls*	*Percent*	*Examples of controls*
Security policy	0	2	0.0%	-
Organization of information security	0	11	0.0%	-
Asset management	1	5	20.0%	Inventory of assets
Human resources security	1	9	11.1%	Removal of access rights
Physical and environmental security	2	13	15.4%	Physical entry controls
Communications and operations management	15	32	46.9%	Controls against malicious code
				Information back-up
				Audit logging
Access control	13	25	52.0%	Unattended user equipment
				Network connection control
Information systems acquisition, development and maintenance	4	16	25.0%	Key management
				Control of technical vulnerabilities
Information security incident management	0	5	0.0%	-
Business continuity management	0	5	0.0%	-
Compliance	1	10	10.0%	Technical compliance checking

Abb. 6: Automation possibilities information security management [Montesino and Fenz, 2011]

Ein weiterer wichtiger Punkt, der vor dem Bewertungsprozess bestimmt werden muss, ist die Entscheidung darüber, in welcher Zeitspanne überprüft, gemessen, analysiert und bewertet werden soll. Außerdem muss die Organisation auch festlegen, wer die Analyse durchführt. [ISO/IEC27004, 2016]

Die Wichtigkeit der Sicherheitskennzahlen wurde schon mehrmals in vorherigen Kapiteln angesprochen. Nun wird im nächsten Kapitel die Entwicklung der Sicherheitskennzahlen beschrieben und anschließend Sicherheitskennzahlen für die Analyse entwickelt.

3.1 Entwicklung Sicherheitskennzahlen

Das Problem ist, dass keine Sicherheitskennzahlen verfügbar sind, die eine umfassende Sicherheitsbewertung des gesamten Systems ermöglichen. Daher ist es notwendig, Kennzahlen zu entwickeln, um die Bewertung der Sicherheit in einer Organisation durchführen zu können. Dabei sind zwei Hauptaspekte bei der Entwicklung der Kennzahlen zu berücksichtigen. Der erste Aspekt ist, dass ein geeigneter Sicherheitsindikator für die Bewertung erforderlich ist. Der zweite wichtige Punkt ist, dass eine Methode notwendig ist, die die einzelnen Sicherheitsaspekte zu einer Gesamtsicherheitsbewertung für die Organisation zusammenstellt. [Weiß et al., 2005]

Um Sicherheitskennzahlen zu entwickeln, die die Sicherheit der gesamten Organisation darstellen, müssen bestimmte Anforderungen laut Weiß [Weiß et al., 2005] berücksichtigt werden. Die wichtigsten Kriterien sind:

Umfassende Bewertung der gesamten Organisation:
Es ist nicht nur relevant die einzelnen Aspekte zu messen, die Bewertung des Gesamtsicherheitszustandes einer Organisation ist auch von Bedeutung. Die Gesamtsicherheit umfasst nicht nur Angriffe wie Viren, sondern auch die Ereignisse wie Feuer oder Überschwemmungen. [Weiß et al., 2005]

Objektivität:
Mit Objektivität ist gemeint, dass die Vergleichbarkeit eingefordert werden muss. Mit anderen Worten ausgedrückt, dass Sicherheitsexperten unter ähnlichen Bedingungen ähnliche Sicherheitsergebnisse erzielen. Außerdem muss die wiederholte Anwendung der Kennzahl zu ähnlichen Ergebnissen führen. Somit schließt in diesem Zusammenhang Objektivität auch Wiederholbarkeit ein. [Weiß et al., 2005]

Vergleichbarkeit:
Die Analyseergebnisse müssen mit den Ergebnissen anderer Organisation vergleichbar sein. Darüber hinaus ist es von Bedeutung, die Sicherheitsverbesserungen im Laufe der Zeit zu überwachen und zu messen. [Weiß et al., 2005]

3.2 Entwicklung Kennzahlen zum Testen

Im Rahmen dieser Masterarbeit wurde ein Prototyp für die Bewertung eines Systems entwickelt. Dieser wurde dann vom Unternehmen Plus Mobile getestet. [Plusmobile, 2018] Aus diesem Grund wurde das System des Unternehmens näher betrachtet. Der Webpage des Unternehmens verfügt über einen Login Bereich und über ein Such-Feld. Daher wird das Augenmerk auf die beiden Bereiche gelegt. Im Zusammenhang dazu wurden mögliche Gefahren analysiert und folglich Sicherheitsanforderungen definiert bzw. Sicherheitsziele festgelegt. Das erste Ziel ist die Zugriffsversuche ins System durch Login zu überwachen. Ein weiteres Ziel sind die SQL-Injections Versuche im Such-Feld zu überwachen. In diesem Fall wurden für die Analyse bzw. bei der Definition von Kennzahlen die Security Metrics bzw. die Informationen aus ISO/IEC 27004 Standard und aus NIST SP 800-55 herangezogen. [ISO/IEC27004, 2016] [Chew et al., 2008]

Um die Zugriffskontrolle im System zu analysieren, wird die Kennzahl ‚Anzahl der erfolgreichen Zugriffe' definiert. Mit dieser Kennzahl wird überprüft, wie viele Zugriffsversuche im System stattgefunden haben, beziehungsweise wie viele erfolgreiche und fehlgeschlagene Logins erfolgt sind. Anhand der Audit Logs kann dies analysiert werden. Das Thema wird im Kapitel Test näher erläutert. Mit dieser Analyse kann das Unternehmen sehen, ob die fehlgeschlagenen Zugriffe eine Bedrohung für das Unternehmen darstellen oder nicht. Dazu wird eine Messgröße bzw. ein Parameter von Unternehmen festgelegt. In diesem Fall wird für die Bewertung die Messgröße 80% ausgewählt. Bei der Auswahl von Messgrößen bzw. bei der Definition von Kennzahlen wurden die Informationen in ISO/IEC 27004 Standards und in NIST SP 800-55 berücksichtigt. [ISO/IEC27004, 2016] [Chew et al., 2008]

Tabelle 1 zeigt die definierte Kennzahl in Form des Kennzahlensteckbriefs.

Information Descriptor	Zugriffskontrolle
Name Metric	Anzahl der erfolgreichen Zugriffe
Measure ID	M1
Information need	Zugriffskontrolle der Benutzer, die auf das System zugreifen bewerten
Measure	Anzahl der Zugriffe Anzahl der erfolgreichen Zugriffe
Formula/Scoring	Ratio: 80% (Anzahl der erfolgreichen Zugriffe / Anzahl der Zugriffe)*100 Vergleich des Ergebnisses mit Ratio
Target	Wenn das Ergebnis größer als 80% ist, sind keine Maßnahmen erforderlich
Implementation evidence	Alle erfolgreichen und fehlgeschlagenen Logins zählen, speichern
Frequency	Wöchentlich
Responsible parties	Security Manager
Data source	Audit logs
Reporting format	Pie Chart, Table

Tabelle 1: Anzahl der erfolgreichen Zugriffe

Das zweite Ziel ist die SQL-Injections Versuche in den Suchfeldeingaben zu überwachen beziehungsweise zu erkennen. Hier wird nach häufig gesuchten Buchstaben, Sonderzeichen, Zahlen sowie Symbolen analysiert. In diesem Fall geht es nicht darum SQL-Injection zu verhindern. Es geht vielmehr darum, die Angriffsversuche mit Suchfeldeingaben zu überprüfen. Dazu wurde die Kennzahl ‚Anzahl der sicheren Sucheingaben' definiert. Anhand dieser Analyse kann das Unternehmen feststellen, ob eine mögliche SQL-Injection Bedrohung vorhanden ist oder nicht. Dabei werden die Sucheingaben im Suchfeld analysiert. Mit dieser Analyse wird überprüft, wie viele sichere Suchen beziehungsweise wie viele unsichere Suchen stattgefunden haben. Auch in diesem Fall muss das Unternehmen eine Messgröße definieren. Als Parameter wird hier 80% definiert, um eine Bewertung durchführen zu können. Für die Analyse wurden die

Informationen aus ISO/IEC 27004 Standard und aus NIST SP 800-55 herangezogen. [ISO/IEC27004, 2016] [Chew et al., 2008]

Tabelle 2 zeigt die definierte Kennzahl in Form des Kennzahlensteckbriefs.

Information Descriptor	SQL-Injection
Name Metric	Anzahl der sicheren Suche
Measure ID	M2
Information need	Analyse der Suchfeldeingaben auf mögliche SQL-Injection Versuche
Measure	Anzahl der gesamten Suche Anzahl der sicheren Suche
Formula/Scoring	Ratio: 80% (Anzahl der sicheren Suche / Anzahl der gesamten Suche)*100 Vergleich des Ergebnisses mit Ratio
Target	Wenn das Ergebnis größer als 80% ist, sind keine Maßnahmen erforderlich
Implementation evidence	Alle gesuchten Sucheingaben zählen, speichern
Frequency	Wöchentlich
Responsible parties	Security Manager
Data source	Search Logs
Reporting format	Pie Chart, Table

Tabelle 2: Anzahl der sicheren Suche

Im nächsten Kapitel wird das ISO-Messmodell beschrieben und basierend auf das Messmodell wird ein Messprozess modelliert.

3.3 Messmodell ISO/IEC 27004:2016

Der ISO/IEC 27004 Standard stellt ein Messmodell bereit, das auf Information Management Security Systems (ISMS) angewendet werden kann. Um die Performance und Effektivität des ISMS zu bewerten, müssen Indikatoren, nämlich Key Performance Indicators (KPI), identifiziert werden. Die Organisation bestimmt „Base measures“ und leitet daraus „Derived measures“ ab, indem eine Messfunktion verwendet wird, die zwei oder mehrere „Base measures“ verwendet. Auf diese Weise können Key Performance Indicators (KPI) ermittelt werden. [ISO/IEC27004, 2016]

Das Messmodell in der Abbildung 7 ist ein Beispiel dafür. Es gibt auch andere alternative Betrachtungsweisen, um die Prozesse der Messung, Analyse und Bewertung zu modellieren. [ISO/IEC27004, 2016]

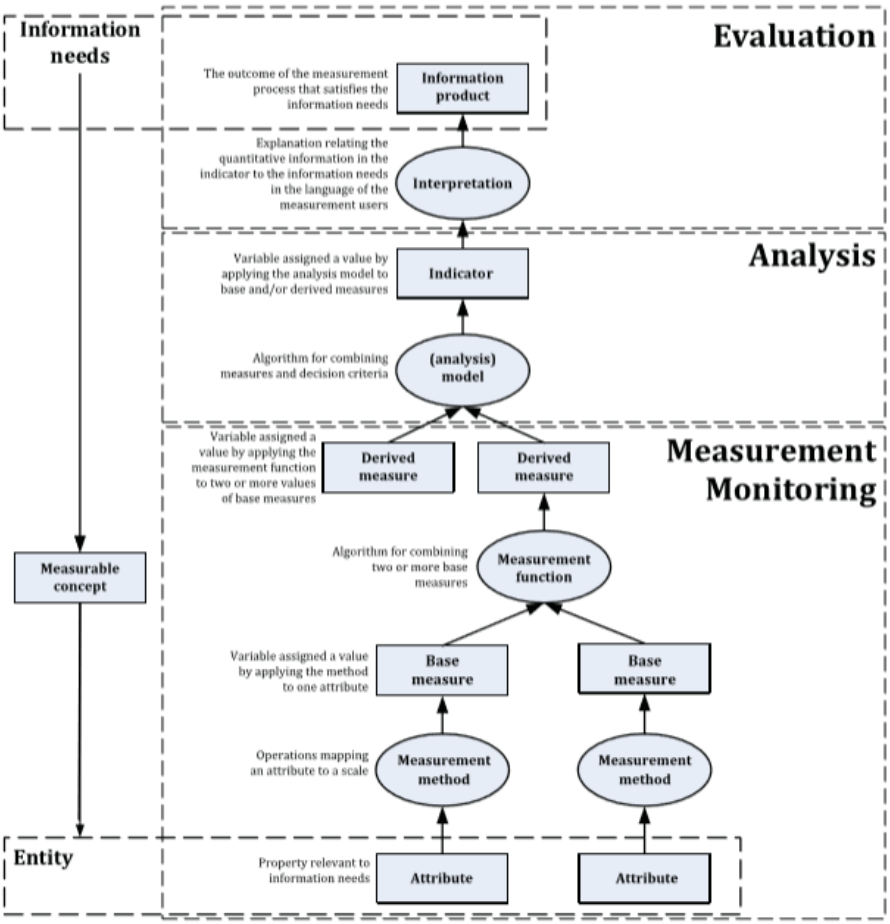

Abb. 7: Plan-Do-Check-Act Zyklus [ISO/IEC27004, 2016]

Um Messungen durchführen zu können, muss zuerst definiert werden, welche Attribute zu den Security Controls gehören. Das heißt, es werden sicherheitsrelevante Attribute ermittelt, die für die Bewertung erforderlich sind. [Peláez, 2010]

Securtiy Control	**Attribute**
Audit logging	Audit Logs von erfolgreichen Zugriffen
	Audit Logs von fehlgeschlagenen Zugriffen
Controls against malicious code	Search Logs von sicheren Sucheingaben
	Search Logs von nicht sicheren Sucheingaben

Tabelle 3: Kontrollattribute

Von den Kontrollattributen werden „Base Measures“ entworfen. Um eine Bewertung durchführen zu können, müssen die Maßnahmen quantitativ bestimmbar sein. Als Vergleichsbasis eignet sich der Prozentsatz um die Performance der Security Controls zu messen. Die Bewertung erfolgt indem die ‚Derived Measures aus den ‚Base Measures‘ als Prozentanteil abgeleitet werden und mit dem definierten Grenzwert bzw. Indicator verglichen werden. [Peláez, 2010]

Base Measures	**Derived Measures**	**Target/Indicator**
Anzahl der erfolgreichen Zugriffe	(Anzahl der erfolgreichen Zugriffe/Anzahl aller Zugriffe)*100	80%
Anzahl aller Zugriffe		
Anzahl der sicheren Sucheingaben	(Anzahl der sicheren Sucheingaben/Anzahl aller Sucheingaben)*100	80%
Anzahl aller Sucheingaben		

Tabelle 4: Base Measures-Derived Measures

Wenn die Ergebnisse dem definierten Grenzwert entsprechen oder größer sind, kann man davon ausgehen, dass die Zugriffskontrollen und die Sucheingaben im sicheren Bereich liegen und daher keine Maßnahmen erforderlich sind.

In den nächsten zwei Abbildungen wird der Mess-Prozess basierend auf dem Messmodel ISO/IEC 27004:2016 grafisch dargestellt. [ISO/IEC27004, 2016] Die Abbildung 8 zeigt das Messmodel für Zugriffsversuche und die Abbildung 9 für Sucheingaben.

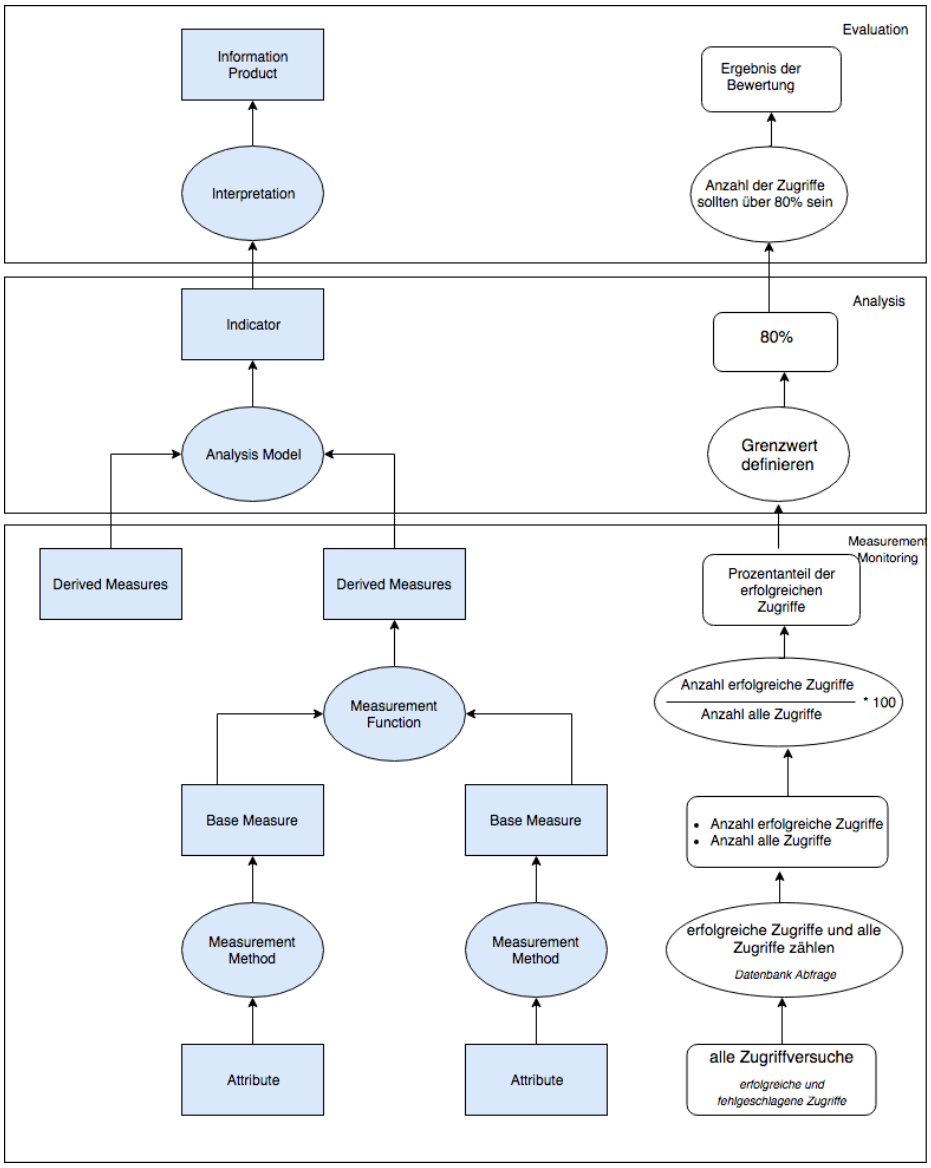

Abb. 8: Messbeispiel für Zugriffsversuche [ISO/IEC27004, 2016], (eigene Darstellung)

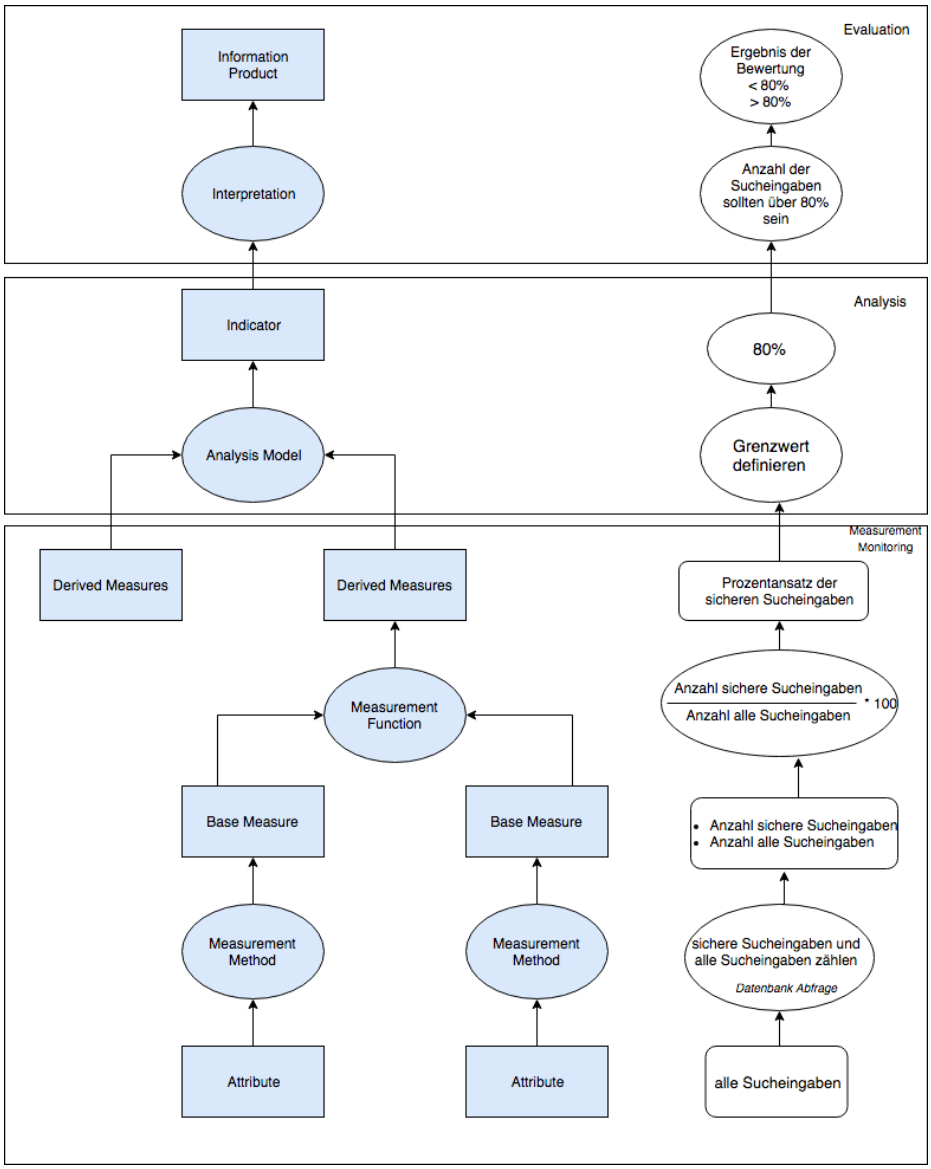

Abb. 9: Messbeispiel für Sucheingaben [ISO/IEC27004, 2016], (eigene Darstellung)

4 Balanced Scorecard-(BSC)

In diesem Kapitel wird die Balanced Scorecard behandelt. Zuerst wird ein Überblick über die Balanced Scorecard gegeben. Als nächstes werden die IT-Security Balanced Scorecard und die einzelnen Perspektiven von ITSec BSC näher erläutert. Schließlich werden die Merkmale der Sicherheitsleistungsmessung beschrieben und die im Rahmen dieser Arbeit modellierte IT-BSC dargestellt.

Heutzutage sind Organisationen immer mehr von computergestützten Informationssystemen abhängig. Störungen in den Systemen können dem Unternehmen Sorgen bereiten, aber auch zu Katastrophen führen. Die Technologie-Abhängigkeit verursacht, dass neue Cyberkriminalität und andere Informationssystemrisiken zunehmen. Daraus folgt, dass ein Bedarf an IT-Sicherheit auch zunimmt. [Herath et al., 2010]
Die Risikomanagementstrategie des Unternehmens sollte alle wesentlichen Bedrohungen der Organisation behandeln. Um dies gewährleisten zu können, ist ein integrierter Ansatz erforderlich. Mit Hilfe dieses Ansatzes können IT- Sicherheitsmanager bewerten, ob Sicherheitsinvestitionen die organisatorischen Ziele erfüllen. Es ist erforderlich Ziele zu setzen und Leistungsmaßnahmen zur Bewertung von Sicherheitsprozessen zu entwickeln. [Herath et al., 2010]

In vielen Unternehmen werden Performance Messsysteme eingesetzt, um den Fortschritt bei der Zielerreichung zu überwachen. Außerdem werden die Ursachen für nicht zufriedenstellende Leistungen identifiziert und somit laufende Verbesserungen verwaltet. Als Performance Messsystem verwenden die Unternehmen meistens die Balanced Scorecard (BSC). Der Grund dafür ist, dass das Balanced Scorecard-Modell in der Praxis weit verbreitet ist. [Herath et al., 2010]

Die Balanced Scorecard (BSC) ermöglicht ein Modell, das die finanziellen Maßnahmen durch die nicht-finanziellen Maßnahmen in drei zusätzlichen Perspektiven ergänzt, nämlich in Kunden, interner Prozess und Lernen und Innovation. Des Weiteren bietet es eine Auswahl von mehreren Performance-Maßnahmen im Zusammenhang mit strategischen Zielen. [Herath et al., 2010] Die Balanced Scorecard kann als Framework im Unternehmen eingesetzt werden, das die langfristigen Strategieziele eines Unternehmens mit kurzfristigen Maßnahmen kombiniert. [Kaplan and P. Norton, 2007]

Abbildung 10 zeigt das von Kaplan und Norton [Kaplan and P. Norton, 1991] eingeführte BSC-Modell. Besonders hervorzuheben ist in diesem Zusammenhang, dass die Bewertung einer Organisation nicht nur finanzielle Bewertung berücksichtigt. Die Kundenzufriedenheit, die internen Prozesse und die Lern- und Innovationsfähigkeit sollte auch in die Bewertung miteinbezogen werden. [Herath et al., 2010]

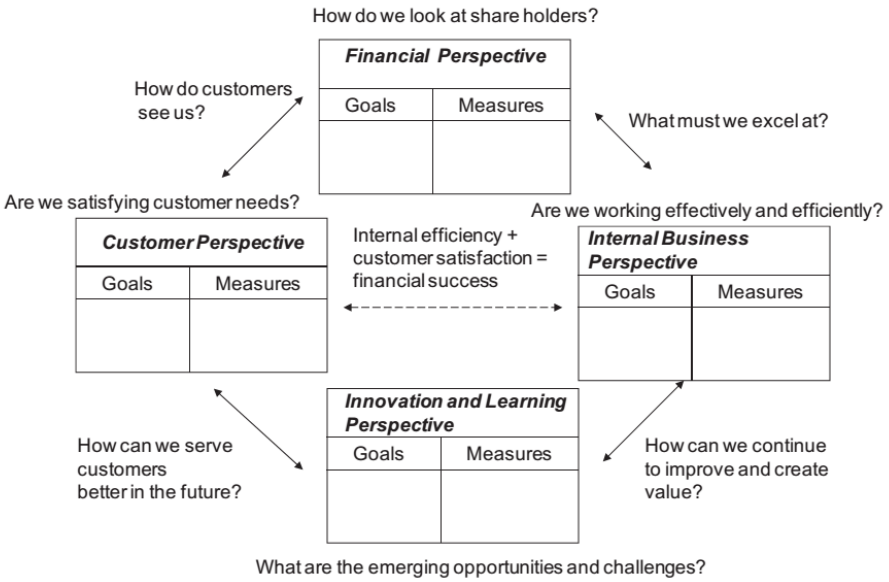

Abb. 10: Kaplan and Norton 1992 generic model [Herath et al., 2010]

Die 4 Perspektiven im Balanced Scorecard Modell, die in Abbildung 10 dargestellt sind:

- **Innovation and Learning:**
  In dieser Perspektive werden Kennzahlen identifiziert, die für den Wettbewerbserfolg von Unternehmen beitragen. Diese Performance-Kennzahlen für diese Perspektive im Balanced Scorecard kann zum Beispiel in Bildungskapital, in Informationskapital und in Organisationskapital unterteilt werden. [Herath et al., 2010]

– **Internal Business:**
  Die Perspektive ‚Internal Business' kann auch als prozessbasierte Sichtweise betrachtet werden, die vier Kernbereiche, nämlich das Betriebsmanagement, das Kundenmanagement, die Innovation und die soziale Aspekte beinhaltet. [Herath et al., 2010]

– **Customer Perspective:**
  Die Kunden-Perspektive (Customer Perspective): Hier liegt der Fokus auf Kunden. Dabei wird ein Wert auf Kundennutzen und auf das Kundenbeziehungsmanagement gelegt. [Herath et al., 2010]

– **Financial Perspective**
  Die finanzielle Perspektive (Financial Perspektive) fokussiert sich auf finanzielle Kennzahlen. Mit Hilfe dieser Kennzahlen können im Unternehmen zum Beispiel Maßnahmen wie Return on Investment und Gewinnwachstum gemessen werden. [Herath et al., 2010]

Die Balanced Scorecard (BSC) ist als entscheidungsunterstützendes Werkzeug auf der strategischen Managementebene entstanden. Martinsons [Martinsons et al., 1999] adaptierten die Balanced Scorecard und entwickelte eine Balanced Scorecard, die die IS-Aktivitäten aus den folgenden Perspektiven misst und bewertet. Diese Perspektiven sind: „Business Value Perspective, User Orientation Perspective, Internal Process Perspective und Future Readiness Perspective." [Herath et al., 2010]

Die IT-Abteilung ist in der Regel eher ein interner als ein externer Service. Aber die Projekte werden sowohl für die Endnutzer als auch für die Organisation durchgeführt. [Herath et al., 2010] Aus diesem Grund adaptierten Martinsons [Martinsons et al., 1999] die Balanced Scorecard.

In der Abbildung 11 ist die Balanced Scorecard von [Martinsons et al., 1999] dargestellt.

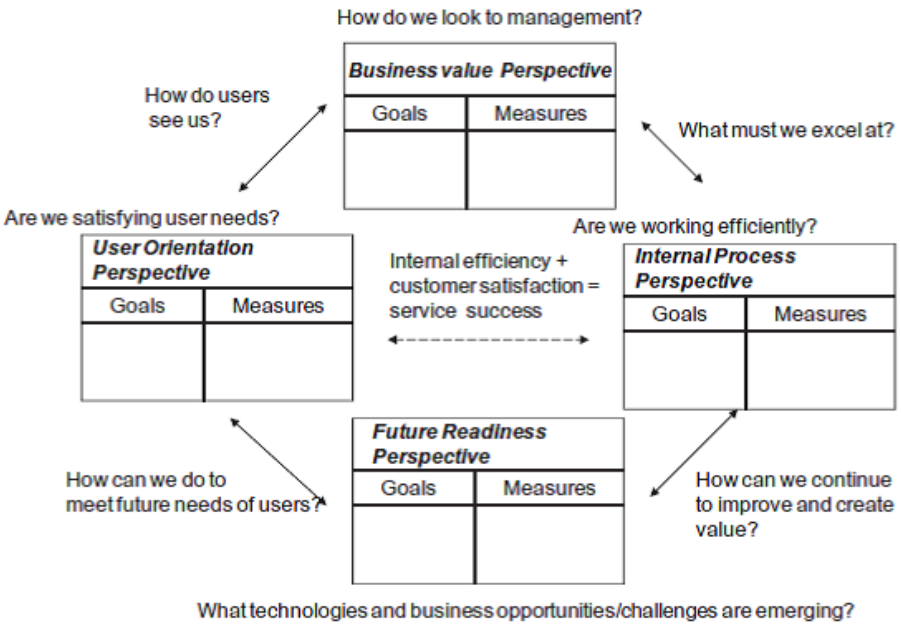

Abb. 11: Martinson BSC model for Information Systems. [Herath et al., 2010]

Die IT-Sicherheit kann von vielen Faktoren beeinflusst werden. Zum Beispiel müssen Unternehmen vielen Vorschriften wie Buchhaltungsvorschriften Datenschutzbestimmungen und internationalen Vorschriften folgen. Diese Vorschriften wirken sich auf IT-Sicherheit in Organisationen aus. [Herath et al., 2010]
Aufgrund der Finanzskandale der beiden amerikanischen Unternehmen Enron und WorldCom wurde in den USA der Sarbanes-Oxley Act (SOX) verabschiedet. Das Ziel dieses Gesetzes ist Finanzbetrug zu verhindern. Die meisten Buchhaltungsunterlagen werden mit IT-Programme erstellt und gepflegt. Aus diesem Grund stellen interne und externe Bedrohungen ein grundlegendes Risiko für das Unternehmen dar. [Herath et al., 2010]

Die meisten Unternehmen sind immer mehr von ihren IT-Systemen abhängig. Daher ist die Verwaltung von IT-Systemen sehr wichtig. Zudem

definiert die Information Security Governance (ISG) fünf gewünschte Ergebnisse der Information Security Governance (ISG). [Institute, 2006] Diese sind:

- Strategische Ausrichtung: Anpassung der Informationssicherheit an die Geschäftsstrategie, um die organisatorischen Ziele zu unterstützen. [Institute, 2006]

- Risikomanagement: Durchführung und Implementierung geeigneter Maßnahmen zur Bewältigung und Senkung von Risiken und um die möglichen Auswirkungen auf Informationsressourcen gering zu halten. [Institute, 2006]

- Ressourcenmanagement: Effiziente und effektive Verwaltung von IT-Sicherheit Know-how und die Infrastruktur. [Institute, 2006]

- Performance-Messung: Bewertung, Überwachung und Reporting von Sicherheitskennzahlen, um sicherzustellen, dass die organisatorischen Ziele erreicht sind. [Institute, 2006]

- Wertschöpfung: Die Informationssicherheitsinvestitionen zu optimieren, um die Unternehmensziele zu unterstützen. [Institute, 2006]

4.1 IT-Security Balanced Scorecard

Um die geschäftlichen Aspekte der Organisation zu überwachen, werden meistens Balanced Scorecards eingesetzt. Ein ähnlicher Ansatz kann aber auch verwendet werden, um die IT-Sicherheitsaspekte eines IT-Systems zu überwachen und zu verwalten. [Issa Atoum, 2016]

Die modifizierte Balanced Scorecard von Herath (2010) [Herath et al., 2010] trägt den Namen ITsec BSC und besteht aus vier Perspektiven.

Business Value-Perspektive von ITSec BSC
Die Informationssicherheit steht im Zusammenhang mit dem Schutz der wertvollen Informationen beziehungsweise Daten. Die Daten werden vor Verlust, unangemessener Offenlegung oder Beschädigung während der Übertragung oder Verarbeitung geschützt. Diese Perspektive deckt die wichtigsten Sicherheitsziele ab. [Herath et al., 2010]

Diese Sicherheitsziele sind:

- Vertraulichkeit: Daten und Informationen werden nur an diejenigen weitergegeben, die auch das Recht haben. [Herath et al., 2010]
- Integrität: Daten und Informationen vor unbefugter Änderung geschützt. [Herath et al., 2010]
- Verfügbarkeit: Informationssysteme sind verfügbar und können bei Bedarf genutzt werden und können den Angriffen standhalten. [Herath et al., 2010]
- Authentizität und Verbindlichkeit: beinhaltet die Echtheit und die Glaubwürdigkeit der Business Transaktionen und die Verbindlichkeit der Transaktion. [Herath et al., 2010]

Stakeholder Orientation of ITSec BSC
Die Informationssicherheit ist ein wichtiger Bestandteil der IT-Governance und kann als gewinnsteigernde Investition betrachtet werden. Des Weiteren müssen Sicherheitsmanager bei der Bereitstellung der IT-Sicherheitsdienste die Benutzern und Stakeholdern berücksichtigen. Aus Kundensicht ist es zum Beispiel wichtig die organisatorischen Praktiken ausreichend abzusichern, da Kunden mehr Online Aktivitäten durchführen, wenn sie in die E-Transaktionen vertrauen. [Herath et al., 2010]

Interne Prozessperspektive von ITSec BSC
Die internen Prozesse stehen in Bezug auf die Planung, Beschaffung,

Bereitstellung und Wartung von IT-Produkten und IT-Diensten. Außerdem beziehen sie sich auf die Verwaltung von Anfragen von verschiedenen Systembenutzern und Stakeholdern. Um die internen sicherheitsrelevanten Tätigkeiten bewerten zu können, müssen die drei grundlegenden Prozesse gemessen und bewertet werden. [Herath et al., 2010] Diese sind: „Planung und Priorisierung von Sicherheitsinitiativen, Einsatz von Sicherheitsdiensten und Sicherheitsprodukten, Operationen und Wartung der aktuellen Sicherheitsdienste.“ [Herath et al., 2010]

Diese Prozesse können wie beispielsweise mit dem Prozentanteil der für diese Aktivitäten bereitgestellten Ressourcen bewertet werden. Weitere Möglichkeiten für die Bewertung der Prozesse sind zum Beispiel die Anzahl der bereitgestellten Anwendungen und Dienste, die Anzahl der abgewickelten Abfragen und die für diese Abfragen aufgewendete Zeit und die Anzahl der verhinderten Bedrohungen. Die Reduzierung der E-Mail-Bedrohungen und der Schwachstellen durch Verbesserungen der Intrusion Detection System-Leistungsziele wäre ein Beispiel für die ITSec BSC-Perspektive des internen Prozesses. [Herath et al., 2010]

Future Readiness Perspektive von ITSec BSC
Um die Daten vor Verlust oder vor Beschädigung während der Speicherung, Übertragung oder Nutzung zu schützen, werden im Unternehmen Gegenmaßnahmen getroffen. Das Problem ist jedoch, dass sich die Bedrohungen auch ständig weiterentwickeln. Zum Beispiel haben sich in den letzten zehn Jahren neue IT-Sicherheitsbedrohungen entwickelt. [Herath et al., 2010] Die Verbreitung von Viren durch Disketten waren früher die Hauptbedrohungsquelle. Diese wurden aber durch Bedrohungen wie E-Mail-Viren ersetzt. Daher ist die kontinuierliche Schulung von IT-Sicherheitspersonal und Benutzern ein Aspekt der Future Readiness Perspektive. [Herath et al., 2010]

In der nachfolgenden Abbildung ist die im Rahmen dieser Arbeit modellierte IT-BSC dargestellt.

Abb. 12: IT-BSC (eigene Darstellung)

Als erstes werden die Ziele der Organisation ermittelt, anschließend werden die quantifizierbaren Metrics definiert. In Abbildung 12 wird die Assoziation der Ziele mit den Metrics grafisch dargestellt. Die IT-Sicherheit im Unternehmen sicherzustellen ist nicht nur kompliziert, sondern auch kostenintensiv. Das Ziel in der Business Value Perspektive ist primär die IT-Kosten zu kontrollieren. Daher ist ein wichtiges Ziel zum Beispiel die Kosten zu reduzieren. [Keyes, 2005] Da die Zufriedenheit der Kunden einen Einfluss auf den finanziellen Erfolg hat, ist das Ziel im User Orientation Perspective zum Beispiel die Erhöhung der Website-Besuche. Anhand der Anzahl der neuen Besucher und der Anzahl der wiederkehrenden Besucher kann gemessen werden, wie viele neue Besucher beispielsweise pro Monat auf die Website aufmerksam werden bzw. wie viele wiederkehrende Besucher auf www.Plusmobile.at Services wie zum Beispiel Reparatur-Anfragen in Anspruch nehmen. [Keyes, 2005] [Plusmobile, 2018] Die Ziele der internen Prozesse bzw. der Internal Process Perspective sind die Verbesserung der Zugriffskontrolle und die Reduzierung der SQL-Injection Angriffe. Im Rahmen dieser Arbeit werden diese zwei Ziele näher betrachtet und anhand der definierten Sicherheitskennzahlen die Sicherheitslage des Unternehmens gemessen und bewertet. In diesem Fall wird veranschaulicht, wie die Bewertung der Sicherheit im System erfolgt. Dazu wird ein Prototyp

entwickelt und getestet.
Um kontinuierliche Verbesserung anbieten zu können und um auf zukünftige Herausforderungen vorbereitet zu sein, ist es wichtig, dass sich die Mitarbeiter im Unternehmen auch weiterbilden. Daher ist im Future Readiness Perspective das Training der Mitarbeiter das Ziel. [Keyes, 2005]

Im folgenden Absatz werden die Merkmale der Performance-Messungen beschrieben.

4.2 Merkmale der Sicherheitsleistungsmessung

Bei der Entwicklung einer Balanced Scorecard für die Informationssicherheit sind Schlüsselkonzepte aus der Literatur zur Leistungsmessung relevant. In der Literatur dokumentierte Leistungsmessmerkmale haben Auswirkungen auf alle BSC-Anwendungen. [Herath et al., 2010] Ein wichtiger Punkt ist die Betrachtung der BSC-Maßnahmen der Organisation auf unterschiedliche Weise, da sich die Maßnahmen auf der Balanced Scorecard im Laufe der Zeit ändern. Eine Voraussetzung ist, dass die Performance-Messungen objektiv und überprüfbar sein müssen. Außerdem müssen sie auditiert werden können. [Herath et al., 2010]

Die organisatorischen Funktionen sind eine andere Dimension. Die Maßnahmen in den folgenden vier Kategorien, Inputs, Aktivitäten, Outputs und Ergebnisse verwenden viele Performance Messmodelle. Daraus folgt, dass eine Balanced Scorecard für Informationssicherheit, die aus einer Mischung von Maßnahmen in diesen vier Kategorien besteht, eine Perspektive bietet. [Herath et al., 2010] Eine Balanced Scorecard für das Informationssicherheitsmanagement sollte eine Mischung aus allgemeinen Maßnahmen und aus spezifischen Maßnahmen bestehen. Die Verwendung von allgemeinen Maßnahmen bietet den Vorteil, dass die Informationssicherheitsinformationen nach dem neuesten Stand der Technik integriert werden können. [Herath et al., 2010]

Ein Beispiel für die allgemeinen Maßnahmen ist das National Institute of Standards [Chew et al., 2008], das einen Leitfaden zum Performance-Messung für die Informationssicherheit herausgegeben hat. Das Modell für die Informationssicherheit verwendet keine Balanced Scorecard, aber die Konzepte können in einer BSC-Implementierung verwendet werden. Das Handbuch enthält einen Anhang mit allgemeinen Beispielen für Sicherheitsmaßnahmen. [Chew et al., 2008]

Die akademische Literatur ist eine weitere Quelle für die Verwendung der allgemeinen Maßnahmen. Das von [Huang et al., 2006] entwickelte BSC-Modell für Informationssicherheitsmanagement enthält eine Strategiekarte mit 12 Strategiethemen und 35 KPIs. Die Strategiekarte des Modells zeigt, wie Strategiethemen mit wichtigen KPIs (Key Performance Indicator) verknüpft werden können. Die 35 Indikatoren sind „gemeinsame Maßnahmen“für die Informationssicherheit. [Huang et al., 2006]

Eine wichtige Voraussetzung für alle KPIs ist die, dass sie messbar, realistisch und zeitnah sein müssen. Darüber hinaus müssen zu den Kennzahlen auch die richtigen Grenzwerte definiert werden. Die KPIs werden immer in einem Zeitintervall, zum Beispiel pro Tag oder pro Monat gemessen. Ebenso wichtig ist es, dass die Kennzahlen mit allen beteiligten Business-Partnern abgestimmt und vereinbart werden müssen. [Huang et al., 2006]

5 Modellentwicklung

In dem folgenden Kapitel wird das entwickelte Modell dargestellt und näher beschrieben. Des Weiteren werden das Klassendiagramm, das Komponentendiagramm, das Prozessdiagramm und die Use Cases erklärt. Anschließend wird die IT-BSC Plugin Architektur veranschaulicht.

Vor der Erstellung des Prototyps wurde eine ausführliche Recherche durchgeführt, um herauszufinden, wie so ein Evaluations-Tool entwickelt werden könnte. Zusätzlich musste ein System bestimmt werden, um den Prototyp testen zu können.

Vor der Implementierung des Prototyps wird zunächst das IT-Security Bewertungs-Modell entwickelt. Aufbauend auf das Modell wird der Prototyp implementiert und im nächsten Kapitel wird die prototypische Implementierung beschrieben.

Die nächste Abbildung 13 stellt das entwickelte Modell dar.

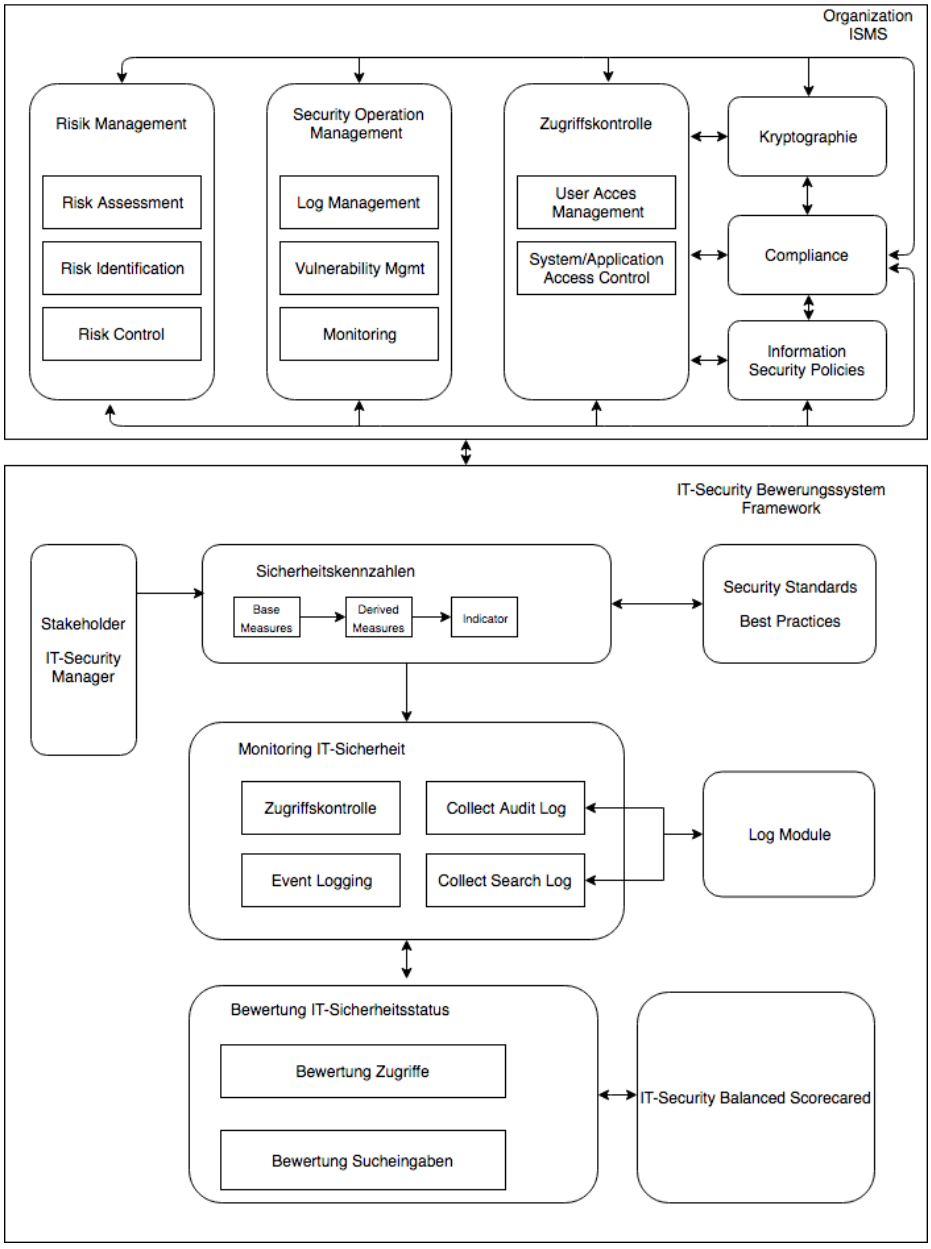

Abb. 13: IT-Security Bewertungssystem Modell (eigene Darstellung)

Informationssicherheitsmanagement ist ein wichtiges Thema in Organisationen. Organisationen können ihre IT-Risiken identifizieren und analysieren. Neben dem Risikomanagement sind noch andere Bereiche im Unternehmen zu berücksichtigen, um die Sicherheit der Organisation gewährleisten zu können. Alle Aktivitäten im System wie zum Beispiel Administratoraktivitäten und Benutzeraktivitäten, aber auch Fehler im System sollten protokolliert und geschützt werden. Monitoring, Log Management und Vulnerability Management sind dafür zuständig und wird als Security Operation Management zusammengefasst. [ISO27k, 2018]

Einer der wichtigsten Punkte ist die Zugriffskontrolle. Unter User Access Management werden Zugriffsrechte der Benutzer und Passwörter überprüft, verwaltet und aktualisiert. Außerdem sollte der Zugriff auf Informationen im System gemäß Sicherheitsrichtlinien eingeschränkt bzw. kontrolliert werden. In Hinsicht der Informationssicherheit müssen Unternehmen ihre Verpflichtungen gegenüber Behörden und anderen Dritten identifizieren und dokumentieren. Daher ist Compliance ein wichtiger Bestandteil im Unternehmen. [ISO27k, 2018]
Eine der essentiellen Aufgaben des Unternehmens ist die Definition der Informationssicherheitsrichtlinien. Die Verwendung von Verschlüsselung und kryptografischen Authentifizierungselementen ist unter Kryptographie zusammengefasst und es wird dafür auch eine Richtlinie definiert. [ISO27k, 2018]

Um Informationen über die Sicherheitslage des Systems zu haben, wird im Rahmen dieser Arbeit ein Modell entwickelt. Das Modell gibt einen Überblick über das IT-Security Bewertungssystem. Um den IT-Sicherheitsstatus des Systems zu messen und zu bewerten, müssen Sicherheitskennzahlen definiert werden. Im Rahmen dieser Arbeit wurden zwei IT-Sicherheitskennzahlen entwickelt. Diese Kennzahlen sind ‚Anzahl der erfolgreichen Zugriffe' und ‚Anzahl der sicheren Sucheingaben'. Die Entwicklung von Kennzahlen ist im Kapitel Kennzahlen Entwicklung genauer beschrieben.

Einer der wichtigsten Aufgaben in der Check-Phase des Plan-Do-Check-Act Zyklus ist die Überwachung der IT-Sicherheit. Es werden die Zugriffskontrolle und das Event Logging überwacht. Des Weiteren werden die Logs wie zum Beispiel Audit- und Search Logs, protokolliert, um die Bewertung durchführen zu können. Die Log-Daten

sind in Log Modulen zu finden. Hier sind Log-files, Firewall Protokolle etc. zu finden.

Der zweite Prozessschritt in der Check-Phase ist die Bewertung des IT-Sicherheitsstatus. Die Zugriffsversuche und die Sucheingaben werden bewertet und die Ergebnisse der Bewertung werden in der IT-Security Balanced Scorecard angezeigt. Neben den Ergebnissen und dem Status ist auch eine grafische Darstellung gegeben. Dazu wird im Kapitel Prototyp Implementierung näher eingegangen.

Für die Bewertung des Sicherheitsstatus eines Systems wurde ein WordPress Plugin entwickelt. Die Begründung für die Entwicklung des Plugins ist die, dass die Plugin Architektur und die Funktionen erweitert werden können. WordPress ermöglicht außerdem die Daten anhand von Template Files zu rendern. [WordPress, b] [WordPress, a]
Zur Installation wird die vorhandene Plugin-Oberfläche in WordPress verwendet. Das Plugin wird für das Unternehmen zur Verfügung gestellt. Der Admin kann dann das entwickelte Plugin installieren.

In Abbildung 14 ist das WordPress Architecture Diagramm dargestellt.

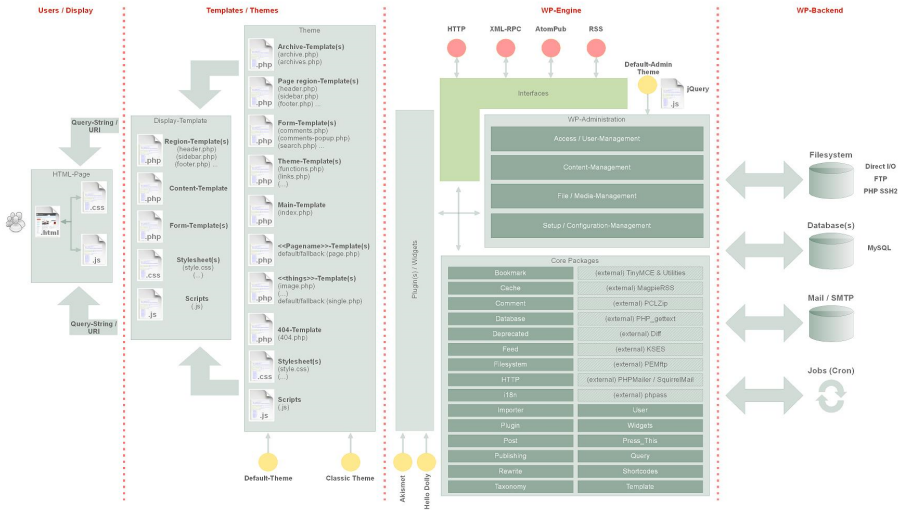

Abb. 14: WordPress Architecture (Omkar Software) [OmkarSoft, 2018]

Die WordPress Struktur besteht aus vier Teilen, nämlich aus Display, Templates, WP-Enginge und WP-Backend. [OmkarSoft, 2018]

Das für diese Masterarbeit entwickelte WordPress Plugin besteht aus mehreren Funktionen, die in PHP-Skriptsprache geschrieben sind. Für die Erstellung des PHP-Codes wird PHPStorm verwendet, da PHPStorm für die Arbeit mit WordPress geeignet ist. Als Datenbank wird eine MySQL Datenbank verwendet. [PhpStorm, 2018] [MySQL, 2018]

Im nächsten Kapitel wird es einen Überblick über die Architektur des entwickelten Plugins gegeben.

ITBSC-Plugin Architektur

In der nächsten Abbildung ist die ITBSC Plugin Architecture abgebildet.

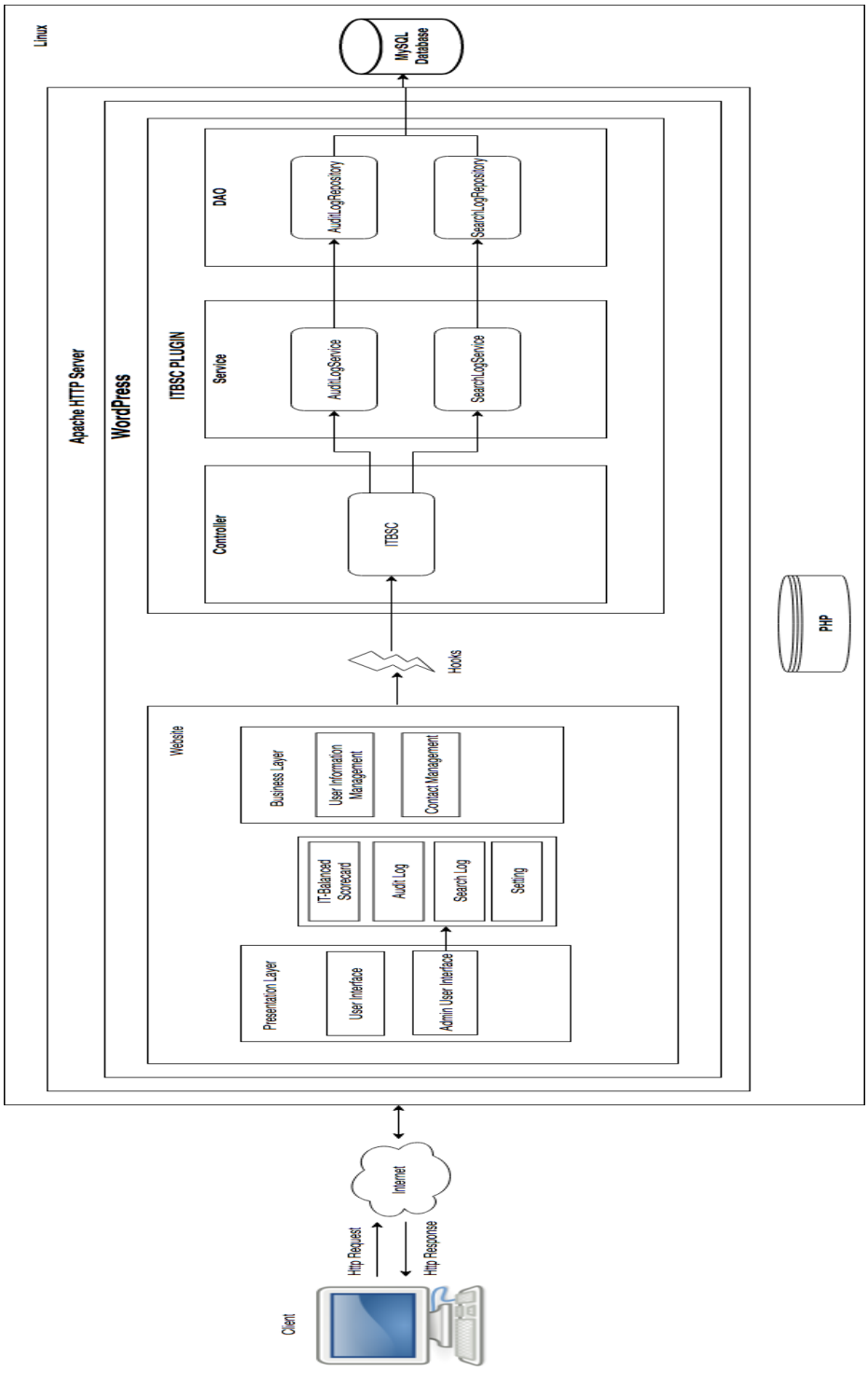

Abb. 15: ITBSC Plugin Architectur (eigene Darstellung)

Es wird ein HTTP Request vom Client an WordPress gesendet. Das Unternehmen Plusmobile verwendet den Linux Server, in dem PHP, Apache http Server und die MySQL Datenbank aufgebaut sind. WordPress wird über den Apache-Server ausgeführt. In WordPress kann dann das Plugin installiert werden. Da WordPress das ITBSC Plugin verwendet, werden dann nur die Hooks bzw. Events berücksichtigt, die für ITBSC Plugin auch relevant sind. Diese Events sind User Login, Admin Login und Search. Im WordPress sind User Login und Admin Login als Action-Hook und Search als Filter-Hook definiert. [WordPress, b]
Im Presentation Layer gibt es zwei User Interfaces, nämlich das Admin User Interface, in dem er das Plugin bedienen kann und das User Interface für alle anderen Benutzer, die nicht auf das Plugin zugreifen können. Des Weiteren verfügt das System über User Information Management, in dem Benützer verwaltet werden. Außerdem gibt es Contact Management, damit die Benützer über das Kontaktformular auf der Website das Unternehmen kontaktieren können. [Plusmobile, 2018]

Sobald der Admin oder der Benutzer versucht sich im System einzuloggen, werden die relevanten Events im Controller abgehört. Diese werden weiter an das Service gesendet. Nachdem die benötigten Daten der Events gesammelt wurden, werden sie in der Datenbank gespeichert. Der Admin kann Daten unter Audit Log und unter Search Log sehen. Des Weiteren kann er den Grenzwert für die Bewertung unter Setting definieren. Anschließend findet dann die Bewertung statt und es werden unter IT-Balanced Scorecard die Ergebnisse sowie die Grafik dazu angezeigt. Eine detaillierte Beschreibung der einzelnen Funktionen erfolgt im nächsten Kapitel Prototyp Implementierung.

In der folgenden Abbildung ist der Prototyp bzw. das Plugin Modell IT-BSC abgebildet.

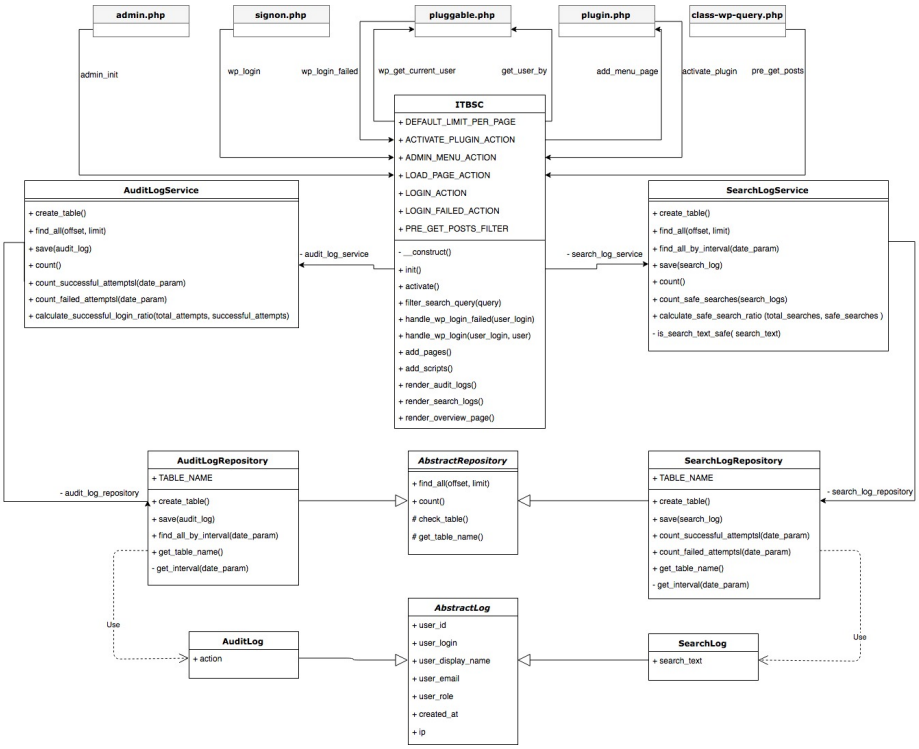

Abb. 16: Plugin Klassendiagramm IT-BSC (eigene Darstellung)

Das Klassendiagramm zeigt die Beziehungen zu den jeweiligen Klassen. Jeder der Klassen enthält Methoden bzw. Funktionen. Die grau markierten Klassen sind im WordPress vorhandene Klassen, die die jeweilige Aktion ausführen. [Database, 2018] In der ITBSC Klasse sind Konstanten definiert. Der AuditLogService und der SearchLogService wird verwendet, um die Logins und Sucheingaben analysieren zu können. Der AuditLogService benutzt dazu den AuditLogRepository und der SearchLogService den SearchLogRepository. Diese zwei Repository Klassen erben von AbstractRepository. Die AbstractLog Klasse vererbt ihre Methoden an AuditLog und an SearchLog. Diese werden von Repository Klassen benutzt, um die Daten in die Datenbank zu speichern.

Die nächste Abbildung 17 zeigt das Komponentendiagramm. In dem Diagramm werden die Komponenten des Systems und die Schnittstellen dazu dargestellt. Über den Web Browser wird mit der Schnittstelle http/https eine Verbindung mit der Web Application aufgebaut.

Die Web Application benötigt die Schnittstelle zu den Audit Logs und Search Logs, um die Bewertung durchführen zu können. Die Datenbank-Komponenten Audit Logs und Search Logs stellen die Schnittstellen zu den beiden Komponenten dar. Mit der Datenabfrage werden die erforderlichen Daten für die Bewertung geholt. Anschließend kann die Bewertung ausgeführt werden, indem der Grenzwert bzw. Parameter verwendet wird.

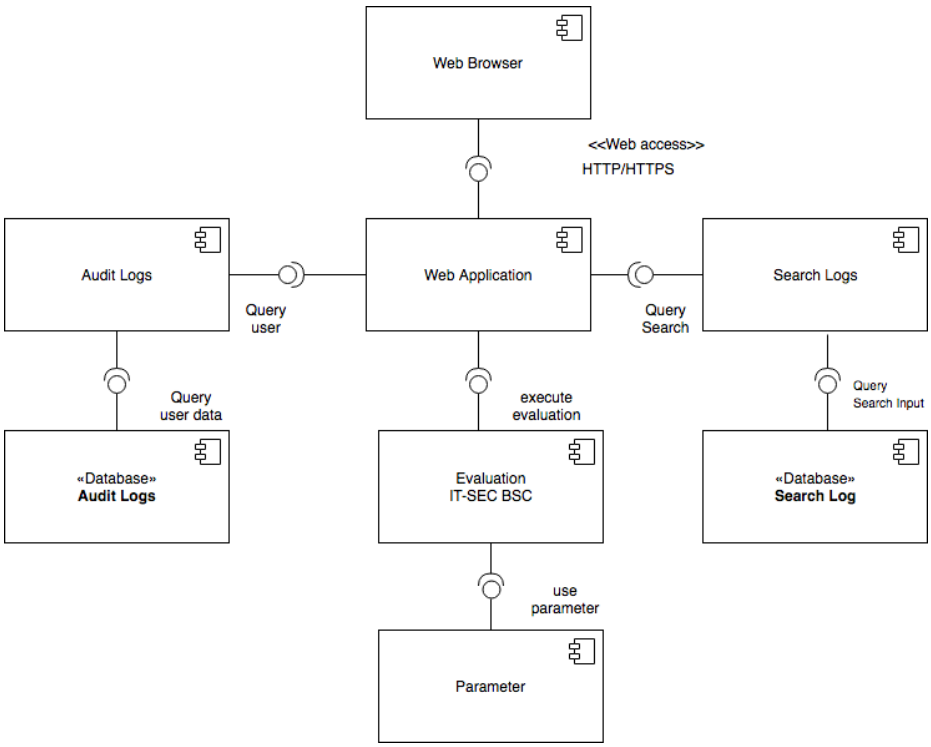

Abb. 17: Komponentendiagramm des Systems (eigene Darstellung)

In der nächsten Abbildung werden die Prozess-Schritte im Prototyp dargestellt.

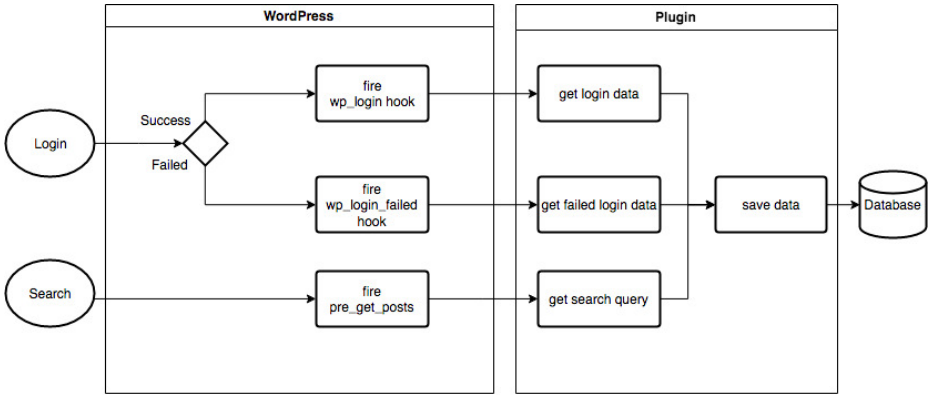

Abb. 18: Prozessmodell (eigene Darstellung)

Der Benutzer loggt sich mit seinen Benutzerdaten ein. Die Funktion wp_signon authentifiziert und protokolliert einen Benutzer mit der Remember-Fähigkeit. [wpsignon, 2018] Je nachdem ob die Anmeldung erfolgreich war oder nicht, wird der jeweilige Hook ausgelöst. Wenn der Login erfolgreich war, wird die Aktion wp_login ausgelöst ansonsten die Aktion wp_login_failed. Die Funktion handle_wp_login berücksichtigt beziehungsweise behandelt die erfolgreichen Logins. Mit der Funktion handle_wp_login_failed werden die fehlgeschlagenen Anmeldungen bearbeitet. Alle Logins, sowohl erfolgreiche als auch fehlgeschlagene werden mit der Funktion add_audit_log in die Datenbank gespeichert. Der gleiche Prozess läuft auch beim Search ab. Hier werdem mit der Funktion pre_get_posts die Sucheingaben gefiltert. Anschließend werden diese search queries in der Datenbank gespeichert.

In der nächsten Abbildung wird der Use Case dargestellt. Hier wird das Verhalten aus Sicht des Admin beschrieben. Der Actor ‚Admin‘ kann im System das Plugin installieren, aktivieren, deaktivieren und löschen.

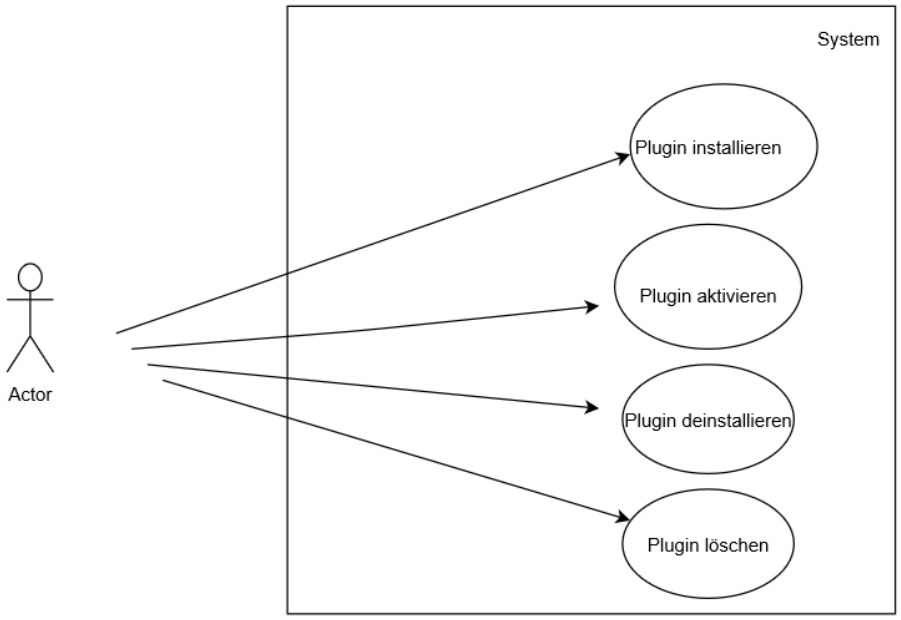

Abb. 19: Use Case ’Admin’ (eigene Darstellung)

Sowohl der User als auch der Admin können sich im System anmelden, abmelden und suchen. Der User kann aber nicht auf das Plugin zugreifen bzw. Aktionen wie Plugin installieren oder deinstallieren durchführen. Die Abbildung zeigt den Use Case dazu.

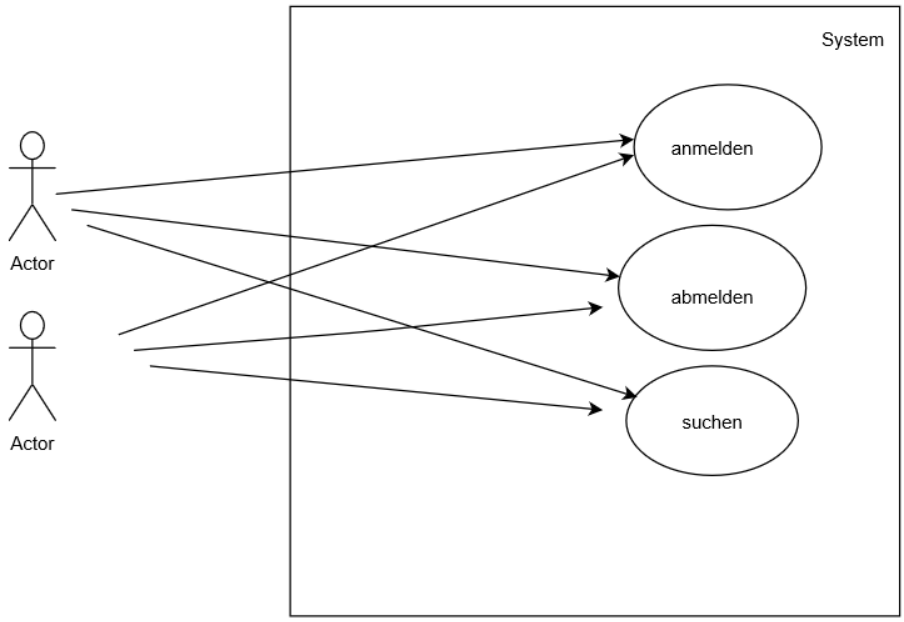

Abb. 20: Use Case 'User' und 'Admin' (eigene Darstellung)

6 Prototyp Implementierung

In diesem Kapitel erfolgt eine detaillierte Beschreibung der IT-BSC Plugin Implementierung. Zunächst wird das entwickelte Plugin dargestellt. Danach erfolgt die genaue Erklärung der Implementierung.

Der entwickelte Prototyp ist webbasiert und als Open-Source-Content-Management-System wurde WordPress verwendet. Der Grund dafür ist, dass WordPress gute Funktionalität bietet. WordPress wurde ursprünglich als Blogging Plattform konzipiert. Jedoch hat sich WordPress als nützliches CMS verändert. Einer der größten Vorteile von WordPress ist die große Anzahl von Plugins, die von unabhängigen Entwicklern veröffentlicht werden. Plugins können als Add-ons betrachtet werden, die die Funktionalität der Benutzeroberfläche verbessern. [Patel et al., 2011]

Mit Hilfe von entwickelten Plugins soll WordPress Informationen über die Sicherheitslage des Systems für die Organisation zur Verfügung stellen. Das Plugin kann mit der WordPress Site integriert werden, indem Zugriffspunkte und Methoden verwendet werden, die von der WordPress Plugin Application Program Interface (API) bereitgestellt werden. Um die Sicherheitslage des Systems zu prüfen, wird die Hook-Struktur in der WordPress-Plugin-Architektur verwendet. Hooks sind eine Möglichkeit für einen Code, um mit einem anderen Code zu interagieren bzw. ihn zu modifizieren. Sie bilden die Grundlage für die Interaktion von Plugins und Designs mit WordPress. Es gibt zwei Arten von Hooks, nämlich Aktionen und Filter. Um beides zu verwenden, muss eine benutzerdefinierte Funktion geschrieben werden, die als Callback bezeichnet wird, und wird dann für bestimmte Aktionen oder Filter bei WordPress Hook registriert. [WordPress, b]

WordPress kann auf dem lokalen Server ausgeführt und bearbeitet werden. Als lokaler Server wird WAMP verwendet. WampServer ist eine Windows-Webentwicklungsumgebung. Er ermöglicht Web-Anwendungen mit Apache2, PHP und mit einer MySQL-Datenbank zu erstellen. [Wampserver, 2018] Als Datenbanksystem unterstützt WordPress MySQL oder MariaDB. Im Rahmen der Plugin-Entwicklung wird das MySQL Datenbanksystem verwendet. Alle benötigten Tabellen werden in der Datenbank erstellt. In der WordPress Datenbank gibt es mehrere Tabellen. Außerdem sind auch die Tabellen, die von Plugins angelegt

werden, in dieser Datenbank vorhanden. WordPress verwendet das Präfix wp_ als Standard. [Database, 2018] Nachdem WordPress installiert wurde, können entwickelte Plugins hochgeladen werden. Darüber hinaus können auch vorhandene Plugins verwendet werden. [WordPress, b]

Das entwickelte Plugin wird zur Installation dem Unternehmen zur Verfügung gestellt. Der IT-Mitarbeiter von Plusmobile kann das Plugin nun uploaden und die Analyse durchführen. Dazu muss er als erstes das Plugin im Dashboard unter ‚Plugin installieren' hochladen, indem er auf ‚Plugin hochladen' geht und das zur Verfügung gestellte Plugin unter ‚Durchsuchen' wählt. Die Datei ‚itbsc.zip' muss jetzt hochgeladen werden. Nachdem das Zip-File ausgewählt und hochgeladen wurde, muss das Plugin noch aktiviert werden. Die Aktivierung erfolgt unter ‚Installierte Plugins", wo alle installierten beziehungsweise hochgeladenen Plugins aufgelistet sind. Mit der Aktivierung werden die Methoden im PHP-Skript (itbsc.php) aufgerufen. [Installation, 2018] Nun muss im Dashboard ein Menüfeld mit dem Namen ‚IT-Balanced Scorecard' verfügbar sein. Außerdem muss noch ein Submenü ‚Audit Logs', ‚Search Logs' und ‚Settings' vorhanden sein.

Diese ganzen Funktionen werden über PHP-Skripts ausgeführt. Im folgenden Absatz werden die Funktionen erklärt.

In der Abbildung 21 sind die definierten Konstanten und die Funktionen zu sehen.

```php
require_once( plugin_dir_path( file: __FILE__ ) . 'model/AbstractLog.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'model/AuditLog.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'model/SearchLog.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'repository/AbstractRepository.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'repository/AuditLogRepository.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'repository/SearchLogRepository.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'service/AuditLogService.php' );
require_once( plugin_dir_path( file: __FILE__ ) . 'service/SearchLogService.php' );

class ITBSC {

    const DEFAULT_LIMIT_PER_PAGE = 10;
    const DEFAULT_LOWER_LIMIT_RATIO = 80;
    const SETTINGS_GROUP = 'itbsc-settings-group';

    const ACTIVATE_PLUGIN_ACTION = 'activate_plugin';
    const ADMIN_INIT_ACTION = 'admin_init';
    const ADMIN_MENU_ACTION = 'admin_menu';
    const LOAD_PAGE_ACTION = 'load-';
    const LOGIN_ACTION = 'wp_login';
    const LOGIN_FAILED_ACTION = 'wp_login_failed';
    const PRE_GET_POSTS_FILTER = 'pre_get_posts';

    private $audit_log_service;
    private $search_log_service;

    private function __construct() {
        $this->audit_log_service  = new AuditLogService();
        $this->search_log_service = new SearchLogService();
        add_action( self::ACTIVATE_PLUGIN_ACTION, array( $this, 'activate' ) );
        add_action( self::ADMIN_MENU_ACTION, array( $this, 'add_pages' ) );
        add_action( self::LOGIN_FAILED_ACTION, array( $this, 'handle_wp_login_failed' ) );
        add_action( self::LOGIN_ACTION, array( $this, 'handle_wp_login' ), 10, 2 );
        add_filter( self::PRE_GET_POSTS_FILTER, array(
            $this,
            'filter_search_query'
```

Abb. 21: Code Auszug Konstanten und Funktionen

Um das Plugin verwenden zu können beziehungsweise die Analyse durchführen zu können, muss zuerst das Plugin aktiviert werden. Mit der Aktion ‚activate plugin' wird das Plugin aktiviert. Nachdem das Plugin aktiviert ist, wird zuerst eine Tabelle in der Datenbank erstellt. In diesem Fall wird MySQL als Datenbanksystem verwendet und jede neu erstellte Tabelle wird in der WordPress Datenbank gespeichert. Es werden zwei Tabellen erstellt, nämlich die Tabelle ‚itbsc_audit_logs' für die Login-Daten und die Tabelle ‚itbsc_search_logs'

für die Sucheingabe-Daten. Es wird eine neue Tabelle erstellt, wenn noch keine Tabelle erstellt wurde. Das heißt in diesem Fall, wenn die Tabelle itbsc_audit_logs noch nicht vorhanden ist, wird diese erstellt. Außerdem wird mit der ‚update_option' die Plugin Version in der Datenbank abgespeichert.

In der nächsten Abbildung ist der Code-Auszug dazu abgebildet.

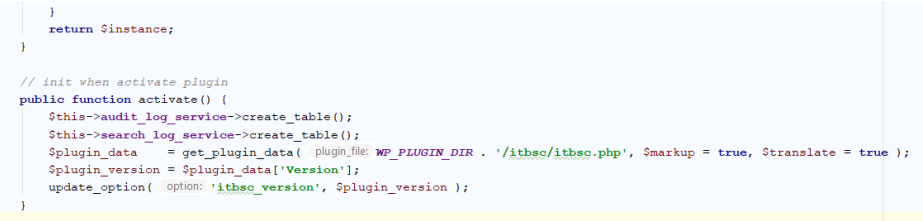

Abb. 22: Code Auszug activate plugin

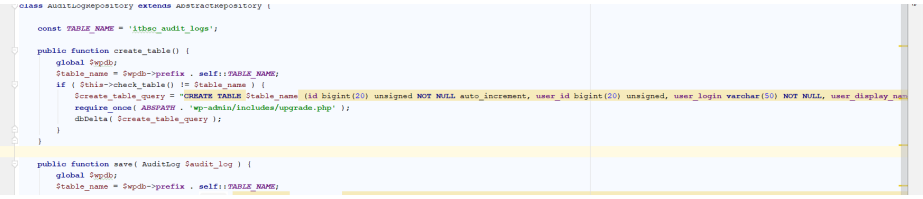

Abb. 23: Code Auszug create table

Mit der Funktion ‚add_pages ‘ werden Top-Level-Menü und Submenü in die Admin-Panel-Menüstruktur hinzugefügt. Der ‚function_name‘ ist der Name der aufzurufenden Funktion. Mit der Funktion ‚add_menu_page‘ und ‚add_submenu_page‘ werden neue Top-Menü beziehungsweise Submenü erstellt. Als Top Menüs wird ‚IT-Balanced Scorecard‘ und als Sub-Menüs wird ‚Audit Logs‘, ‚Search Logs‘ und ‚Settings‘ erstellt.

In der folgenden Abbildung ist der zugehörige Code zu sehen.

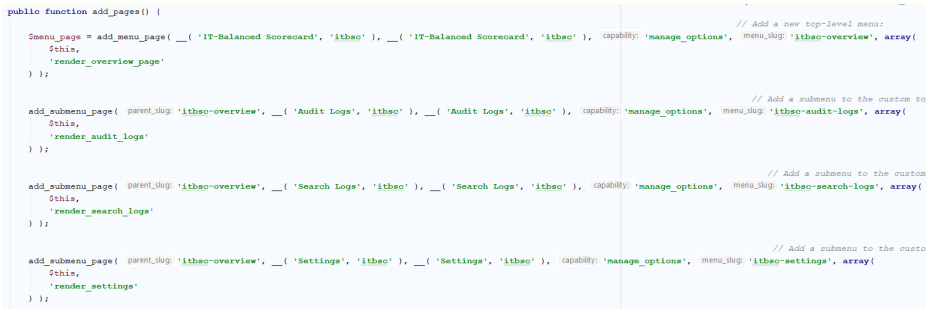

Abb. 24: Code Auszug add menu

Als nächstes werden die Login Funktionen näher erläutert. Die Abbildung 25 ist der Code-Auszug von , handle_wp_login_failed‘ und von ‚handle_wp_login‘.

```
97      }
98
99      public function handle_wp_login_failed( $user_login ) {
100         $audit_log              = new AuditLog();
101         $audit_log->action      = self::LOGIN_FAILED_ACTION;
102         $audit_log->ip          = $_SERVER['REMOTE_ADDR'];
103         $audit_log->created_at  = current_time( type: 'mysql' );
104         $audit_log->user_login  = $user_login;
105         $user_detail            = get_user_by( field: 'login', $user_login );
106         if ( isset( $user_detail ) ) {
107             $audit_log->user_id           = $user_detail->ID;
108             $audit_log->user_display_name = $user_detail->display_name;
109             $audit_log->user_email        = $user_detail->user_email;
110             if ( ! empty( $user_detail->roles ) && is_array( $user_detail->roles ) ) {
111                 $audit_log->user_role = reset( &array: $user_detail->roles );
112             }
113         }
114         $this->audit_log_service->save( $audit_log );
115     }
116
117     public function handle_wp_login( $user_login, $user ) {
118         $audit_log                  = new AuditLog();
119         $audit_log->action          = self::LOGIN_ACTION;
120         $audit_log->ip              = $_SERVER['REMOTE_ADDR'];
121         $audit_log->created_at      = current_time( type: 'mysql' );
122         $audit_log->user_login      = $user_login;
123         $audit_log->user_email      = $user->user_email;
124         $audit_log->user_id         = $user->ID;
125         $user                       = new WP_User( $user->ID );
126         $audit_log->user_display_name = $user->display_name;
127         if ( ! empty( $user->roles ) && is_array( $user->roles ) ) {
128             $audit_log->user_role = reset( &array: $user->roles );
129         }
130         $this->audit_log_service->save( $audit_log );
131     }
132
133
```

Abb. 25: Code Auszug handle_wp_login_failed‘ und von ‚handle_wp_login‘

Die Funktion ‚handle_wp_login_failed‘ dokumentiert alle fehlgeschlagenen Anmeldungen im System. Wenn ein User sich im System anzumelden versucht, werden die Informationen in der Datenbank von WordPress gespeichert. Diese Informationen, die in wp_ itbsc_audit_logs gespeichert werden, sind:

Datum: Der Zeitpunkt, an dem der User sich angemeldet hat. Angezeigt wird das Datum und die Uhrzeit.

User: Der Benutzername, mit dem der User versucht hat sich anzumelden, wird gespeichert.

Displayname: Der öffentliche Name ist in der Datenbank beziehungsweise in der Tabelle gespeichert. Wenn der Benutzer im System gespeichert ist, wird auch sein öffentlicher Name bei der Auswertung für das Unternehmen angezeigt. Dazu wird im nächsten Abschnitt näher eingegangen.

Role: Unter Role werden die Rollen, die für den Benutzer bestimmt werden, gespeichert. Zum Beispiel hat der Admin die Rolle als Administrator.

E-Mail: Die E-Mail Adressen der Benutzer werden in der Spalte Email gespeichert.

IP-Adresse: Die IP-Adressen werden von den Benutzern, die versucht haben sich anzumelden auch gespeichert.

Action: Unter Action wird die Information gespeichert, ob die Anmeldung erfolgreich war oder nicht. In diesem Fall wird ‚Login failed' für fehlgeschlagene Anmeldungen und ‚Logged in' für gelungene Anmeldungen gespeichert.

In der Funktion ‚handle_wp_login_failed' werden die fehlgeschlagenen Logins behandelt. Wenn ein Benutzer versucht sich im System anzumelden, wird mit dieser Funktion überprüft, ob der User vorhanden ist. Wenn der User nicht vorhanden ist, werden die Informationen wie Datum, Username, IP-Adresse sowie die Aktion, dass die Anmeldung fehlgeschlagen ist, gespeichert. Diese Informationen werden dann für die Analyse verwendet.

Die Funktion ‚handle_wp_login' dokumentiert alle erfolgreichen Logins. Wenn der User sich im System anmeldet und der User im System vorhanden ist, werden die Informationen zu dem User in die Datenbank in der Tabelle wp_itbsc_audit_logs für die Analyse gespeichert. Diese Informationen sind Datum, Username, Displayname, Role, Email, IP-Adresse und die Aktion, dass die Anmeldung erfolgreich war.

Mit dem Filter pre_get_post werden die Sucheingaben gefiltert. Es

wird analysiert ob die Sucheingaben ein Risiko für das Unternehmen darstellen oder nicht. Als sichere Sucheingaben werden Buchstaben, Zahlen, Leerzeichen und Punkt definiert, da meistens die Sucheingaben aus diesen vier Merkmalen bestehen. Alle anderen Sucheingaben werden näher analysiert, da sie eine Gefahr für Unternehmen bedeuten könnten. Zum Beispiel kann es sich um einen SQL-Injection Angriff handeln, in dem der Angreifer sich den Zugriff auf die Datenbank schafft. [Halfond et al., 2006]
In diesem Fall wird nicht der Angriff verhindert, sondern die Sucheingaben analysiert, ob es sich um auffällige Sucheingaben handelt.

Der Code-Auszug vom Search-Filter wird in Abbildung 26 dargestellt.

```
77
78      public function filter_search_query( $query ) {
79          if ( $query->is_main_query() && $query->is_search() ) {
80              $search_log              = new SearchLog();
81              $search_log->search_text = $query->get( "s" );
82              $search_log->ip          = $_SERVER['REMOTE_ADDR'];
83              $search_log->created_at  = current_time( type: 'mysql' );
84              $current_user            = wp_get_current_user();
85              if ( isset( $current_user ) ) {
86                  $search_log->user_login        = $current_user->user_login;
87                  $search_log->user_id           = $current_user->ID;
88                  $search_log->user_display_name = $current_user->display_name;
89                  $search_log->user_email        = $current_user->user_email;
90                  if ( ! empty( $current_user->roles ) && is_array( $current_user->roles ) ) {
91                      $search_log->user_role = reset( &array: $current_user->roles );
92                  }
93              }
94              $this->search_log_service->save( $search_log );
95          }
96          return $query;
97      }
98
```

Abb. 26: Code Auszug Search-Filter

7 ITBSC-Plugin Test

In diesem Kapitel wird das Plugin getestet und beschrieben. Das Plugin wurde nach Funktionsfähigkeit mehrmals getestet.

Die gespeicherten Informationen werden in WordPress unter dem Submenü Audit Logs und unter Search Logs als Tabelle angezeigt. Anhand dieser Informationen wird die Analyse automatisch durchgeführt und bewertet. Für die Bewertung wird ein Parameter festgelegt. Dies erfolgt unter Settings. Es sind zwei Settings festzulegen, nämlich für ‚erfolgreiche Logins' und für ‚safe search'.

In der Abbildung 27 sind Audit Logs zu sehen.

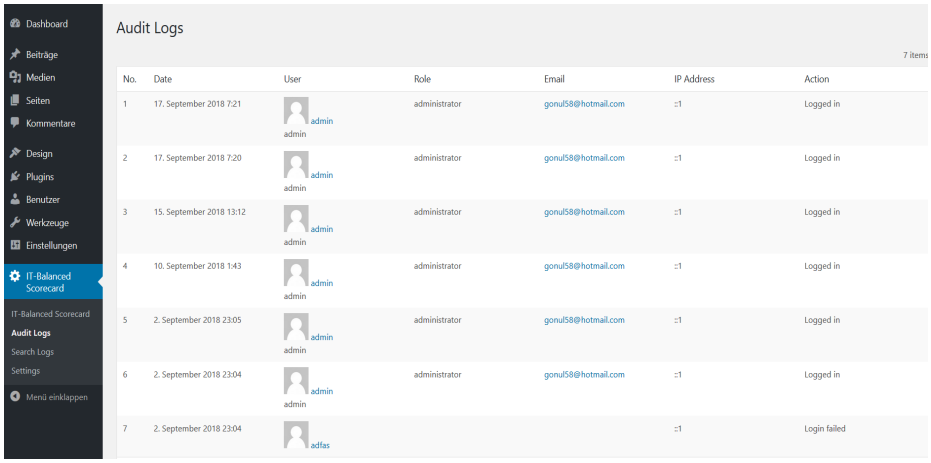

Abb. 27: Audit Logs

In der Abbildung 28 sind Search Logs zu sehen.

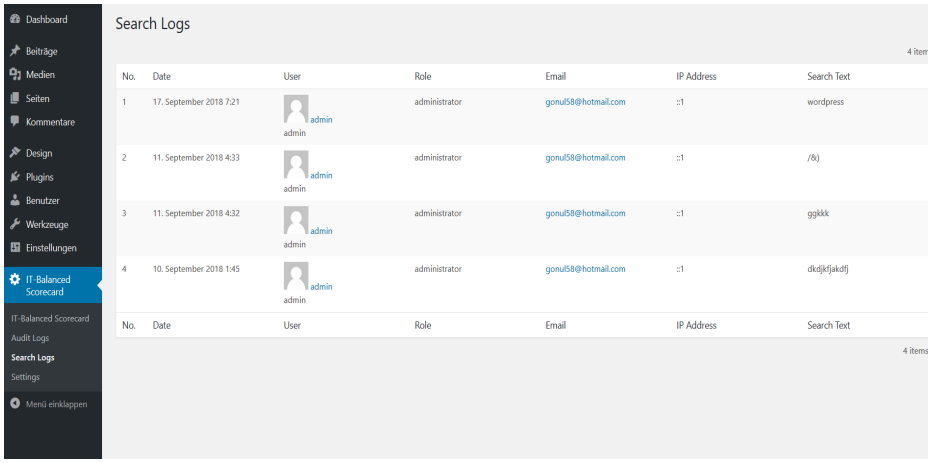

Abb. 28: Search Logs

Die Messergebnisse werden mit Hilfe von IT-Balanced Scorecard in Prozentanteil dargestellt. Somit ist es möglich einen Überblick über den Sicherheitsstatus des Systems zu haben. Des Weiteren werden die Ergebnisse auch anhand von Diagrammen für das Unternehmen übersichtlich gemacht.

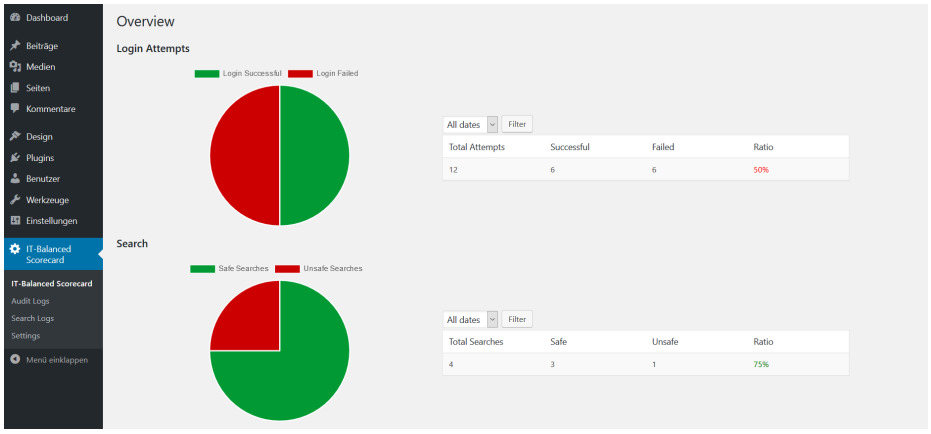

Abb. 29: IT-Balanced Scorecard

Unter IT-Balanced Scorecard werden die Login-Ergebnisse und die Such-Ergebnisse in Scorecard angezeigt. Es wird ein Überblick über Login-Versuche mit den Ergebnissen Total Zugriffe, erfolgreiche Zugriffe, fehlgeschlagene Zugriffe und Ratio gegeben. Des Weiteren können die Ergebnisse nach Jahr, Monat, Woche, Gestern und Heute gefiltert werden. Dazu gibt es eine Filterfunktion, die je nach der Filterwahl die Anzahl der Zugriffe, die Anzahl der erfolgreichen Zugriffe, die fehlgeschlagenen Zugriffe sowie das Messergebnis für den ausgewählten Zeitraum anzeigt. Wenn zum Beispiel die Zugriffe für eine ganze Woche bewertet werden sollen, wird ab dem aktuellen Zeitpunkt 1 Woche in der Vergangenheit analysiert. Berechnet wird der Prozentanteil aller erfolgreichen Zugriffe.

Wenn Zugriffe größer 0 sind, das heißt, wenn Zugriffe auf das System stattfinden, werden diese für die Berechnung berücksichtigt.

In der nächsten Abbildung wird die Oberfläche für Parameter Settings angezeigt.

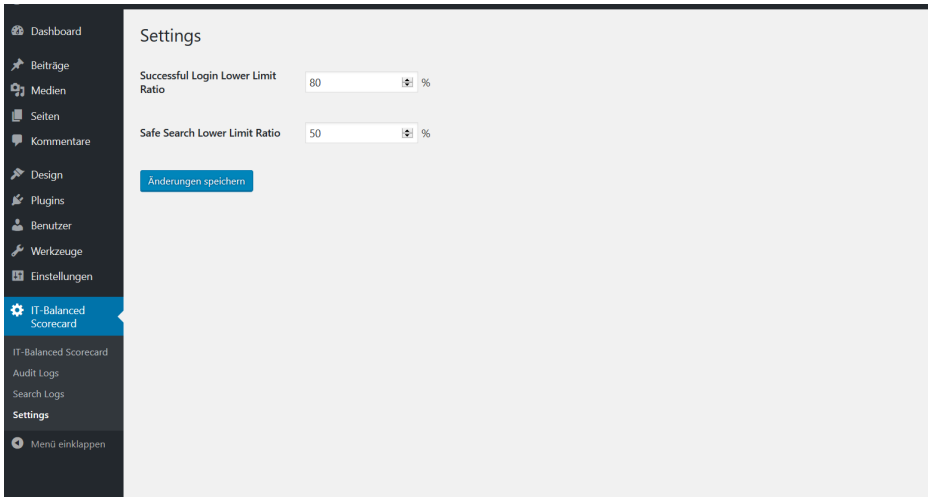

Abb. 30: Parameter Settings

Als Grenzwert wird 80% definiert. Dieser Parameter kann manuell vom Unternehmen geändert werden. Wenn die Ratio größer als 80% ist, wird das Ergebnis in grün angezeigt, wenn es unter 80% ist wird das Ergebnis rot angezeigt. Für Search wird als Grenzwert 50% gewählt. Wenn die sicheren Sucheingaben größer als 50% sind, wird das Ergebnis grün angezeigt, ansonsten wird es rot angezeigt.

Die Filterfunktion wurde auch getestet. Die Analyse kann nach Jahr, Monat, Woche, Gestern und nach Heute gefiltert werden.

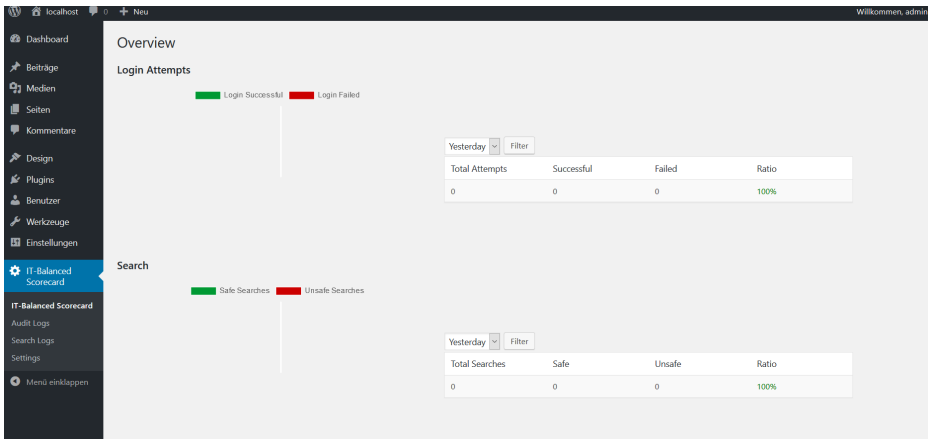

Abb. 31: Filter Yesterday

In der Abbildung 31 wurde als Filter "Yesterday"gewählt. Die Bewertung wird nur für den Zeitraum Gestern durchgeführt. In diesem Fall gab es keine Login-Versuche und Sucheingaben, daher wird 0 angezeigt. Die Ratio bleibt 100%, weil keine Zugriffe stattgefunden haben.

Die Abbildung 32 zeigt alle Logins für den Filter "Today".

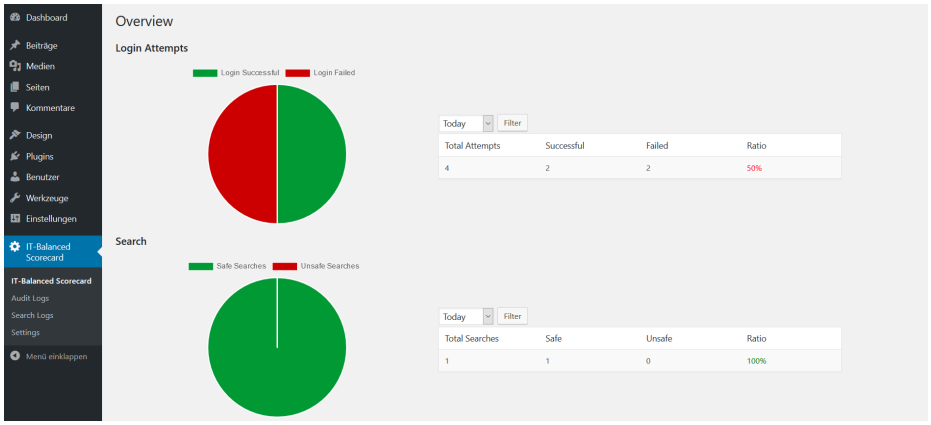

Abb. 32: Filter Today

Es werden nur jene Zugriffe und Sucheingaben berücksichtigt, die ‚Heute' stattgefunden haben.

In den folgenden Abbildungen (Fig. 33, Fig. 34, Fig. 35) werden die Filter Woche, Monat und Jahr dargestellt.

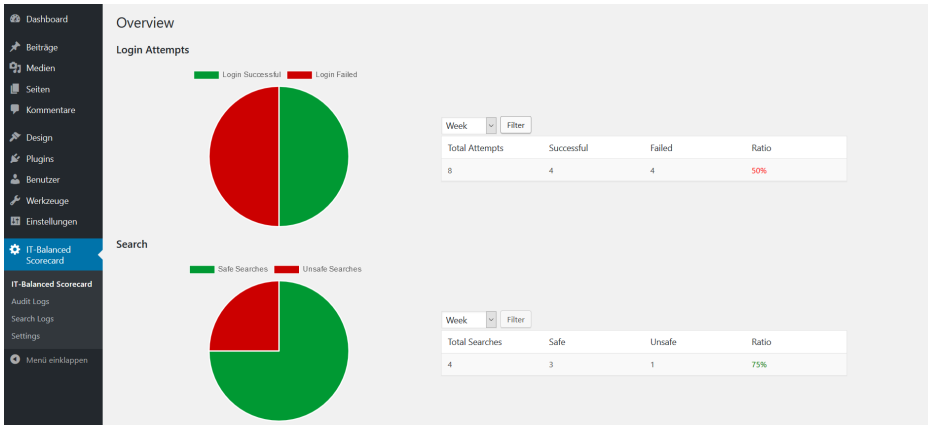

Abb. 33: Filter Week

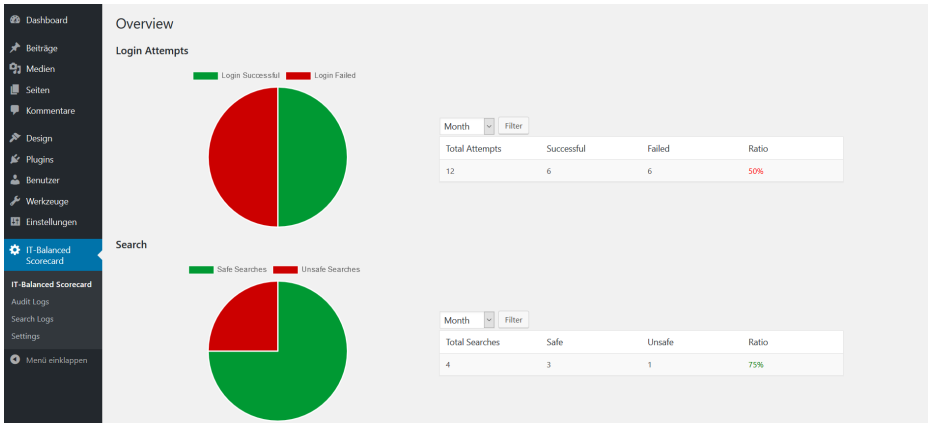

Abb. 34: Filter Monat

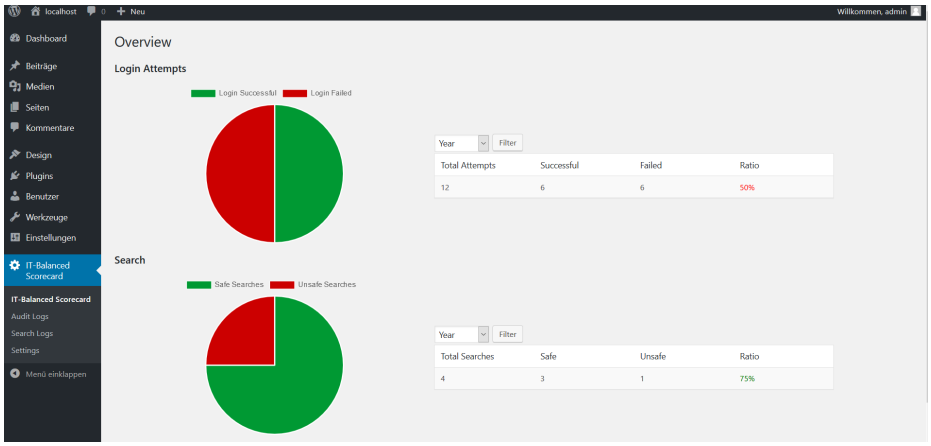

Abb. 35: Filter Year

Der Test zeigt, dass alle Filter-Auswahl-Funktionen erfolgreich sind. Je nachdem welcher Filter ausgewählt wird, werden nur die Daten in diesem Zeitraum berücksichtigt bzw. bewertet. Das Testen des Grenzwerts bzw. des Parameters war auch erfolgreich. Der definierte Parameter wird bei der Bewertung berücksichtigt. Sowohl erfolgreiche als auch fehlgeschlagene Zugriffsversuche werden erfasst und in der Datenbank gespeichert. Die Sucheingaben werden auch erfasst und in der Datenbank gespeichert. Die Bewertung der Sucheingaben wurde auch erfolgreich getestet. Somit ist der Test erfolgreich abgeschlossen. Das Plugin kann nun getestet werden, ob es praxistauglich ist. Dieser Test wird im nächsten Kapitel beschrieben.

8 Test von Plus Mobile

Nach Fertigstellung des Plugins wurde es zum Testen an Plus Mobile zur Verfügung gestellt. Mit dem Prototyp werden die Zugriffskontrollen und die Sucheingaben analysiert. Das Ziel ist es einen Überblick über die Audit Logs und über Search Logs zu haben, die in einem bestimmten Zeitraum stattgefunden haben. Anhand der Bewertungsergebnisse kann das Unternehmen dementsprechend Entscheidungen treffen, ob Maßnahmen erforderlich sind oder nicht.

Der Prototyp wurde wie im Abschnitt ‚Prototyp Implementierung' beschrieben von Plus Mobile installiert und anschließend mit der Analyse begonnen.
Der erste Login erfolgte am Mittwoch, 29. August 2018. Ab dem Zeitpunkt wurden alle erfolgreichen und nicht erfolgreichen Zugriffe erfasst und bewertet.

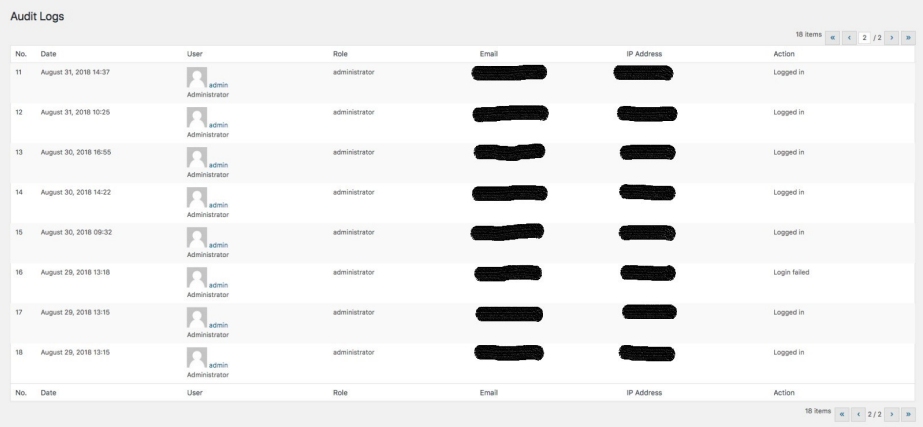

Abb. 36: Audit Logs Daten

In der Abbildung 36 sind die Login-Daten zu sehen. Es wird angezeigt, welcher User sich zur welchen Zeit sich im System angemeldet hat beziehungsweise sich nicht anmelden konnte. Die E-Mail Adressen und IP-Adressen werden auf Grund der Datenschutzbestimmungen nicht angezeigt. [DSG, 2018] In der letzten Spalte ist ersichtlich, ob die Anmeldung möglich war oder nicht. Es werden pro Seite 10 Zeilen angezeigt, damit es übersichtlich ist. Anhand dieser Informationen wird

die Bewertung automatisch durchgeführt.

In der nächsten Abbildung kann herausgelesen werden wann der letzte Login war.

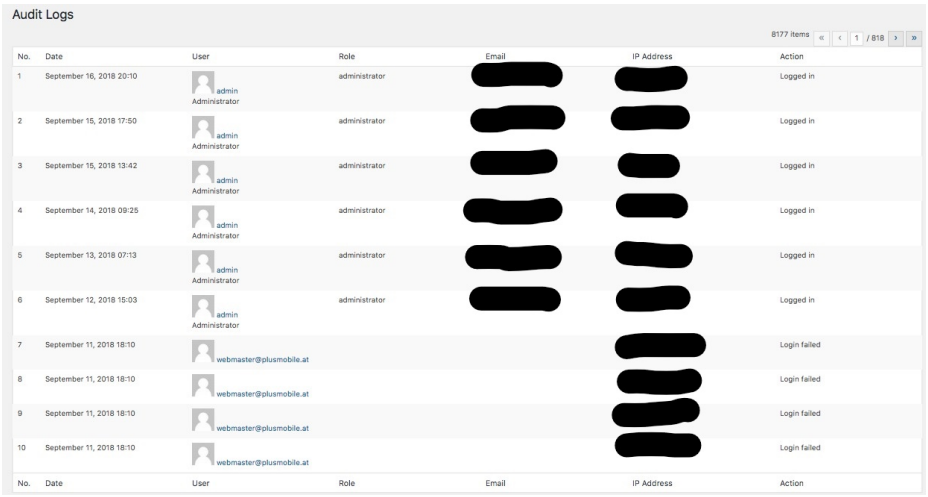

Abb. 37: Audit Logs Daten - letzter Login

Der letzte Login war am 16. September 2018. Es können nicht alle Login Daten angezeigt werden. Es stellte sich nämlich heraus, dass insgesamt 8177 Login Versuche stattgefunden haben. In der nächsten Abbildung werden alle Login Versuche und alle Sucheingaben angezeigt.

Die nächste Abbildung gibt einen Überblick über die Logins.

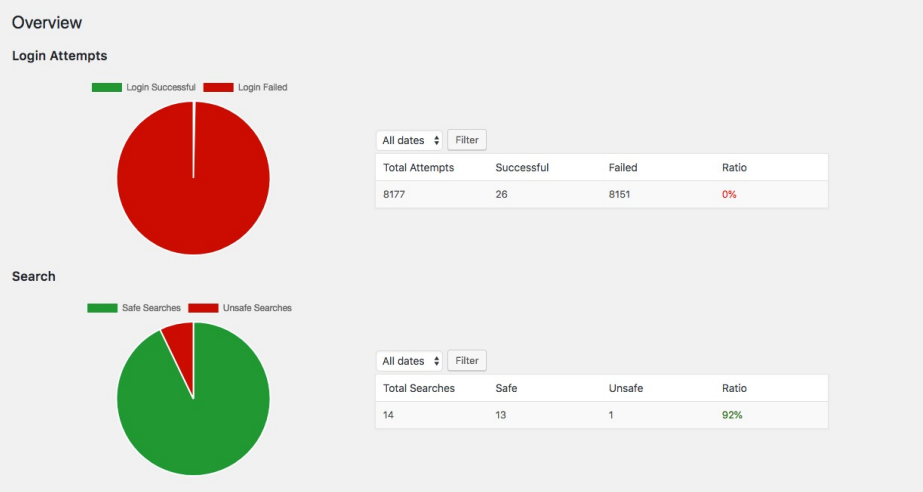

Abb. 38: Überblick

Es wurden 8177 Login-Versuche durchgeführt, davon waren nur 26 erfolgreich. 8151 Login-Versuche sind fehlgeschlagen. Daher ist das Ergebnis 0% und somit im roten Bereich. Das heißt, dass das Bewertungsergebnis unter dem definierten Grenzwert, nämlich unter 80% ist. In diesem Fall ist die Sicherheit der Zugriffskontrollen im roten Bereich. Es sind Maßnahmen erforderlich um schwere Folgen eines Angriffes zu vermeiden.

Wenn die nächste Abbildung 39 näher betrachtet wird, ist erkennbar, dass in der letzten Woche 8156 Zugriffsversuche stattgefunden haben, davon aber nur 9 erfolgreiche Zugriffe waren.

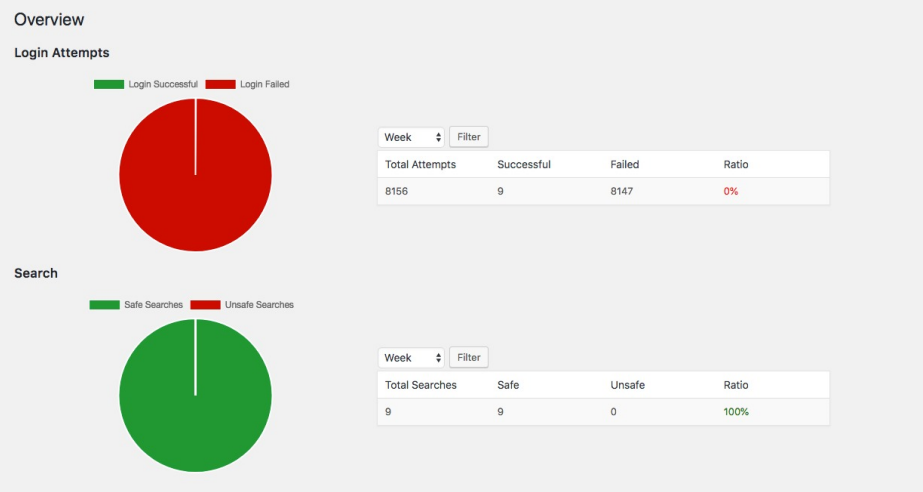

Abb. 39: Überblick Login und Search

Wenn man die Informationen aus der Abbildung 37 dazu betrachtet, kann man davon ausgehen, dass am 11.09.2018 ein Brute-Force Angriff stattgefunden hat. In diesem Fall sollte das Unternehmen Maßnahmen treffen, wie zum Beispiel sichere komplexe Passwörter verwenden. [Vaithyasubramanian et al., 2014]

Die nächste Abbildung 40 zeigt die Search Logs.

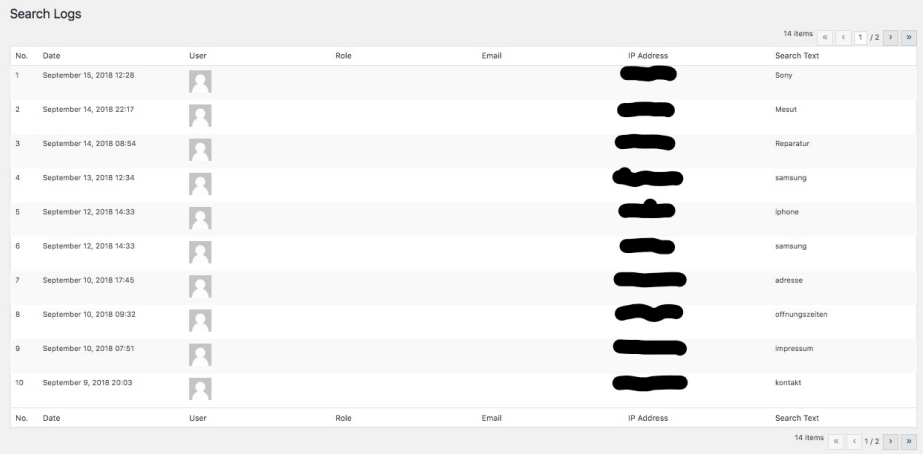

Abb. 40: Search Logs

In den Search Logs werden die Sucheingaben gespeichert. Anhand dieser Informationen kann analysiert werden, ob die Sucheingaben eine Gefahr für das Unternehmen darstellen oder nicht.

9 Diskussion der Ergebnisse

Der entwickelte Prototyp wurde erfolgreich vom Unternehmen Plus Mobile getestet. Die Testergebnisse wurden auch zur Verfügung gestellt und im vorherigen Kapitel erläutert.

Grundsätzlich kann das entwickelte Plugin von kleinen Unternehmen angewendet werden, die WordPress nutzen. Der Grund dafür ist, dass das Plugin WordPress Funktionen verwendet, die erweitert werden können. [WordPress, b] Die Installation des Plugins ist prinzipiell nicht aufwändig, jedoch muss das Plugin nach der Installation aktiviert werden. Erst nach der Aktivierung ist es einsatzbereit. Die Verwendung des Plugins wurde als benutzerfreundlich definiert, da das Unternehmen bzw. der beauftragte Mitarbeiter nicht viel unternehmen muss. Die Analyse wird, wie im vorherigen Kapitel beschrieben, automatisch durchgeführt. Das Unternehmen muss nur den Parameter definieren, um die Bewertung durchführen zu können.

Die Ergebnisse der Analyse können dem Unternehmen einen Überblick darüber geben, inwieweit ihr System durch Angriffe gefährdet ist. Mit Hilfe dieses Bewertungstools kann die Organisation die Sicherheitslage des Systems messen und bewerten. Das Ziel ist es nicht das Unternehmen mit anderen Unternehmen zu vergleichen, um den Sicherheitsstatus zu ermitteln. In diesem Fall wird der Sicherheitsstatus des Systems mit quantifizierbaren Kennzahlen gemessen und bewertet. Anhand der Ergebnisse kann die Organisation Entscheidungen bezüglich der Maßnahmen treffen. Außerdem kann das Unternehmen die Ergebnisse laufend vergleichen und dementsprechend auch weitere Maßnahmen treffen. Es kann zum Beispiel verglichen werden, ob die erfolgreichen Logins im Gegensatz zum nächsten Monat gesunken sind oder nicht. Daher sind die Ergebnisse der Tests nicht ganz aussagekräftig, um sofort Entscheidungen treffen zu können. Die Analyse sollte über einen längeren Zeitraum durchgeführt werden, um den Sicherheitsstatus des Systems bewerten zu können. In diesem Fall ist es von Vorteil, wenn das Bewertungstool Filter-Funktionen hat, die es ermöglichen die Bewertungsergebnisse für einen bestimmten Zeitraum anzuzeigen. Der im Rahmen dieser Arbeit entwickelte Prototyp ermöglicht die Ergebnisse der Bewertung nach Jahr, Monat, Woche, Gestern und Heute anzuzeigen.

Es stellte sich heraus, dass das entwickelte Plugin nicht ausreichend ist,

um eine gesamte IT-Sicherheitsbewertung des Systems durchzuführen. Um bessere Ergebnisse erzielen zu können, kann das Plugin mit zusätzlichen Funktionen erweitert werden. Darüber hinaus müssen weitere Sicherheitskennzahlen definiert werden.

Die Ergebnisse der Bewertung von Plusmobile zeigten, dass ein Brute Force Angriff auf das System stattgefunden hat. Brute Force Angriffe sind eine ernsthafte Bedrohung für das Unternehmen. Der Angreifer versucht auf das System zuzugreifen, in dem er versucht das Passwort zu knacken. [Vaithyasubramanian et al., 2014]

Der Angriff konnte mittels Analyse der Audit Logs identifiziert werden. Aus der Bewertung kann herausgelesen werden, dass innerhalb einer Woche 8156 Zugriffsversuche auf das System stattgefunden haben. Dies ist definitiv eine hohe Zahl und sollte näher betrachtetet werden. In diesem Fall sollte das Unternehmen Maßnahmen treffen, um solchen Angriffen vorbeugen zu können. Dafür sollten zum Beispiel sichere Passwörter verwendet werden. Ein sicheres Passwort besteht beispielsweise aus 10 Zeichen, die Klein- und Großbuchstaben, Sonderzeichen und Zahlen enthalten. [Vaithyasubramanian et al., 2014]

Die Analyse bzw. die Bewertung der Zugriffsversuche im System ist somit ein wichtiger Punkt im Unternehmen. Im Rahmen der Testdurchführung wurden auch die Sucheingaben im System analysiert. Hier waren die Ergebnisse im grünen Bereich, das heißt, dass es keine Auffälligkeiten gab, die auf einen SQL-Injection Angriff deuten könnten. In diesem Fall sind keine Maßnahmen erforderlich. Jedoch sollte das Unternehmen die Überwachung und die Bewertung der Sucheingaben weiterhin durchführen, da die SQL-Injection Angriffe auch eine große Gefahr für Unternehmen darstellen. Die Angreifer können auf die Datenbank zugreifen und die Daten manipulieren. Dies könnte für das Unternehmen ernsthafte Folgen haben. [Halfond et al., 2006]

Aus diesem Grund sind die Überwachung der Systeme und die Bewertung der IT-Sicherheit im Unternehmen von großer Bedeutung. Der IT-Sicherheitsstatus des Systems hilft dem Unternehmen bei der Entscheidung über die weiteren Sicherheitsmaßnahmen.

10 Conclusio

Die IT-Sicherheit ist ein wichtiges Thema im Unternehmen. Das Management muss daher die Sicherheit im Betrieb gewährleisten. Dies ist jedoch nicht so einfach, da Unternehmen vielen Risiken ausgesetzt sind. Ein Angriff auf das System kann ernsthafte Schäden für die Organisation bedeuten. Aus diesem Grund sollten regelmäßig Sicherheitsanalysen und IT-Sicherheitsbewertungen durchgeführt werden. [Pereira and Santos, 2014]

Die Überwachung der IT-Sicherheit und die Bewertung des IT-Sicherheitsstatus des Systems ist nicht nur eine herausfordernde, sondern auch eine kostenintensive Aufgabe. Der Grund dafür ist, dass in Unternehmen automatisierte Methoden fehlen. [Montesino and Fenz, 2011] Besonders hervorzuheben ist in dieser Hinsicht die Bedeutung von Sicherheitskennzahlen. Die im Unternehmen getätigten finanziellen Ausgaben und die getroffenen Maßnahmen können anhand von Sicherheitskennzahlen gemessen werden. Das Unternehmen kann somit überprüfen, ob die Ergebnisse den definierten Zielen entsprechen. Auf diese Weise können weitere Maßnahmen getroffen werden, um die IT-Sicherheit im Unternehmen weiterhin gewährleisten zu können. [Herath et al., 2010]

Es ist ein Bewertungstool notwendig, um den IT-Sicherheitsstatus des Unternehmens bewerten zu können. Es gibt diverse Ansätze, die sich mit der Sicherheitsbewertung des Systems befassen. Die ISO/IEC 27002 und ISO/IEC 27001 Standards sind die meist referenzierten Sicherheitsmodelle. Die Standards geben einen Überblick über die Sicherheitskontrollen und über die Sicherheitskennzahlen. Des Weiteren stellen sie Informationen zum Aufbau des Information Security Management System (ISMS) und Details über die Implementierung unter Verwendung des Plan-Do-Check-Act Zyklus zur Verfügung. [ISO/IEC27000, 2014] [ISO/IEC27004, 2016]

Im Rahmen dieser Arbeit wurde ein IT-Sicherheitsbewertungs-Modell entwickelt und die prototypische Implementierung umgesetzt. Anschließend wurde der Test durchgeführt und die Ergebnisse behandelt.

Die Bewertung des IT-Sicherheitsstatus eines Systems ist ein Prozess, der aus mehreren Aktionen besteht. Um die Bewertung durchführen

zu können, müssen Sicherheitskennzahlen entwickelt werden. Unter Berücksichtigung der existierenden Standards und Best Practices wurden Sicherheitskennzahlen für das Unternehmen Plus Mobile entwickelt. Zuerst wurde analysiert, welche Sicherheitsfaktoren des Systems gemessen und bewertet werden können. Anschließend wurden die Sicherheitsziele und die Sicherheitskontrollen definiert. Basierend auf dem ISO-Messmodell wurden anhand von Sicherheitskontrollen Attribute ermittelt. Von den Attributen wurden Base Measures entwickelt und die Derived Measures aus den Base Measures abgeleitet. Die entwickelten Kennzahlen wurden auch als Kennzahlensteckbrief dokumentiert. Im Rahmen dieser Arbeit wurden zwei Sicherheitskennzahlen ermittelt, um die Zugriffskontrolle und die Sucheingaben im System zu überwachen und zu bewerten. Demzufolge wurde dann ein Plugin entwickelt, um die IT-Sicherheit des Systems anhand von Sicherheitskennzahlen bewerten zu können. Neben den Sicherheitskennzahlen musste noch ein Indikator bzw. ein Grenzwert vom Unternehmen definiert werden.

Da die IT-Sicherheit als strategische Investition in Betracht gezogen wird, wurde eine IT-Balanced Scorecard modelliert. Die Balanced Scorecard ist ein weit verbreitetes Modell, das die langfristigen Strategieziele eines Unternehmens mit kurzfristigen Maßnahmen kombiniert. [Kaplan and P. Norton, 1991]

Anschließend wurde das IT-Sicherheitsbewertungs-Plugin getestet. Der Test zeigte, dass das Plugin gut in die Website des Unternehmens integriert werden konnte und bezüglich Überprüfung der Zugriffskontrolle und Sucheingaben seinen Zweck erfüllte.

Zusammenfassend lässt sich sagen, dass die Herausforderdung bei der Bewertung des IT-Sicherheitsstatus eines Systems die Entwicklung von Sicherheitskennzahlen ist. Für eine effiziente Bewertung des IT-Sicherheitsniveaus sind quantitative IT-Sicherheitskennzahlen die Bedingung. [Kahraman, 2005] Für die praktische Umsetzung in dem Fall ist die Literatur eine essenzielle Unterstützung.

Alles in allem ist IT-Sicherheit ein weitverbreitetes Forschungsgebiet, das sich vor allem mit der Automatisierung der IT-Sicherheitsbewertung beschäftigt. Die IT-Sicherheit im Unternehmen wird weiterhin ein wichtiges Thema sein. Um die Gesamtsicherheit eines Systems zu gewährleisten, müssen jedoch noch andere Sicherheitsfaktoren

berücksichtigt werden. Zudem muss das Unternehmen den Schutz der Daten auch zukünftig sicherstellen. Aus Unternehmersicht ist es auch wichtig den Fortschritt bezüglich der IT-Sicherheit weiter zu verfolgen und dementsprechend in die IT-Sicherheit im Unternehmen zu investieren.

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

Allen, J. H. (2006). Plan, do, check, act. URL: https://www.us-cert.gov/bsi/articles/best-practices/deployment-and-operations/plan-do-check-act [Stand:18.08.2018].

BKA (2014). Österreichisches informationssicherheitshandbuch.version 4.0.0. 15.10.2014. URL: https://www.sicherheitshandbuch.gv.at [Stand: 22.08.2018].

BSI (2018). Common criteria. URL: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ITSicherheitskriterien/CommonCriteria/commoncriteria_node.html [Stand:23.08.2018].

Chaula, J. A., Yngström, L., and Kowalski, S. (2004). Security metrics and evaluation of information systems security. Department of uni.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. (2008). Performance measurement guide for information security. *NIST Special Publication 800-55 Revision 1*.

Database (2018). Database. URL: https://codex.wordpress.org/Database_Description [Stand:25.08.2018].

Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. 04:92–100.

DSG (2018). Dsgvo. URL: https://www.dsb.gv.at/verordnungen-in-osterreich [Stand:25.08.2018].

Eloff, J. and Eloff, M. (2005). Information security architecture. *Computer Fraud & Security*, 2005(11):10 – 16.

Eloff, M. and von Solms, S. (2000). Information security management: A hierarchical framework for various approaches. 19:243–256.

Farn, K.-J., Lin, S.-K., and Fung, A. R.-W. (2004). A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6):501–513.

Halfond, W. G. J., Viegas, J., and Orso, A. (2006). A classification of sql injection attacks and countermeasures.

Herath, T., Herath, H., and Bremser, W. G. (2010). Balanced scorecard implementation of security strategies: A framework for it security performance management. *Information Systems Management*, 27(1):72–81.

Huang, S., Lee, C., and Kao, A. (2006). Balancing performance measures for information security management: A balanced scorecard framework. *Industrial Management & Data Systems*, 106(2):242–255.

Installation, P. (2018). Plugin installation. URL: `https://codex.wordpress.org/Managing_Plugins` [Stand:25.08.2018].

Institute, I. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*. Books 24x7 IT PRO. IT Governance Institute.

ISO (2018). Iso/iec 27002:2005. URL: `https://www.iso.org/standard/50297.html` [17.09.2018].

ISO27k (2018). Iso27k information security. URL: `http://www.iso27001security.com/index.html` [17.09.2018].

ISO/IEC27000 (2014). Information technology-security techniques-information security management systems-overview and vocabulary. *International Organization of Standardization*.

ISO/IEC27004 (2016). Information technology-security techniques-information security management-monitoring, measurement, analysis and evaluation. *International Organization of Standardization*.

Issa Atoum, A. O. (2016). Holistic performance model for cyber security implementation frameworks. *International Journal of Security and Ist Applications.*, 10(3):111–120.

Isselhorst, H. (2016). Überblick it-grundschutz. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Ueberblick-IT-Grundschutz.pdf?__blob=publicationFile&v=5` [Stand:23.08.2018].

Kahraman, E. (2005). Evaluating it security performance with quantifiable metrics. Master's thesis, Stockholm University and Royal Institute of Technology, Sweden.

Kaplan, R. and P. Norton, D. (1991). The balance scorecard-measures that drive performance. 70:71–9.

Kaplan, R. and P. Norton, D. (2007). Using the balanced scorecard as a strategic management system. 85.

Keyes, J. (2005). *Implementing The It Balanced Scorecard: Aligning It With Corporate Strategy*. Auerbach Publications, Boston, MA, USA.

Lee, J. S., Kim, S. C., and Sohn, S. W. (2001). A design of the security evaluation system for decision support in the enterprise network security management. In Won, D., editor, *Information Security and Cryptology — ICISC 2000*, pages 246–260, Berlin, Heidelberg. Springer Berlin Heidelberg.

Martinsons, M., Davison, R., and Tse, D. (1999). The balanced scorecard: a foundation for the strategic management of information systems. *Decision Support Systems*, 25(1):71 – 88.

Montesino, R. and Fenz, S. (2011). Automation possibilities in information security management. In *2011 European Intelligence and Security Informatics Conference*, pages 259–262.

MySQL (2018). Mysql. URL: `https://www.mysql.com/de/` [Stand:25.08.2018].

OmkarSoft (2018). Wordpress architecture. URL: `https://www.omkarsoft.com/wordpress-plugin-development/` [Stand:25.08.2018].

Patel, S., R. Rathod, V., and Prajapati, J. (2011). "performance analysis of content management systems joomla, drupal and wordpress". 21:39–43.

Patriciu, V.-V., Priescu, I., and Sebastian, N. (2006). Security metrics for enterprise information systems.

Peláez, M. H. S. (2010). Measuring effectiveness in information security controls. *The SANS Institute*.

Pereira, T. and Santos, H. (2014). Security metrics to evaluate organizational it security. In *Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance*, ICEGOV '14, pages 500–501, New York, NY, USA. ACM.

PhpStorm (2018). Phpstorm. URL: `https://www.jetbrains.com/phpstorm/` [Stand:25.08.2018].

Plusmobile (2018). Plus mobile. URL: `http://www.plusmobile.at/l` [17.08.2018].

Sahibudin, S., Sharifi, M., and Ayat, M. (2008). Combining itil, cobit and iso/iec 27002 in order to design a comprehensive it framework in organizations. In *Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)*, AMS '08, pages 749–753, Washington, DC, USA. IEEE Computer Society.

Savola, R. (2009). A security metrics taxonomization model for software-intensive systems. *JIPS*, 5:197–206.

Siebenhandl, M. (2011). Schaffung eines nachhaltigen it-security managementkonzepts für kleine und mittlere unternehmen. Master's thesis, Universität Wien.

Tashi, I. and Ghernaouti, S. (2007). Security metrics to improve information security management. *Security Conference, Las Vegas*.

Vaithyasubramanian, S., Christy, A., and Saravanan, D. (2014). An analysis of markov password against brute force attack for effective web applications. 8:5823–5830.

Wampserver (2018). Wampserver. URL: http://www.wampserver.com/en/ [Stand:25.08.2018].

Weiß, S., Weissmann, O., and Dressler, F. (2005). A comprehensive and comparative metric for information security. Proceedings of IFIP International Conference on Telecommunication Systems, Modeling and Analysis.

Whitman, M. and Mattord, H. (2005). *Principles of Information Security.* (Fourth Edition). Cengage Learning.

WordPress. Template files. URL: https://developer.wordpress.org/themes/basics/template-files/ [Stand:25.08.2018].

WordPress. Writing a plugin. URL: https://codex.wordpress.org/Writing_a_Plugin [Stand:25.08.2018].

wpsignon (2018). wpsignon. URL: https://developer.wordpress.org/reference/functions/wp_signon/ [Stand:25.08.2018].