Fraunhofer IEE

FRAUNHOFER-INSTITUT FÜR ENERGIEWIRTSCHAFT UND ENERGIESYSTEMTECHNIK, IEE

ABSCHLUSSBERICHT

Handlungsempfehlungen für den sicheren Betrieb von Regionalkraftwerken

ABSCHLUSSBERICHT

Handlungsempfehlungen für den sicheren Betrieb von Regionalkraftwerken

M. Sc. Stefan Siegl
M. Sc. Vitalij Pankraz
B. Sc. Claudius Sonntag

Projektnummer: 113565

Inhalt

Abkürzungsverzeichnis

ALG Application Level Gateways
ASVS Application Security Verification Standard
BDEW Bundesverband der Energie- und Wasserwirtschaft
BSI Bundesamt für Sicherheit in der Informationstechnik
CERTs Computer Emergency Response Teams
CWE Common Weakness Enumeration
DBMS Dastabase Management System
DBS Dastabase System
DMZ Demilitarized Zone
DoS Denial of Service
EEX European Energy Exchange
EPEX European Power Exchange
ESB Enterprise Service Bus
HTTPS Hypertext Transfer Protocol Secure
ICS Industrial Control System
IEC International Electrotechnical Commission
IKT Informations- und Kommunikationstechnik
IoT Internet of Things
ISO International Organization for Standardization
ISMS Information Security Management
ITU International Telecommunication Union
ITL Information Technology Laborator
ITG IT-Grundschutz
ITSiG Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
KWK Kraft-Wärme-Kopplung
NERC CIP North American Electric Reliability Corporation Critical Infrastructure Protection Introduction
NTP Network Time Protocol
NIST National Institute of Standards and Technology
OSI Open System Interconnection Referenzmodell
OWASP Open Web Application Security Project
PL Procedural Language
REST Remote Terminal Unit
RTU Remote Terminal Unit
RFID Radio-Frequency Identification
SCADA Supervisory Control and Data Acquisition
SSL Secure Socket Layer
SOA Service Oriented Arhitecture
SOAP Simple Object Access Protocol
SPS Speicherprogrammierbare Steuerung
SQL Structured Query Language
TLS transport Layer Security
TCP Transmission Control Protocol
TCP/IP Transmission Control Protocol/Internet Protocol
UDP User Datagram Protocol
VK Virtuelles Kraftwerk bzw. Regionalkraftwerk
VPN Virtual Private Network
WSC World Standards Cooperation

1
Einleitung

1.1
Motivation

Im Übereinkommen von Paris im Jahr 2015 [1] hat die internationale Gemeinschaft ihre Bereitschaft signalisiert, die globale Erderwärmung auf unter 2° C zu begrenzen. Lange vor diesem Abkommen stand bereits fest, dass regenerative Energiequellen für die zukünftige Energieversorgung eine zentrale Rolle einnehmen. Gemäß der aktuellen Empfehlung [2] an die Bundesrepublik wird als nationales Ziel ein Ausgleich zwischen Emissionen und Senken bzw. Netto-Null Treibhausemissionen bis weit vor dem Jahr 2050 gefordert.
Regionalkraftwerke, im folgendem auch als Virtuelle Kraftwerke (VK) bezeichnet, sind das zentrale Werkzeug, um eine stabile Energieversorgung auf der Grundlage von erneuerbaren Energiequellen zu ermöglichen und Stabilität im Stromnetz zu gewährleisten. Durch den Einsatz von virtuellen , wird den Energieversorgern ein Werkzeug angeboten, eine stabile Energieversorgung auf der Grundlage von erneuerbaren Energiequellen umsetzen zu können. Unabhängig von der räumlichen Verteilung der Erzeugungsanlagen eröffnet sich hierbei ein hohes Maß an Flexibilität bezüglich der Reaktion auf Laständerungen im Stromnetz.
Aus der IT-Sicherheitsperspektive unterscheiden sich zentrale Stromerzeugungsanlagen zu VK in einer deutlich umfangreicheren Informations- und Kommunikationstechnik (IKT) und bieten dadurch eine weit größere Angriffsfläche [3]. Diese Entwicklung ist vergleichbar zur verstärkten Nutzung von IoT-Geräten in der Industrie sowie im privaten Bereich. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt dazu auch im aktuellen Bericht [4] wieder eine Einschätzung zur Gefährdung durch den verstärkten Einsatz von IoT-Geräten. Je mehr Anlagen in einem VK integriert sind, desto mehr steuerbare Leistung liegt in der Verantwortung des VK-Betreibers. Ein Ausfall von genügend vielen Anlagen stellt ein großes Risiko für die elektrische Energieversorgung dar.
Aus diesen und weiteren Ereignissen wie z.B. Terroranschläge und (Hacker)-Angriffe auf das Stromnetz hat der Gesetzgeber 2015 das IT-Sicherheitsgesetz (ITSiG) verabschiedet. Das Artikelgesetz weist dem BSI die zentrale Rolle beim Schutz von kritischer Infrastruktur zu und führt zudem eine Meldepflicht bei Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Systemen, Komponenten oder Prozessen ein, welche zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit geführt haben oder führen können [5].

1.2
Ziele

Aufgrund der sensiblen Rolle, die ein VK innerhalb der Energieversorgung einnimmt, hat das Thema Sicherheit eine große Bedeutung für Betreiber von VK. Dieser Bericht soll zum einen ein Grundlagenverständniss zu aktuellen Normen und Standards vermitteln sowie für das Thema Sicherheit sensibilisieren und zum anderen konkrete Handlungsempfehlungen für den sicheren Betrieb von VK geben. Die vorgestellten Handlungsempfehlungen basieren auf der in Kapitel 3 beschriebenen Architektur und beschränken sich nur auf die Kernkomponenten eines VK. Als Grundlage werden aktuelle Standards, welche vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie des National Institute of Standards and Technology (NIST) herangezogen. Weiterhin wird sich nur auf den Betrieb eines VK beschränkt obwohl das Thema Sicherheit bereits in der Entwick-

lung berücksichtigt werden muss. Zur Einschränkung des Umfangs muss das Thema Sicherheit in der Entwicklung von VK zu einem späteren Zeitpunkt erarbeitet werden. Weiterhin liefern die hier beschriebenen Handlungsempfehlungen noch keine Grundlage für eine Zertifizierung in irgendeiner Form, geben jedoch eine Orientierung.

1.3 Inhalte

Im Kapitel 1 wird eine Übersicht gegeben sowie die Ziele und der Rahmen dieses Berichts erläutert. Kapitel 2 gibt eine Übersicht über den aktuellen Stand von relevanten Normen, Gremien und Standards welche sich mit Sicherheitsaspekten beschäftigen. Es wird ein Fokus auf den ITG gelegt, da es die Hauptreferenz für Empfehlungen darstellt. Weiterhin wird die grundlegende Architektur eines VK erläutert um ein Verständnis zu schaffen welche Aspekte eines VK schutzbedürftig sind. Für die konkreten Handlungsempfehlungen wird zunächst in Kapitel 3 ein VK gemäß ITG modelliert um die konkreten Bausteine untersuchen zu können. Kapitel 4 gibt konkrete Handlungsempfehlungen für die einzelnen Kernkomponenten des zuvor modellierten VK. Den Schluss bildet eine Zusammenfassung in Kapitel 5 sowie Details zur praktischen Sicherheitsanalys der Powertrade Plattform der Enertrag.

2
Grundlagen

2.1
Standards, Organisationen und Verbände

2.1.1
ISO/IEC

Internationale Normen schaffen die Bedingungen für das Handeln der Marktteilnehmer auf dem globalen Markt. Sie schaffen gleiche Bedingungen für die Marktteilnehmer und sollen damit einem fairen und freien Welthandel fördern. Diese internationalen Normen werden von der Internationalen Organisation für Normung (ISO) und der internationalen elektrotechnischen Kommission (IEC) erarbeitet[1], die gemeinsam mit der Internationalen Fernmeldeuniunion (ITU) die International Organisation für Normung bilden. Die Internationale Organisation für Normung (ISO) erarbeitet internationale Normen in fast allen Bereichen. Für den Bereich der Elektrik und Elektronik ist die Internationale elektrotechnische Kommission (IEC) zuständig. Für Normung im Bereich der Telekommunikationstechnik ist die Internationale Fernmeldeunion (ITU) zuständig. Diese Organisation bilden zusammen die Arbeitsgemeinschaft World Standards Cooperation[2] (WSC). Die drei Organisationen haben sich zusammengeschlossen, um ihre gemeinsamen Interessen im Hinblick auf die Stärkung und Weiterentwicklung eines freiwilligen und konsenbasierten internationalen Normensystems zu wahren. Diese internationalen Normen funktionieren durch einen gemeinsamen Konsens und Transparenz. Die Gemeinschaft unter dem Titel World Standard Cooperation vertritt die Ansicht, dass internationale Normen ein wichtiges Instrument für den globalen Handel und die wirtschaftliche Entwicklung sind, weil sie eine Vereinheitlichung der weltweit genutzten Technologien bedeuten. Gleichzeitig erhöhen internationale Normen die Marktrelevanz und -akzeptanz und sind somit wichtig für den globalen Handel und die Entwicklung.

2.1.2
NIST

In den Vereinigten Staaten werden Standards durch das National Institute of Standards and Technology[3] (NIST) erlassen. Es wurde durch den National Institute of Technology Act, 2007, zu einer Institution von nationaler Bedeutung erklärt, die sich mit der Forschung in den Bereichen von Ingenieurswesen, Technologie, Management, Bildung, Wissenschaft bis hin zur Kunst beschäftigt. Das NIST soll bei der Entwicklung von Innovationen helfen. Die Grundlage für diese Unterstützung sind Messungen. Die standardisierten und festgelegten Maßeinheiten erlauben es, dass heutige Innovationen, die zumeist aus Systemen bestehen, miteinander funktionieren. Am National Insitute of Standard and Technology (NIST) gibt es das Information Technology Laboratory (ITL), das die Aufgabe hat, die US-Industrie, die Regierung und die akademische Welt insoweit zu unterstützen, dass es die Messung von Informationstechnologie auf eine Art und Weise fördert, welche die wirtschaftliche Sicherheit erhöht. Dafür haben Forscher des ITL detaillierte Protokolle und Betriebsstandards entwickelt, welche die Sicherheit in ihrem Vorhaben verbessern und haben Bewertungskriterien sowie Testdatensätze für die

[1] https://www.din.de/de/din-und-seine-partner/din-in-der-welt/internationale-normung
[2] https://www.itu.int/en/ITU-T/extcoop/Pages/wsc.aspx
[3] https://www.nist.gov/

Validierung von Indsutrieprodukten festgelegt. Das ITL legt Metriken, Tests und Werkzeuge für ein breites Spektrum von Themen wie Informationskomplexität und -verständnis, vertrauenwürdiger Software, koordinierter mobiler und drahtloser Datenverarbeitung sowie Fragen der Informationsqualität, -integrität und -verwendbarkeit fest. Nach dem Federal Information Security Management Act ist das ITL mit der Entwicklung von Cybersicherheitsstandards, Richtlinien und damit verbundenen Methoden und Techniken betraut.

2.1.3 OWASP

Das Open Web Application Security Project[4] (OWASP) ist eine Non-Profit-Organisation. Sie hat sich das Ziel gesetzt, die Sicherheit von Anwendungen und Diensten im World Wide Web zu stärken. Dabei soll dem Endanwender sowie anderen Organisationen durch eine hohe Transparenz geholfen werden, wichtige Entscheidungen hinsichtlich der Sicherheitsrisiken bei Software zu treffen. Es bietet mit seinem OWASP Application Security Verification Standard (ASVS) die Grundlage, um die Sicherheit von Webanwendungen zu testen und stellt den Enwicklern zusätzlich eine Liste von Anforderungen für eine sichere Entwicklung zur Verfügung. Das primäre Ziel dahinter ist, Sicherheit so zu gewährleisten, dass sie in der Wirtschaft auch angewendet werden kann. Der Standard kann verwendet werden, um eine Vertrauensebene an die Sicherheit von Webanwendungen zu schaffen.

2.1.4 ICS Security Kompendium

Das Grundlagenwerk [6] bietet einen guten Überblick über die industriellen Steuerungs- und Automatisierungstechniken sowie deren Absicherung. Die wichtigsten Kapitel des Kompendiums sind:

- Grundlagen von ICS
- Gefährdung der IT Security
- Organisationen, Verbände und deren Standards
- Best Practice Guide für Betreiber
- Methodik für Audits von ICS-Installationen
- Trends und daraus resultierender Forschungs- und Entwicklungsbedarf

2.1.5 VGB-Standard IT-Sicherheit

Das ICS Security Kompendium weist auf den VGB-Standard IT-Sicherheit für Erzeugungsanlagen (VGB-S-175-00-2014-04-DE) hin, welcher vom VGB PowerTech e.V. [7] herausgegeben wird. An dem Werk waren 14 Autoren aus verschiedenen Energiekonzernen sowie TÜV und IT-Sicherheitsberater beteiligt. Es besteht aus Grundlagen zur IT-Sicherheit im ersten Teil und einem aus 66 Anforderungen bestehenden Katalog im zweiten Teil. Dabei werden viele Anforderungen aufgegriffen, welche aus dem IT-Grundschutz und IT-Grundschutz-Kompendium bekannt sind. Der Vorteil dieses Standards liegt vor allem in der Kompaktheit der zielgruppenspezifischen Darstellung der Inhalte und den Handlungsempfehlungen im Anhang. Der Fokus des Standards liegt auf Großkraftwerken und Erzeugungsanlagen. Für virtuelle Kraftwerke spielt der Standard daher keine weitere Rolle.

[4] https://owasp.org/

2.1.6
Industrieforum VHPready e.V.

Das Industrieforum VHPready e. V.[5] entwickelt einen Industriestandard für die Vernetzung dezentraler Energieanlagen sowie ein Zertifizierungsprogramm und dazugehörige Prüfwerkzeuge. Beteiligt sind derzeit 47 Unternehmen aus Wirtschaft und Forschung. Die von Vattenfall Europe Wärme AG [8] veröffentlichten technischen Anforderungsspezifikationen von VHPready e. V. beschreiben Anforderungen für die Interoperabilität von virtuellen Kraftwerken. Sicherheitsanforderungen werden in dieser Spezifikation nur in sehr geringem Umfang betrachtet. Es wird hauptsächlich auf die sichere Kommunikation via VPN eingegangen.

2.2
IT-Grundschutz

Der IT-Grundschutz (ITG) wurde erstmals 1994 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Kooperation mit führenden Wirtschaftsunternehmen konzipiert und als sogenanntes IT-Grundschutzhandbuch veröffentlicht[6]. Zunächst lag der Schwerpunkt des ITG bei Vorschlägen für Sicherheitsmaßnahmen und Sicherheitskonzepten für Ministerien und öffentliche Stellen. Das IT-Grundschutzhandbuch entwickelte sich weiter, woraus die BSI-Standards 100-1, 100-4 und der ITG-Katalog im Jahr 2005 hervorgingen. Mit der Veröffentlichung der BSI-Standards hatte der IT-Grundschutz die Entwicklung von einer überwiegend technischen Sicherheitssicht hin zu einem umfassendem Werk vollzogen. Das Thema Sicherheitsmanagement gewann stärker an Bedeutung und als Folge hat es sich als Standardwerk für das IT-Sicherheitsmanagement in Deutschland etabliert [9].

> Seit mehr als 20 Jahren ist der IT-Grundschutz eine bewährte Methodik, um das Niveau der Informationssicherheit in Behörden und Unternehmen jeder Größenordnung zu erhöhen[7].

Mit der Modernisierung des ITG im Jahr 2017 wurden die folgenden Verbesserungen umgesetzt [10].

- schnellere Bereitstellung von Inhalten und Empfehlungen
- bessere Strukturierung und Verschlankung der IT-Grundschutz-Kataloge
- Skalierbarkeit an Größe und Schutzbedarf der Institution
- Berücksichtigung von Risikomanagement-Prozessen
- Integration von industrieller IT
- Berücksichtigung von anwenderspezifischen Anforderungen

Dazu wurden die BSI-Standards 200-1, 200-2 und 200-3 veröffentlicht und lösten die entsprechenden Standards der 100-x Reihe ab.
Wie in Abbilidung 1 dargestell, setzt sich der modernisierte ITG aus den folgenden fünf Dokumenten zusammen, welche im Weiteren näher erläutert werden.

2.2.1
BSI-Standard 200-1

Der Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) [11]. Er ist vollständig kompatibel zur Norm ISO/IEC

[5] https://www.vhpready.de/de/home/
[6] https://www.bsi.bund.de/DE/DasBSI/Historie/historie_node.html
[7] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzAbout/itgrundschutzAbout_node.html

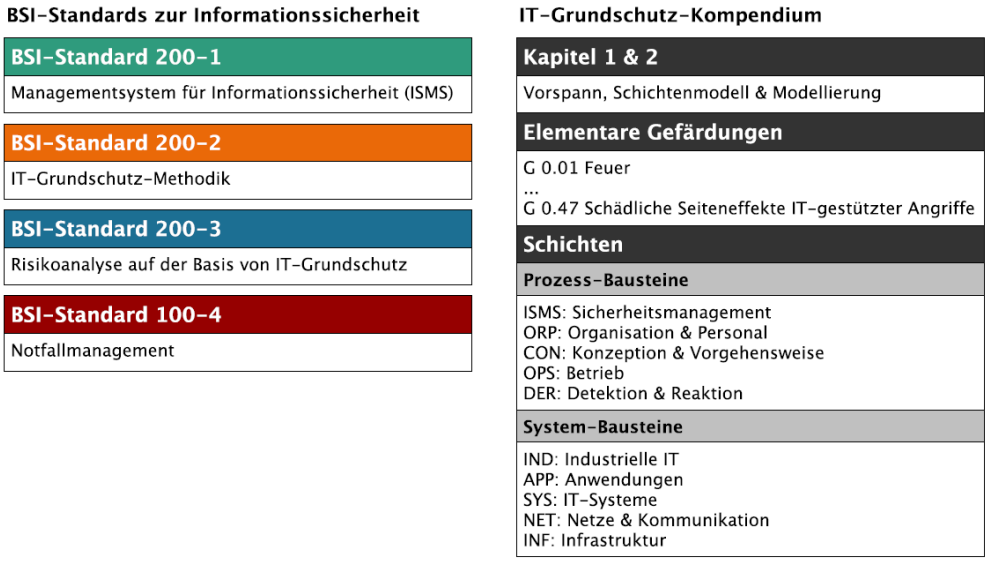


Abb. 1 Übersicht über den modernisierten IT-Grundschutz

27001 und berücksichtigt die Empfehlungen der anderen ISO-Standards wie beispielsweise ISO/IEC 27002. Ein ISMS ist die grundlegende Voraussetzung für die Umsetzung und Aufrechterhaltung wichtiger Sicherheitsmaßnahmen. Ohne ein Management bzw. den richtigen Prozessen ist eine permanente Aufrechterhaltung von Sicherheitsaspekten unrealistisch. Daher ist jede Institution d.h. der VK-Betreiber sowie Parkbetreiber und Anlagenhersteller dafür zuständig, ein ISMS zu etablieren.

2.2.2 BSI-Standard 200-2

Der Standard 200-2 [12] bildet die Basis der bewährten BSI-Methodik und beschreibt dabei Schritt für Schritt den Aufbau eines soliden ISMS. Er etabliert drei Vorgehensweisen (Basis-, Kern- und Standardabsicherung) bei der Umsetzung des ITG. Abbildung 2 zeigt die drei Sicherheitsniveaus und die relative Menge der zu berücksichtigenden Systeme. Für die Basis-Absicherung muss eine Institution über viele Systeme hinweg nur grundlegende Risiken berücksichtigen. Dieses Niveau eignet sich für den Einstieg in ein ISMS und bietet eine grundlegende Erstabsicherung von Geschäftsprozessen und Ressourcen. Bei der Kern-Absicherung wird zunächst eine Menge von besonders kritischen Systemen identifiziert und für diese hohe Sicherheitsanforderungen gestellt. Dieses Vorgehen lässt sich vergleichsweise schnell umsetzen, da nur wenige Systeme zu betrachten sind. Die Standard-Absicherung bietet vollumfänglich Schutz und ist bspw. für die ISO/IEC 27001 Zertifizierung notwendig.

2.2.3 BSI-Standard 200-3

Der BSI-Standard 200-3 beinhaltet alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes [13]. Er bietet sich an, wenn Institutionen bereits erfolgreich mit der ITG-Methodik arbeiten und möglichst direkt eine Risikoanalyse an die ITG-Analyse anschließen möchten. Sie ist zwar nicht Teil der Basis-Absicherung, jedoch Bestandteil der Standard-Absicherung sowie der Kern-Absicherung. Bei der Risikoanalyse werden alle speziellen und elementaren Gefährdungen eines Bausteins einzeln betrachtet. Bspw. wird durch gezielte Diskussion mit Experten und anhand wissenschaft-

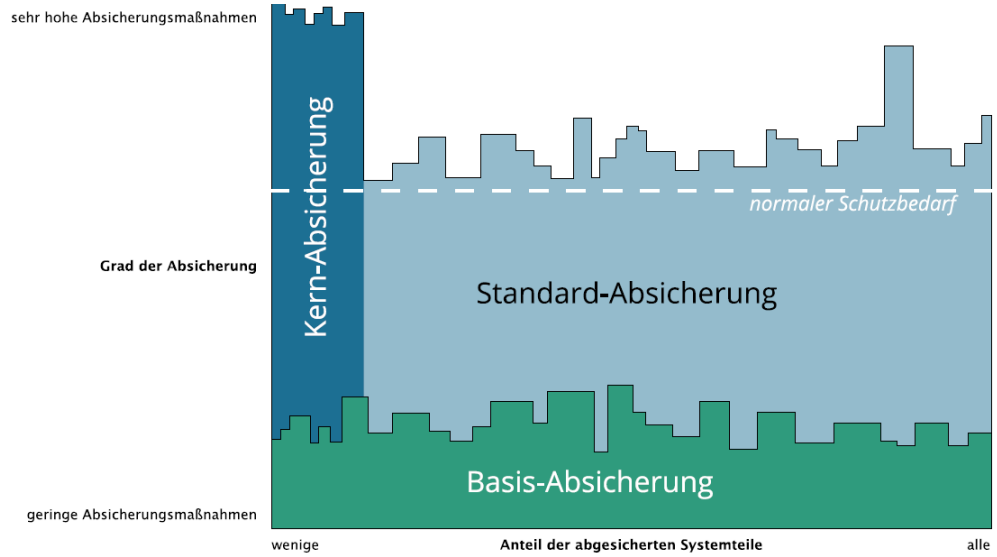


Abb. 2 Menge der zu berücksichtigenden Systeme pro Sicherheitsniveau [10]

licher Erkenntnisse eine Einschätzung darüber getroffen, wie häufig Angriffe und Fehler auftreten und welche Auswirkungen bestimmte Vorfälle haben. Jede Gefährdung eines Bausteins wird anhand von standardisierten Eigenschaften eingeschätzt. Als Beispiel wird für den Baustein APP.3.1 (Webanwendung) die Gefährdungslage 2.2 „Umgehung der Autorisierung bei Webanwendungen“ definiert:

> Angreifer versuchen häufig, auf Funktionen oder Daten von Webanwendungen zuzugreifen, die nur für eine eingeschränkte Benutzergruppe verfügbar sind. Ist die Autorisierung fehlerhaft umgesetzt, kann ein Angreifer unter Umständen die Berechtigungen eines anderen Benutzers mit umfangreicheren Rechten erlangen und somit auf geschützte Bereiche und Daten zugreifen. Das geschieht üblicherweise, indem ein Angreifer seine Eingaben gezielt manipuliert.

In Tabelle 1 sind beispielhaft zwei Gefährdungslagen dargestellt. Die zweite Spalte ist die erwähnte Gefährdungslage 2.2. Durch eine eingeschätzte Eintrittswahrscheinlichkeit dieser Gefährdung und der Kritikalität der Auswirkung lässt sich das Risiko ableiten. Das Risiko wird dabei als gering, mittel, hoch oder sehr hoch eingestuft. Bei einer Einstufung von mittel, hoch oder sehr hoch muss die Gefährdung behandelt werden. Durch eine Einschätzung eines Experten kann die Eintrittswahrscheinlichkeit der Gefährdung 2.2 als häufig sowie die Auswirkung als existenzbedrohend eingeschätzt werden. Daher wird für diese Gefährdung eine hohes Risiko angenommen.

Legende zu den Beschreibungen aus Tabelle 1.

- BS 2.1: Programmierfehler sind wahrscheinlich, Auswirkungen aber nicht immer direkt existenzbedrohend.
- BS 2.7: Sehr gängige Praxis z.B. Brute-Force-Angriffe

Legende zu den Bewertungen aus Tabelle 1.

- BW 2.2: In OWASP Top 10, A2:2017-Broken Authentication, daher häufig.
- BW 2.7: Verhinderung durch Logfile-Analyse (z.B. Fail2Ban) zusätzliche Verzögerungen und Captcha-Techniken. Siehe OWASP Cheat Cheet.

Legende zu den Behandlungen aus Tabelle 1.

- BHR 2.2: Die Anforderung APP.3.1.A22 Durchführung von Penetrationstests(CIA) MUSS in regelmäßigen Abständen durchgeführt werden (Reduktion).

Gefährdung	Vertraulichkeit	Integrität	Verfügbarkeit	Eintrittswkt.	Auswirkung	Risiko	Beschreibung	Bewertung	Behandlung
APP.3.1.SP.2.1 Mängel bei der Entwicklung und der Erweiterung von Webanwendungen	**X**	**X**	**X**	**selten**	**begrenzt**	**gering**	**BS 2.1**		
APP.3.1.SP.2.2 Umgehung der Autorisierung bei Webanwendungen	**X**	**X**		**häufig**	**existenzb.**	**sehr hoch**		**BW 2.2**	**BHR 2.2**
APP.3.1.SP.2.7 Missbrauch einer Webanwendung durch automatisierte Nutzung			**X**	**sehr häufig**	**existenzb.**	**sehr hoch**	**BS 2.7**	**BW 2.7**	**BHR 2.7**

Tab. 1 Beispiel der Risikoanalyse nach BSI-Standard 200-3 für Zielobjekt APP-01, die Webanwendung eines VK.

- BHR 2.7 Anforderungen APP.3.1.A24 Verhinderung der Blockade von Ressourcen [Entwickler] MUSS zusätzlich umgesetzt werden (Reduktion).

Grundsätzlich gibt es vier Möglichkeiten der Risikobehandlung. Die Risiko-Vermeidung steht für eine Umstrukturierung des Geschäftsprozesses oder des Informationsverbunds, die Risiko-Reduktion (BHR) steht dafür, das Risiko durch weitere Sicherheitsmaßnahmen zu reduzieren. Beim Risiko-Transfer wird das Risiko an eine andere Institution z.B. eine Versicherung oder durch Outsourcing behandelt und bei der Risiko-Akzeptanz können die Risiken auf Grundlage einer nachvollziehbaren Faktenlage akzeptiert werden. Wie in Tabelle 1 beschrieben, liefern die gewählten Risikobehandlungen eine Reduktion der Gefährdungen.

2.2.4 BSI-Standard 100-4

Ziel des Notfallmanagements ist es, sicherzustellen, dass die wichtigen Geschäftsprozesse in kritischen Situationen höchstens temporär unterbrochen werden und die wirtschaftliche Existenz der Institution bei einem größeren Schadensereignis gesichert bleibt.

> Das Notfallmanagement ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren. Um die Funktionsfähigkeit und damit das Überleben eines Unternehmens oder einer Behörde zu sichern, sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einem Notfall oder einer Krise ermöglichen. Das Notfallmanagement umfasst das geplante und organisierte Vorgehen, um die Widerstandsfähigkeit der (zeit-)kritischen Geschäftsprozesse einer Institution nachhaltig zu steigern, auf Schadensereignisse angemessen reagieren und die Geschäftstätigkeiten so schnell wie möglich wieder aufnehmen zu können [...] [14].

Der Standard zum Notfallmanagement ist noch nicht in den modernisierten ITG überführt worden, ist jedoch in Planung[8].

2.3 Architektur virtueller Kraftwerke

VKs sind ein wichtiges Werkzeug zur Sicherstellung einer stabilen Eneregieversorgung aus erneuerbaren Energiequellen. Eine wichtige Grundeigenschaft ist ein flexibles Reaktionsverhalten auf Laständerungen im Stromnetz.

> Unter einem virtuellen Kraftwerk wird die zentrale Steuerung mehrerer dezentraler Stromerzeugungsanlagen [aus erneuerbaren Energiequellen unter Berücksichtigung und Einbindung von Energiespeichern und Lasten] verstanden. Dabei müssen die Anlagen räumlich nicht beieinander liegen. Ziel eines virtuellen Kraftwerks ist es, positive strategische Effekte zu erreichen, wie z. B. eine gemeinsame Vermarktung. Weiterhin ist es Ziel, strategisch Verantwortung zu übernehmen, z.B. durch die Bereitstellung von Regelenergie [15].

Eine weitere allgemeine Referenzarchitektur von VK kommt aus dem E-Energy Förderprojekt [9].

> Die E-Energy Referenzarchitektur der Technischen Universität München fasst die wichtigsten Systemkonzepte [...] in einer konsistenten Gesamtarchitektur zusammen [16].

In der E-Energy Referenzarchitektur wird ein VK wie folgt beschrieben.

> Das Virtuelle Kraftwerk bietet einerseits die Möglichkeit, Anlagen zu erfassen, zu verwalten, zu steuern und zu überwachen. Andererseits optimiert es seinen internen Betrieb fortwährend unter Einbezug von Prognosen und vermarktet sich in Form von Angeboten auf dem Marktplatz. Für den Betreiber ist das Management des VK in Form einer Leitwarte gegeben.

Am praktischen Beispiel der Architektur des VK IWES.vpp, wie in Abbildung 3 gezeigt, wird die beschriebene allgemeine Struktur im Detail deutlich und teilweise ergänzt.
Es sind grundlegend drei Geltungsbereiche zu unterscheiden. Im Geltungsbereich des Parkbetreibers befinden sich die Anlagen sowie die Steuerungstechnik (SCADA, RTU). Im Geltungsbereich des VK-Betreibers befindet sich die Backend-Software, Datenbanken sowie weitere Dienste, welche für die sichere Kommunikation (VPN) oder Visualisierung verwendet werden. Die Kommunikation zwischen diesen Bereichen erfolgt über IKT-Technologien (i.d.R. das Internet) und muss daher besonders kritisch behandelt werden. Es gibt unterschiedliche Varianten wie man diese Kommunikation mittels VPN oder anderen Maßnahmen wie geschlossenen Benutzergruppen absichern kann. In dieser Architektur befindet sich der VPN-Server im Geltungsbereich des Anlagenherstellers, jedoch sind andere Varianten ebenfalls möglich. Eine detailierte Modellierung mit Schwerpunkt auf die kritischen Kommunikationswege und Geltungsbereiche wird in Kapitel 3 gegeben.

[8] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/210118_BSI-Standard-200-4.html
[9] https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AbgeschlosseneProgrammeProjekte/E-Energy/e-energy.html

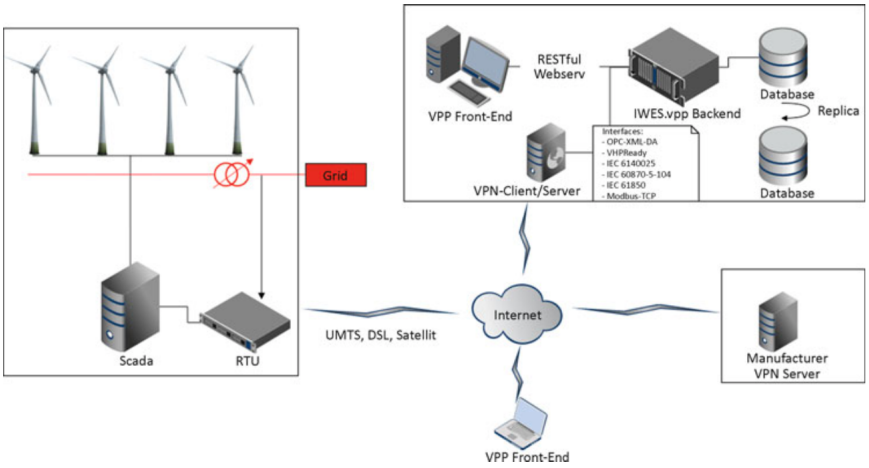


Abb. 3 Grobarchitektur des IWES.vpp

3
Modellierung gemäß IT-Grundschutz

Wie in Kapitel 2.2 bereits angedeutet, ist für eine Untersuchung eines IT-Systems aus Sicherheitsperspektive zunächst eine geeignete Modellierung erforderlich. Für die Modellierung nach ITG ist die Zusammenfassung bzw. die Gruppenbildung ähnlicher Systemteile ein elementarer Schritt zur Komplexitätsreduzierung und verändert die Modellierung nicht. Abbildung 4 zeigt einen grundlegenden Aufbau eines virtuellen Kraftwerkes nach [17]. Diese Modellierung ist so allgemein wie möglich gehalten, erhebt jedoch nicht den Anspruch eine allgemeingültige Referenzarchitektur darzustellen. Die einzelnen Komponenten werden im Folgenden genauer beschrieben.

Anlagensteuerung ist i.d.R. Teil einer Energieanlage wie z.B. einer Biogasanlage oder ein Windrad. Häufig werden diese mit Speicherprogrammierbaren Steuerungen (SPS) realisiert und mehrere Anlagen über eine Steuereinheit geregelt. In dieser Darstellung sind die einzelnen Anlagensteuerungen z. B. über einen Feldbus mit dem SCADA-Server und dem Remote Terminal Unit (RTU) verbunden.

SCADA-Steuerung/RTU bündeln die Steuerung einzelner Anlagen und stellen so die Steuerung einer größeren Anzahl von Anlagen dar. Diese Komponente wird im Allgemeinen auch als Anlagenparksteuerung oder Parksteuerung bezeichnet.

Gateway Das Gateway wird wahlweise in Anlagen verbaut, um TCP/IP basierte Datenpakete in serielle Kommunikation und umgekehrt zu wandeln. Diese technische Anforderung kommt aus dem Regelleistungskontext und wird dort als Medienbruch bezeichnet [18].

VPN-Client/Server sind notwendig, um die Netzwerkkommunikation vor dem öffentlichen Internet abzuschirmen. Grundlegend existieren zwei Varianten. Der VPN-Server ist im Netzwerk des VK-Betreibers und der Parkbetreiber betreibt einen VPN-Client welcher die VPN-Verbindung aufbaut oder der Parkbetreiber betreibt den VPN-Server und der VK-Betreiber baut mit einem Client die Verbindung auf.

Einspeisemanagement Das Einspeisemanagement ist eine Möglichkeit für den verantwortlichen Netzbetreiber, die Einspeisung von Anlagen temporär auszusetzen, wenn die Netzkapazitäten nicht ausreichen, um den erzeugten Strom zu verwerten und alle anderen Möglichkeiten ausgeschöpft sind, um das Netz zu stabilisieren. Näheres regeln § 13 Abs. 2, 3 S.3 EnWG in Verbindung mit §§ 14, 15 EEG und für KWK-Anlagen in Verbindung mit § 3 Abs. 1 S.3 KWKG [19].

Das Einspeisemanagement kommt nach der gesetzlichen Rangfolge allerdings nur zum Einsatz, wenn der Netzengpass nicht bereits durch andere geeignete Maßnahmen – insbesondere durch eine Abregelung konventioneller Kraftwerke – ausreichend entlastet werden kann. Wird EE- oder KWK-Strom per Einspeisemanagement abgeregelt, hat der Anlagenbetreiber gegenüber seinem Anschlussnetzbetreiber einen Anspruch auf Entschädigung.

Anlagenanbindung Damit die Anlagen bzw. Anlagenparks mit der zentralen Steuerung kommunizieren können, müssen diese über Informations- und Kommunikationstechnik (IKT) angebunden werden. Hierbei können Mobilfunk-, Kabel- oder Satellitenverbindungen zum Einsatz kommen. Bei der Anlagenanbindung kann es sich auch um die Anbindung mittels einer geschlossenen Benutzergruppe handeln, wie dies beispielsweise für den Regelleistungsbetrieb vorgesehen ist [18]

Webanwendung und zentrale Steuerung Der Kern eines VK ist eine Backend-Softwarekomponente, welche aus Eingangsgrößen wie Anlagen-Messdaten, Prognosen, Fahrplänen oder manueller Eingaben, Steuersignale für Anlagen berechnet. Für das Management der Anlagensteuerung wird eine Datenbank verwendet. Die Kommunikation zu Anlagen sowie anderer Gegenstellen erfolgt über definierte Schnittstellen, welche das jeweilige Kommunikationsprotokoll umsetzen.

Modellierung gemäß IT-Grundschutz

Web-Services und Schnittstellen sind weitere Softwarekomponenten, welche im Allgemeinen Informationen zwischen der VK-internen Informationsrepräsentation und einem externen Format übersetzen. Dabei werden die zu übersetzenden Informationen validiert und ggf. angereichert. Die meisten Informationen, welche über Schnittstellen eingehen, werden in eine Datenbank persistiert, um sie dem VK-Kern zur Verfügung zu stellen. Einige Schnittstellen sind herstellerspezifisch wie z.B. die SOAP-Schnittstelle[1] vom Windkraftanlagenhersteller Vestas. Andere wiederum richten sich nach einem allgemeinen Standard wie z.B. IEC 60870-5-104. Dabei sind Sicherheitsaspekte wie z.B. Authentifizierung nicht immer definiert. Auf der technischen Kommunikationsebene bewegen sich die Schnittstellen zwischen der Schicht 4 (TCP-basiert) und Schicht 7 (HTTP-basiert), bezogen auf das OSI-Referenzmodell[2]. Als Web-Service wird eine allgemeine Schnittstelle bezeichnet, mit der z.B. ein Web-Client (Webbrowser) kommunizieren kann und einem Nutzer eine grafische Oberfläche anbietet. Diese Schnittstelle muss sich um das Usermanagement sowie Rechteverwaltung kümmern, um unzulässige Zugriffe zu vermeiden.

Datenbank In einer (oder mehrerer) Datenbank(en) werden alle wichtigen Daten persistiert, um z.B. bestimmte Steuerentscheidungen treffen zu können oder das Rechtemanagement für Nutzer umsetzen zu können.

Client Ein Client kann, wie oben beschrieben, ein Webbrowser sein oder aber auch eine weitere externe Softwarekomponente, welche mit dem VK kommuniziert. Ein Client wird z.B. zum Modellieren eines Parkaufbaus im VK, zum Überwachen von Anlagenverhalten oder zum Steuern verwendet. Da sich ein Client außerhalb des Geltungsbereiches des VK-Betreibers befinden kann, müssen Informationen, welche über die Web-Schnittstelle eingehen, besonders kritisch betrachtet werden.

Externe Daten können beispielsweise Prognosedaten sein, welche über ein dateibasiertes Protokoll eingehen oder auch Wartungsmeldungen via E-Mail.

Marktschnittstelle Hierunter versteht man eine marktorientierte Schnittstelle wie z.B. EEX oder EPEX zum Handeln an der Strombörse oder dem Regelleistungsmarkt. Die Integration eines Smart-Meter-Gateways kann ebenfalls unter dieser Komponente verstanden werden.

Im weiteren Verlauf werden die Sicherheitsbetrachtungen auf Basis der Komponenten dieses Modells erwogen.

[1] https://www.w3.org/TR/2000/NOTE-SOAP-20000508/
[2] https://www.selflinux.de/selflinux/html/osi.html

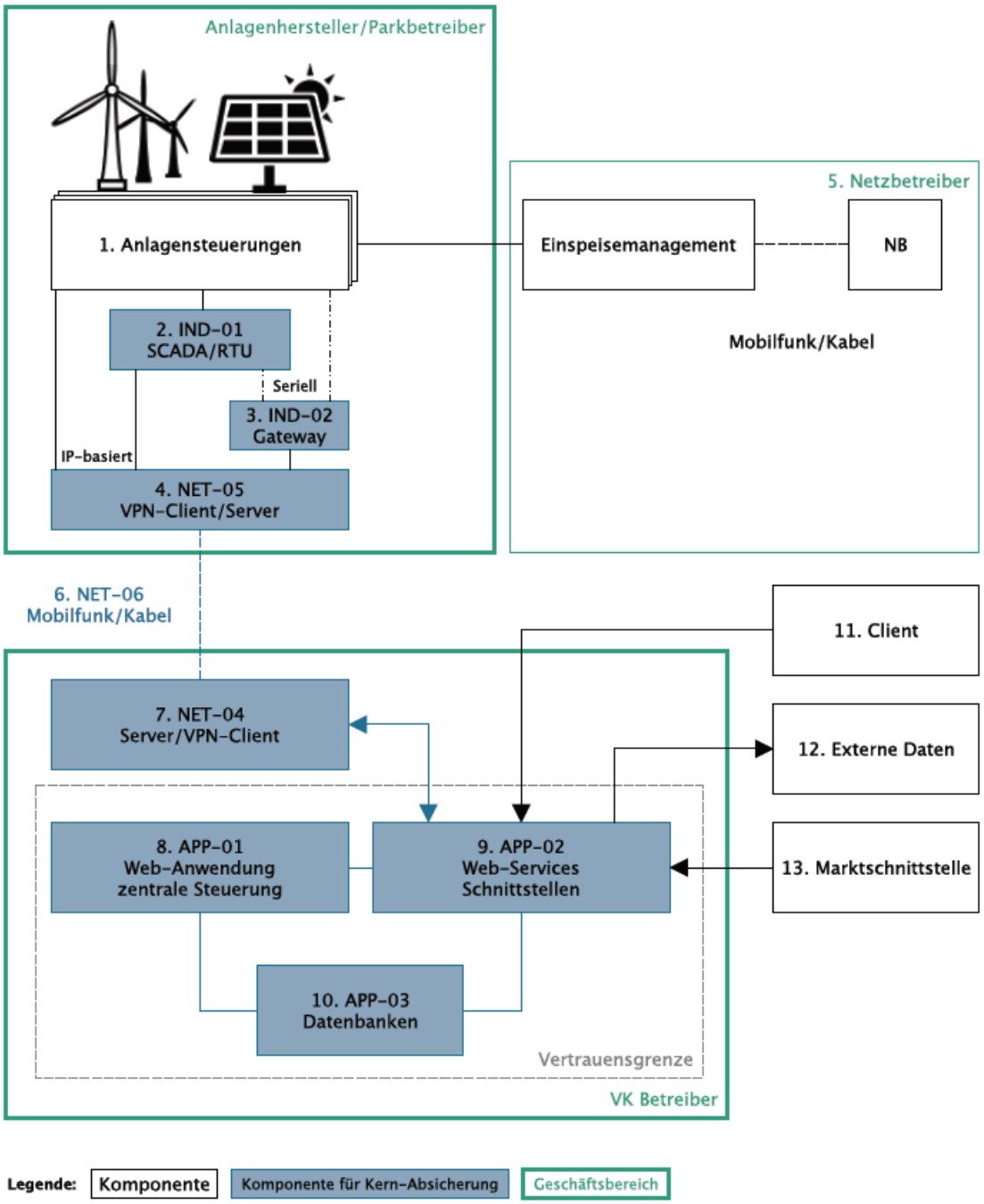


Abb. 4 Beispielarchitektur virtueller Kraftwerke nach [17]

4
Handlungsempfehlungen für Betreiber

Die folgenden Kapitel beinhalten Empfehlungen für den sicheren Betrieb einer Webanwendung (APP-01), eines Web-Services (APP-02) sowie dazugehörigen Datenbanken (APP-03) eines VK. Die Empfehlungen entsprechen überwiegend den Richtlinien wie sie in [20] formuliert sind und sind z.T. zusammengefasst.
Ebenfalls wird der Sprachgebrauch übernommen, um harte Anforderungen mit MUSS zu formulieren sowie weiche Anforderungen mit SOLLTE bzw. SOLLTE NICHT.

4.1
Betrieb einer Webanwendung

4.1.1
Updates und Sicherheitspatches

Administratoren MÜSSEN sich regelmäßig über aktuelle Schwachstellen informieren und sicherheitsrelevante Updates zeitnah einspielen. Software-Updates und Patches für Webanwendungen MÜSSEN aus vertrauenswürdigen Quellen bezogen werden. Sie MÜSSEN vor dem Roll-Out ausreichend getestet werden. Bevor Updates oder Patches installiert werden, MUSS stets sichergestellt sein, dass der ursprüngliche Zustand der Webanwendung wiederhergestellt werden kann. Das aktuelle Patchlevel MUSS dokumentiert werden.

4.1.2
Systemarchitektur

Bereits in der Entwurfsphase einer Webanwendung SOLLTEN Sicherheitsaspekte beachtet werden. Auch SOLLTE darauf geachtet werden, dass die Architektur der Webanwendung die Geschäftslogik der Institution exakt erfasst und korrekt umsetzt. In der Systemarchitektur SOLLTE vorgesehen werden, die Serverdienste durch jeweils separate IT-Systeme voneinander zu trennen. Auch SOLLTEN jeweils eigene Benutzerkonten für die unterschiedlichen Serverprozesse der Systemkomponenten verwendet werden. Dabei SOLLTEN die Rechte dieser Dienstkonten auf Betriebssystemebene soweit eingeschränkt werden, dass nur auf die erforderlichen Ressourcen und Dateien des Betriebssystems zugegriffen werden kann.
Die Netzarchitektur SOLLTE einen mehrschichtigen Ansatz verfolgen (Multi-Tier-Architektur). Dabei SOLLTEN mindestens die Sicherheitszonen Webschicht, Anwendungsschicht und Datenschicht berücksichtigt werden. Aus diesen Zonen SOLLTE NICHT auf Systeme im Intranet zugegriffen werden können.
Die Softwarearchitektur der Webanwendung SOLLTE mit allen Bestandteilen und deren Abhängigkeiten dokumentiert werden. Die Dokumentation SOLLTE bereits während des Projektverlaufs aktualisiert und angepasst werden, sodass sie schon in der Entwicklungsphase benutzt werden kann und Entscheidungsfindungen nachvollziehbar sind.
Es SOLLTEN in der Dokumentation alle für den Betrieb notwendigen Komponenten, die nicht Bestandteil der Webanwendung sind, als solche gekennzeichnet werden. Ebenso SOLLTE daraus hervorgehen, welche Komponenten welche Sicherheitsmechanismen umsetzen, wie die Webanwendung in eine bestehende Infrastruktur integriert wird und welche kryptografischen Funktionen und Verfahren eingesetzt werden.

4.1.3 Beschaffung, Entwicklung und Erweiterung

Wenn Produkte für Webanwendungen beschafft werden, SOLLTE ein Anforderungskatalog erstellt werden. Um verschiedene Produkte miteinander vergleichen zu können, SOLLTE eine Bewertungsskala entwickelt werden. Wird die eigentliche Webanwendung oder eine Erweiterung hierzu eigenentwickelt, SOLLTE ein geeignetes Vorgehensmodell genutzt werden. Dabei SOLLTEN vor der Inbetriebnahme alle Phasen des Modells durchlaufen werden. Für die Entwicklung SOLLTEN zudem Programmierrichtlinien vorgegeben werden, die dabei helfen, ein einheitliches Sicherheitsniveau zu etablieren.
Wenn die Sicherheitsmechanismen einer Webanwendung entworfen und entwickelt werden, SOLLTEN diese möglichst zukünftige Standards und Angriffstechniken berücksichtigen. Bei der Anwendungsentwicklung SOLLTEN die Entwicklungs-, Test- und Produktivsysteme voneinander getrennt sein. Falls die Webanwendung von einem Dienstleister entwickelt wird, SOLLTE sichergestellt werden, dass dieser Dienstleister die nötigen Sicherheitsanforderungen bei der Entwicklung umsetzt und der Auftraggeber jederzeit auf den Quelltext zugreifen kann.

4.1.4 Tests und Freigabe

Bevor Webanwendungen oder Erweiterungen und Anpassungen, die selbst oder im Auftrag entwickelt wurden, in den Produktivbetrieb übernommen werden, SOLLTEN sie getestet werden. Die Ergebnisse der Tests SOLLTEN dokumentiert werden. Wenn die Tests erfolgreich verlaufen sind, SOLLTE die Webanwendung formal freigegeben werden. Darüber hinaus SOLLTE ein Verfahren zur Fehlerbehebung etabliert werden.

4.1.5 Anbindung von Hintergrundsystemen

Hintergrundsysteme von Webanwendungen, auf denen Funktionalitäten und Daten ausgelagert werden, SOLLTEN ausreichend geschützt werden. Der Zugriff auf Hintergrundsysteme SOLLTE ausschließlich über definierte Schnittstellen und von definierten Systemen aus möglich sein. Der Datenverkehr zwischen den Benutzern und der Webanwendung bzw. den Anwendungen und weiteren Diensten sowie den Hintergrundsystemen SOLLTE durch Sicherheitsgateways reglementiert werden. Bei der Kommunikation über Standort- und Netzgrenzen hinweg SOLLTE der Datenverkehr außerdem authentisiert und verschlüsselt werden. Zugriffe der Webanwendung auf Hintergrundsysteme SOLLTEN zudem mit minimalen Rechten erfolgen.
Beim Einsatz eines Enterprise Service Bus (ESB) MUSS sichergestellt werden, dass sich alle Dienste gegenüber dem ESB authentisieren, bevor ihnen ein Zugriff erlaubt wird. Es SOLLTE ein eigenes logisches Netzsegment für den ESB vorhanden sein. Der Zugriff auf den ESB SOLLTE ausschließlich durch die angeschlossenen Anwendungen und Dienste möglich sein. Alle Zugriffe auf den ESB SOLLTEN authentisiert und bei der Kommunikation über Standort- und Netzgrenzen hinweg verschlüsselt sein.

4.1.6 Rechtemanagement

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktion bevollmächtigt wird, IT-Anwendungen oder Daten zu nutzen. Die Zugriffsrechte (z.B. Lesen, Schreiben, Ausführen) auf IT-Anwendungen, Teilanwendungen oder Daten sind von der Funktion abhängig, die die Person wahrnimmt, z.B. Anwenderbetreuung, Arbeitsvorbereitung, Systemprogrammierung, Anwendungsentwicklung, Systemadministration, Revision, Datenerfassung, Sachbearbeitung. Dabei SOLLTEN immer nur so viele Zugriffsrechte

vergeben werden, wie es für die Aufgabenwahrnehmung notwendig ist ("Need-to-know-Prinzip"). Umgesetzt werden MÜSSEN die Zugriffsrechte durch die Rechteverwaltung des IT-Systems. Eine Vielzahl von IT-Systemen lassen es zu, dass verschiedene Rechte als Gruppenrechte bzw. als Rechteprofil definiert werden (z.B. Gruppe Datenerfassung). Diese Definition entspricht der technischen Umsetzung der Rechte, die einer Funktion zugeordnet werden. Für die Administration der Rechte eines IT-Systems ist es vorteilhaft, solche Gruppen oder Profile zu erstellen, da damit die Rechtezuteilung und deren Aktualisierung erheblich vereinfacht werden kann.

4.1.7 Dokumentation der Benutzer und Rechteprofile

Es MUSS eine Dokumentation der am IT-System zugelassenen Benutzer, angelegten Benutzergruppen und Rechteprofile erfolgen. Dabei gibt es verschiedene Dokumentationsmöglichkeiten wie beispielsweise die folgenden.

- Vorgegebene Administrationsdateien des Systems.
- Individuelle Dateien, die vom zuständigen Administrator verwaltet werden.
- In Papierform.

Es SOLLTE eine geeignete Form ausgewählt werden, welche möglichst einheitlich für die gesamte Institution gilt. Dokumentiert werden SOLLTEN insbesondere folgende Angaben zur Rechtevergabe an Benutzer.

- Zugeordnetes Rechteprofil (gegebenenfalls Abweichungen vom verwendeten Standard-Rechteprofil).
- Begründung für die Wahl des Rechteprofils (und gegebenenfalls der Abweichungen).
- Zuordung des Benutzers zu einer Organisationeinheit, Raum- und Telefonnummer.
- Zeitpunkt und Grund der Einrichtung.
- Befristung der Einrichtung.

Folgende Angaben SOLLTEN zur Rechtevergabe an Gruppen gemacht werden.

- Zugehörige Benutzer.
- Zeitpunkt und Grund der Einrichtung.
- Befristung der Einrichtung.

Die Dokumentation der zugelassenen Benutzer und Rechteprofile SOLLTE regelmäßig (mindestens alle 6 Monate) daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt und ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzer entspricht. Die vollständige Dokumentation ist Voraussetzung für Kontrollen der vergebenen Benutzerrechte. Die Dokumentation MUSS so gespeichert beziehungsweise aufbewahrt werden, dass sie vor unbefugtem Zugriff geschützt ist und so, dass auch bei einem größeren Sicherheitsvorfall oder IT-Ausfall darauf zugegriffen werden kann. Falls die Dokumentation in elektronischer Form erfolgt, MUSS sie in das Datensicherungsverfahren einbezogen werden.

4.1.8 Dokumentation der Veränderungen eines bestehenden Systems

Um einen reibungslosen Betriebsablauf zu gewährleisten, MUSS der Administrator einen Überblick über das System haben bzw. sich verschaffen können. Dieses MUSS auch für seinen Vertreter möglich sein, falls der Administrator unvorhergesehen ausfällt. Der Überblick ist auch Voraussetzung, um Prüfungen des Systems (z.B. auf problematische

Einstellungen, Konsistenz bei Änderungen) durchführen zu können. Daher SOLLTEN die Administratoren die Veränderungen am System vornehmen, diese dokumentieren und nach Möglichkeit SOLLTE der Dokumentationsprozess automatisieren erfolgen. Dieses gilt insbesondere für Änderungen an Systemverzeichnissen und -dateien. Bei Installation neuer Betriebssysteme oder bei Updates sind die vorgenommenen Änderungen besonders sorgfältig zu dokumentieren. Möglicherweise kann durch die Aktivierung neuer oder durch die Änderung bestehender Systemparameter das Verhalten des IT-Systems (insbesondere auch Sicherheitsfunktionen) maßgeblich verändert werden. Unter Unix MÜSSEN ausführbare Dateien, auf die auch andere Benutzer als der Eigentümer Zugriff haben oder deren Eigentümer root ist, vom Systemadministrator freigegeben und dokumentiert werden. Insbesondere MÜSSEN Listen mit den freigegebenen Versionen dieser Dateien geführt werden, die mindestens das Erstellungsdatum, die Größe jeder Datei und Angaben über evtl. gesetzte s-Bits enthalten. Sie sind Voraussetzung für den regelmäßigen Sicherheitscheck und für Überprüfungen nach einem Verlust der Integrität.

4.1.9 Informationsbeschaffung über Sicherheitslücken

Gegen bekannt gewordene und durch Veröffentlichungen zugänglich gemachte Sicherheitslücken MÜSSEN die erforderlichen organisatorischen und administrativen Maßnahmen ergriffen werden. Sicherheitsrelevante Updates oder Patches für die eingesetzte Hard- und Software MÜSSEN gegebenenfalls installiert werden. Sind keine entsprechenden Updates oder Patches verfügbar, so MUSS eventuell zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden. Es ist daher sehr wichtig, dass sich die Systemadministratoren regelmäßig über neu bekannt gewordene Schwachstellen informieren. Informationsquellen zu diesem Thema sind beispielsweise die folgenden.

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI)[1]
- Hersteller bzw. Distributoren von Programmen und Betriebssystemen. Diese informieren oft registrierte Kunden über bekannt gewordene Sicherheitslücken ihrer Systeme und stellen korrigierte Varianten des Systems oder Patches zur Behebung der Sicherheitslücken zur Verfügung.
- Computer Emergency Response Teams (CERTs). Dies sind Computer-Notfallteams, die als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in bezug auf sicherheitsrelevante Vorfälle in Computersystemen dienen. CERTs informieren in sogenannten Advisories über aktuelle Schwachstellen in Hard- und Softwareprodukten und geben Empfehlungen zu deren Behebung. Verschiedene Organisationen oder Verbände unterhalten eigene CERTs. Das ursprüngliche CERT der Carnegie Mellon Universität diente als Vorbild für viele weitere derartige Teams und ist heute eine Art "Dach-CERT"[2]. In Deutschland existiert unter anderem der CERT-Bund, Bundesamt für Sicherheit in der Informationstechnik[3].
- An verschiedenen Hochschulen existieren CERTs, die auch Informationen öffentlich zur Verfügung stellen. Ein Beispiel ist das RUS-CERT der Universität Stuttgart[4].
- Hersteller- und systemspezifische sowie sicherheitsspezifische Newsgruppen oder Mailinglisten. In solchen Foren werden Hinweise auf existierende oder vermutete Sicherheitslücken oder Fehler in diversen Betriebssystemen und sonstigen Softwareprodukten diskutiert. Besonders aktuell sind meist die englischsprachigen Mailinglisten wie Bugtraq, von denen es an vielen Stellen öffentlich zugängliche Archive gibt, beispielsweise das SecurityFocus Forum[5].

[1] http://www.bsi.bund.de/
[2] http://www.cert.org
[3] https://www.bsi.bund.de/certbund/
[4] http://cert.uni-stuttgart.de
[5] http://www.securityfocus.com

- Manche IT-Fachzeitschriften veröffentlichen ebenfalls regelmäßig Beiträge mit einer Übersicht über neue Sicherheitslücken in verschiedenen Produkten.

Idealerweise SOLLTEN sich die Administratoren und der IT-Sicherheitsbeauftragte bei mindestens zwei verschiedenen Stellen über Sicherheitslücken informieren. Dabei ist es empfehlenswert, neben den Informationen des Herstellers auch eine unabhängige Informationsquelle zu benutzen. Die Administratoren SOLLTEN jedoch in jedem Fall auch produktspezifische Informationsquellen des Herstellers nutzen, um beispielsweise darüber Bescheid zu wissen, ob für ein bestimmtes Produkt beim Bekanntwerden von Sicherheitslücken überhaupt Patches oder Updates bereitgestellt werden. Bei Produkten, für die der Hersteller keine Sicherheitspatches mehr zur Verfügung stellt, MUSS rechtzeitig geprüft werden, ob ein Einsatz unter diesen Umständen noch zu verantworten ist und durch welche zusätzlichen Maßnahmen ein Schutz der betroffenen Systeme trotzdem gewährleistet werden kann.

4.1.10 Datenschutzaspekte bei der Protokollierung

Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen zu verstehen, aus denen sich die Fragen beantworten lassen: ”Wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?” Außerdem MÜSSEN sich Systemzustände ableiten lassen: ”Wer hatte von wann bis wann welche Zugriffsrechte?” Art und Umfang von Protokollierungen hängen vom allgemeinen Datenschutzrecht und auch von bereichsspezifischen Regelungen ab. Die Protokollierung der Administrationsaktivitäten entspricht einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend im allgemeinen Datenschutzrecht, während die verfahrensorientierte Protokollierung oft durch bereichsspezifische Regelungen definiert wird. Beispiele für verfahrensorientierte Protokollierung sind u. a. Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze.

4.1.11 Mindestanforderungen an die Protokollierung

Bei der Administration von IT-Systemen sind die folgenden Aktivitäten vollständig zu protokollieren.

Systemgenerierung und Modifikation von Systemparametern Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren SOLLTEN.

Einrichten von Benutzern Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren. Für diese Protokolle SOLLTEN längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

Erstellung von Rechteprofilen Im Rahmen der Protokollierung der Benutzerverwaltung kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Einrichtung bestimmter Benutzerrechte erteilt hat. Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

Änderungen an der Dateiorganisation Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der “Standard-Dateiverwaltungssysteme” ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu.

Durchführung von Datensicherungsmaßnahmen Da derartige Maßnahmen (Backup, Restore) mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbestän-

den verbunden sind und häufig in “Ausnahmesituationen” durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

Sonstiger Aufruf von Administrations-Tools Die Benutzung aller Administrations-Tools ist zu protokollieren, um feststellen zu können, ob Unbefugte sich Systemadministrator-Rechte erschlichen haben.

Bei einem Versuch unbefugten Einloggens und Überschreitung von Befugnissen sind besondere Aspekte zu beachten. Geht man von einer wirksamen Authentisierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller “auffälligen Abnormalien” beim Einloggen und der Benutzung von Hard- und Software-Komponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator. Bei der Verarbeitung von personenbezogenen Daten sind folgende Benutzeraktivitäten in Abhängigkeit von der Sensibilität der Verfahren bzw. Daten vollständig bzw. selektiv zu protokollieren.

Eingabe von Daten Die so genannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, dass Befugnisüberschreitungen anderweitig protokolliert werden, SOLLTE eine vollständige Protokollierung von Dateneingaben als Regelfall angesehen werden.

Datenübermittlungen Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist, kann eine selektive Protokollierung als ausreichend angesehen werden.

Benutzung von automatisierten Abrufverfahren In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahme im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.

Löschung von Daten Die Durchführung der Löschung ist zu protokollieren.

Aufruf von Programmen Dies kann erforderlich sein bei besonders “sensiblen” Programmen, die z.B. nur zu bestimmten Zeiten oder Anlässen benutzt werden DÜRFEN. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

4.1.12 Zweckbindung bei der Nutzung von Protokolldaten

Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung. Sie DÜRFEN NUR zu den Zwecken genutzt werden, die Anlass für ihre Speicherung waren. Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden und die Kontrollen durch interne oder externe Datenschutzbeauftragte. Nur in Ausnahmefällen lassen die bereichsspezifischen Regelungen die Nutzung dieser Daten für andere Zwecke, z.B. zur Strafverfolgung, zu.

4.1.13 Aufbewahrungsdauer von Protokolldaten

Soweit nicht bereichsspezifische Regelungen etwas anderes vorsehen, richtet sich die Aufbewahrungsdauer der Protokolle nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Protokolldaten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gibt es keinen zwingenden Grund für das wei-

tere Vorhalten von Protokolldateien, besteht eine Löschungspflicht. Als Anhaltspunkte können folgende Aspekte dienen.

- Die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß SOLLTE eine Frist von einem Jahr nicht überschritten werden. Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle aus. Auch hier sind die bereichsspezifischen Vorschriften zu beachten.
Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang SOLLTEN folgende Aspekte Berücksichtigung finden.

- Es SOLLTE ein Konzept erstellt werden, das den Zweck der Protokolle und deren Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.
- Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle MUSS ebenso gewährleistet werden wie die Manipulationssicherheit der Einträge in Protokolldateien.
- Entsprechend der Zweckbindung der Datenbestände MÜSSEN wirksame Zugriffsbeschränkungen realisiert werden.
- Die Protokolle MÜSSEN so gestaltet sein, dass eine effektive Überprüfung möglich ist. Dazu gehört auch eine IT-Unterstützung der Auswertung.
- Die Auswertungsmöglichkeiten SOLLTEN vorab abgestimmt und festgelegt sein.
- Kontrollen SOLLTEN so zeitnah durchgeführt werden, dass bei aufgedeckten Verstößen noch Schäden abgewendet sowie Konsequenzen gezogen werden können. Kontrollen MÜSSEN rechtzeitig vor dem Ablauf von Löschungsfristen von Protokolldateien stattfinden.
- Kontrollen SOLLTEN nach dem Vier-Augen-Prinzip erfolgen.
- Die Mitarbeiter SOLLTEN darüber informiert sein, dass Kontrollen durchgeführt werden, ggf. auch unangekündigt.
- Für Routinekontrollen SOLLTEN automatisierte Verfahren (z. B. watch dogs) verwendet werden.
- Personal- bzw. Betriebsräte SOLLTEN bei der Erarbeitung des Protokollierungskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.

4.1.14 Schulungen zu Sicherheitsmaßnahmen

Wie sich an vielen konkreten Beispielen wie den Schadensstatistiken von Elektronik-Versicherern belegen lässt, resultieren Schäden oft schlicht aus der Unkenntnis elementarer Sicherheitsmaßnahmen. Um dies zu verhindern, ist jeder einzelne Mitarbeiter zum sorgfältigen Umgang mit geschäftsrelevanten Informationen und der IT zu schulen und zu motivieren. Nur durch die Vermittlung der notwendigen Kenntnisse kann ein Verständnis für die erforderlichen Maßnahmen zur Informationssicherheit geweckt werden.
Im Folgenden werden die Kernthemen, die bei einer Schulung zu Sicherheitsmaßnahmen vermittelt werden SOLLTEN, vorgestellt.

Sensibilisierung für Informationssicherheit Jeder Mitarbeiter ist auf die Bedeutung der Sicherheitsbelange hinzuweisen. Ein geeigneter Einstieg in die Sensibilisierung ist beispielsweise, die Abhängigkeit der Behörde bzw. des Unternehmens und damit der Arbeitsplätze vom reibungslosen Funktionieren der Geschäftsprozesse aufzu-

zeigen. Darüber hinaus ist der Wert von Informationen unter den Gesichtspunkten Vertraulichkeit, Integrität und Verfügbarkeit herauszuarbeiten. Diese Sensibilisierungsmaßnahmen sind in regelmäßigen Zeitabständen zu wiederholen.

Mitarbeiterbezogene Informationssicherheitsmaßnahmen Zu diesem Thema sollen die Sicherheitsmaßnahmen vermittelt werden, die in einem Informationssicherheitskonzept erarbeitet wurden und von den einzelnen Mitarbeitern umzusetzen sind. Je nach Geschäftsprozess oder Fachaufgabe kann es andere Werte geben, die zu schützen sind oder einen anderen Schutzbedarf haben. Den Mitarbeitern SOLLTE vermittelt werden, welche Bedeutung Informationen oder andere Objekte für die Institution haben und was sie beim Umgang mit diesen beachten SOLLTEN. Dieser Teil der Schulungsmaßnahmen hat eine große Bedeutung, da viele Sicherheitsmaßnahmen erst nach einer entsprechenden Schulung und Motivation effektiv umgesetzt werden können.

Produktbezogene Sicherheitsmaßnahmen Zu diesem Thema sollen die Sicherheitsmaßnahmen vermittelt werden, die inhärent mit einem Produkt wie beispielsweise einem IT-System verbunden sind und häufig bereits im Lieferumfang enthalten sind. Dies können neben Passwörtern zur Anmeldung auch Möglichkeiten zur Verschlüsselung von Dokumenten oder Datenfeldern sein. So können beispielsweise Hinweise und Empfehlungen über die Strukturierung und Organisation von Dateien den Aufwand zur Datensicherung deutlich reduzieren.

Authentifizierung Mitarbeiter SOLLTEN mit den vorhandenen Authentikationsmechanismen und den hierfür genutzten Authentikationsmitteln (z.B. Passwörtern oder Token) korrekt umgehen können. Beispielsweise sollen die Bedeutung von Passwörtern für die Informationssicherheit sowie die Randbedingungen erläutert werden, die einen wirksamen Einsatz eines Passwortes erst ermöglichen.

Bedeutung der Datensicherung und deren Durchführung Die regelmäßige Datensicherung ist eine der wichtigsten Sicherheitsmaßnahmen in jedem Informationsverbund. Vermittelt werden soll das Datensicherungskonzept der Behörde bzw. des Unternehmens und die von jedem einzelnen durchzuführenden Datensicherungsaufgaben. Besonders wichtig ist dies für solche Bereiche, in denen Benutzer selbst die Datensicherungen durchführen MÜSSEN.

Umgang mit personenbezogenen Daten An den Umgang mit personenbezogenen Daten sind besondere Anforderungen zu stellen. Mitarbeiter, die mit personenbezogenen Daten arbeiten, sind für die gesetzlich erforderlichen Sicherheitsmaßnahmen zu schulen. Dies betrifft beispielsweise den Umgang mit Auskunftsersuchen, Änderungs- und Verbesserungswünschen der Betroffenen, gesetzlich vorgeschriebene Fristen zur Datenlöschung, Schutz der Vertraulichkeit und die Übermittlung der Daten.

Einweisung in Notfallmaßnahmen Sämtliche Mitarbeiter sind in bestehende Notfallmaßnahmen einzuweisen. Dazu gehört die Erläuterung der Fluchtwege, die Verhaltensweisen bei Feuer oder anderen Notfällen, der Umgang mit Feuerlöschern und das Notfall-Meldesystem (wer als erstes wie zu benachrichtigen ist).

Vorbeugung gegen Social Engineering Die Mitarbeiter sollen auf die Gefahren des Social Engineering hingewiesen werden. Die typischen Muster solcher Versuche, über gezieltes Aushorchen an vertrauliche Informationen zu gelangen, ebenso wie die Methoden, sich dagegen zu schützen, SOLLTEN erläutert werden. Da Social Engineering oft mit der Vorspiegelung einer falschen Identität einhergeht, SOLLTEN Mitarbeiter regelmäßig darauf hingewiesen werden, die Identität von Gesprächspartnern zu überprüfen und insbesondere am Telefon keine vertraulichen Informationen weiterzugeben.

Bei Auftreten von Schadsoftware ist besonderes Verhalten notwendig. Hier soll den Mitarbeitern vermittelt werden, wie mit Computer-Viren oder anderer Schadsoftware umzugehen ist. Mögliche Inhalte dieser Schulung sind:

- Erkennen einer Schadsoftware-Infektion.

- Wirkungsweise und Arten von Schadsoftware.
- Sofortmaßnahmen im Verdachtsfall.
- Maßnahmen zur Eliminierung von Schadsoftware.
- Vorbeugende Maßnahmen.

Bei der Durchführung von Schulungen SOLLTE immer beachtet werden, dass es nicht reicht, einen Mitarbeiter einmal während seines gesamten Arbeitsverhältnisses zu schulen. Für nahezu alle Formen von Schulungen - insbesondere Front-Desk-Schulungen - gilt, dass sehr viele neue Informationen auf die Teilnehmer einstürzen. Diese gelangen nur zu einem kleinen Teil ins Langzeitgedächtnis, 80% des vermittelten Wissens sind meist schon bei Schulungsende wieder vergessen. Daher SOLLTEN Mitarbeiter immer wieder zu Themen rund um die Informationssicherheit geschult bzw. sensibilisiert werden. Dies kann beispielsweise

- in kürzeren Veranstaltungen zu aktuellen Sicherheitsthemen,
- im Rahmen regelmäßiger Veranstaltungen wie Abteilungsbesprechungen oder
- durch interaktive Schulungsprogramme, die allen Mitarbeitern zur Verfügung stehen, erfolgen.

4.1.15 Konfigurationsänderungen

Die Durchführung von Änderungen an einem IT-System im Echtbetrieb ist immer als kritisch einzustufen und entsprechend sorgfältig MUSS hierbei vorgegangen werden. Bevor mit Änderungen am System begonnen wird, MUSS als erstes die alte Konfiguration gesichert werden, sodass sie schnell verfügbar ist, wenn Probleme mit der neuen Konfiguration auftreten. Bei vernetzten IT-Systemen MÜSSEN die Benutzer rechtzeitig über die Durchführung von Wartungsarbeiten in geeigneter Weise, wie z.B. durch einen Eintrag im Intranet oder per E-Mail, informiert werden, damit sie zum einen ihre Planung auf eine zeitweise Systemabschaltung einrichten können, und zum anderen nach Änderungen auftretende Probleme richtig zuordnen können. Die Konfigurationsänderungen SOLLTEN immer nur schrittweise durchgeführt werden. Zwischendurch SOLLTE immer wieder überprüft werden, ob die Änderungen korrekt durchgeführt wurden und das IT-System sowie die betroffenen Applikationen noch lauffähig sind.
Bei Änderungen an Systemdateien ist anschließend ein Neustart durchzuführen, um zu überprüfen, ob sich das IT-System korrekt starten lässt. Für Problemfälle sind alle für einen Notstart benötigten Datenträger vorrätig zu halten, z.B. Boot-Medien, Start-CD-ROM.
Vor Konfigurationsänderungen SOLLTEN von allen eventuell betroffenen Dateien und Verzeichnissen Datensicherungen angefertigt werden. Komplexere Konfigurationsänderungen SOLLTEN möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen SOLLTEN nach dem Vier-Augen-Prinzip überprüft werden, bevor sie in den Echtbetrieb übernommen werden.
Vor Konfigurationsänderungen SOLLTEN von allen eventuell betroffenen Dateien und Verzeichnissen Datensicherungen angefertigt werden. Komplexere Konfigurationsänderungen SOLLTEN möglichst nicht in den Originaldateien vorgenommen werden, sondern in Kopien. Alle durchgeführten Änderungen SOLLTEN nach dem Vier-Augen-Prinzip überprüft werden, bevor sie in den Echtbetrieb übernommen werden

4.1.16 Protokollierung sicherheitsrelevanter Ereignisse

Sicherheitsrelevante Ereignisse (zum Beispiel Zugriffe auf Ressourcen, Authentisierungsversuche) MÜSSEN nachvollziehbar protokolliert werden, damit im Stör- oder Fehlerfall oder nach Angriffsversuchen die Protokolldaten zur Ursachenfindung herangezogen

werden können. Neben den Maßnahmen in Kapitel 4.1.11 unter Berücksichtigung der Datenschutzaspekte in Kapitel 4.1.10, SOLLTEN zusätzlich die folgenden Punkte bei der Protokollierung sicherheitsrelevanter Ereignisse von Web-Anwendungen und Web-Services beachtet werden.
Zusätzlich zur Protokollierung auf den Server- und Hintergrundsystemen (zum Beispiel Betriebssystem, Web- und Applikationsserver, Datenbank) SOLLTE auch die Anwendung sicherheitsrelevante Ereignisse protokolliert werden. Mindestens folgende Ereignisse SOLLTEN auf Anwendungsebene erfasst werden.

- Erfolgreiche und erfolglose Anmeldeversuche an der Webanwendung oder dem Web-Service.
- Fehlgeschlagene Autorisierungsversuche beim Zugriff auf Ressourcen (zum Beispiel Datenbankzugriffe) und Funktionen der Webanwendung oder des Web-Service.
- Fehlgeschlagene Validierung von Ein- und Ausgabedaten.
- Fehlgeschlagene XML-Schema-Validierungen.
- Serialisierungs- und Deserialiserungs- Fehler (z.B. beim Parsen von XML-Dokumenten).
- Aufgetretene Fehler (z.B. Exceptions).
- Änderungen von Berechtigungen für Benutzer oder Benutzergruppen der Webanwendung oder des Web-Service (zum Beispiel Zugriffsrechte, Änderung an der Web-Service-Policy).
- Änderungen an Benutzerkonten (zum Beispiel Passwortänderung).
- Löschvorgänge der Webanwendung (zum Beispiel Beiträge).
- Erkannte Manipulationsversuche und unerwartete Änderungen (z.B. Anmeldeversuche mit ungültigen oder abgelaufenen Session-IDs),
- Administrative Funktionsaufrufe und Änderungen an der Konfiguration (zum Beispiel Abruf von Benutzerdaten, Aktivierung und Deaktivierung der Protokollierung).
- Starten und Stoppen von Diensten.
- Produktionsübernahme (Deployment) neuer oder bestehender Web-Services.

Um sicherheitsrelevante Vorgänge anhand von Protokolldaten nachvollziehen zu können, MÜSSEN grundlegende Merkmale der Ereignisse verfügbar sein. Daher SOLLTEN mindestens die folgenden Merkmale protokolliert werden.

- Datum und Uhrzeit mit Zeitzone,
- Assoziierter Benutzername,
- Betroffenes Objekt (z.B. Benutzerkonto, Datei, Datenquelle),
- Status der Aktion (z.B. fehlgeschlagen, erfolgreich),
- Ort des Auftretens (z.B. Beispiel Komponente),
- Aktion (z.B. Authentisierung, Autorisierung),
- Schweregrad (z.B. Information, Warnung, Fehler).

Darüber hinaus kann es hilfreich sein, die folgenden Merkmale zu protokollieren.

- Source-IP-Adresse.
- Referenzen auf die SessionID (nicht die SessionID selbst).
- IT-System, an dem der Fehler aufgetreten ist.
- Softwarestand (Version) der Webanwendung.

Vertrauliche und sicherheitsrelevante Daten (z.B. SessionID, Zugangsdaten) SOLLTEN nicht protokolliert werden.
Die protokollierten Daten SOLLTEN in einem einheitlichen Format gespeichert werden, damit eine effiziente Auswertung möglich ist. Die Protokollierungskomponente der Webanwendung oder des Web-Service SOLLTE aus diesem Grund ein Datenformat verwenden, das in bestehende Lösungen integriert werden kann. Wird beispielsweise eine

zentrale Komponente für die Auswertung der Protokolldaten verwendet, so SOLLTEN Datenformate gewählt werden, die diese Komponente unterstützt.
Die Protokollierung der Webanwendung oder des Web-Service ist ausschließlich serverseitig durchzuführen, da nur auf diese Weise die Protokolldaten zentral ausgewertet werden können. Die Protokolldaten SOLLTEN von einer einzigen, zentralen Protokollierungskomponente der Webanwendung oder des Web-Service und nicht von unterschiedlichen Protokollierungskomponenten erhoben werden. Eine fehleranfällige Neuentwicklung der Protokollierungskomponente SOLLTE vermieden werden. Stattdessen SOLLTE auf die Funktionalität etablierter Frameworks zurückgegriffen werden, die in der Regel einen zentralisierten Protokollierungsansatz und die Protokollierung in verbreiteten Protokolldatenformaten unterstützen.
Da die Protokolldaten vertrauliche Informationen (zum Beispiel über das Benutzerverhalten und den Aufbau beziehungsweise die Konfiguration der Webanwendung oder des Web-Service) enthalten können, MUSS der Zugriff auf die Protokolldaten reglementiert und nur befugten Benutzern ermöglicht werden. Der Zugriff auf Protokolldaten SOLLTE NICHT über öffentliche Schnittstellen möglich sein. Protokolldaten SOLLTEN daher in dedizierten Logverzeichnissen (zum Beispiel außerhalb des Web-Root-Verzeichnisses des Web-Servers) gespeichert werden. Werden die Protokolldaten in einer Datenbank abgelegt, so SOLLTEN die Protokolldaten von den eigentlichen Nutzdaten getrennt werden.
Diese Trennung kann mittels einer separaten Datenbanktabelle erreicht werden. Darüber hinaus kann ein eigener Datenbankbenutzer für die Protokollierung den Schutz der Protokolldaten erhöhen. In diesem Fall DARF der Datenbankbenutzer für die Nutzdaten keine Zugriffsrechte auf die Protokolldaten haben. Alternativ können die Protokollierungsdaten mit hohem Schutzbedarf auch in einer separaten Datenbankinstanz gespeichert werden.
Ein Angreifer kann bewusst Protokoll-Einträge provozieren (zum Beispiel wenn Eingabefelder protokolliert werden), die einen schadhaften Programmcode beinhalten. Daher SOLLTE bei der Auswertung der Protokolldaten sichergestellt werden, dass Schadcode in Protokoll-Einträgen vom Auswertungsprogramm nicht interpretiert wird (zum Beispiel durch die Ansicht in einem Browser und der Interpretation von JavaScript-Code in den Protokolldaten). Da bei der Protokollauswertung keine Änderungen an den Protokolldaten vorgenommen werden DÜRFEN, sind die Protokolldaten ausschließlich in einem schreibgeschützten Modus zu analysieren.
Die Protokolldaten verschiedener Komponenten einer Webanwendung oder eines Web-Service (zum Beispiel Applikationsserver, Webserver, Datenbankserver) MÜSSEN in der Regel korreliert werden, um komponentenübergreifende Vorgänge vollständig nachvollziehen zu können. Dazu SOLLTE die Zeit auf den Systemen synchronisiert sein, um anhand der Uhrzeiten Vorgänge in den Protokollen konsistent nachverfolgen zu können. Hierzu SOLLTE der Einsatz eines lokalen NTP-Servers [21] zur Zeitsynchronisation in Betracht gezogen werden.

4.2 Durchführung von Penetrationstests

Penetrationstests sind erprobte und geeignete Vorgehen, um die aktuelle Sicherheit von IT-Systemen und IT-Anwendungen festzustellen. Das BSI setzt hierbei zwei Testmethoden ein, IS-Penetrationstests [22] sowie IS-Webchecks [23]. Der IS-Penetrationstest ist die Vorgehensweise zur Untersuchung des aktuellen Sicherheitsniveaus von IT-Systemen und Netzen. Mittels eines IS-Webchecks wird das aktuelle Sicherheitsniveau des Internetauftritts beziehungsweise von Web-Services einer Institution ermittelt.
Penetrationstests dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund, eines einzelnen IT-Systems oder einer Internetpräsenz abzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten bezie-

hungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen. Für sicherheitskritische Netze und Systeme SOLLTEN regelmäßig Penetrationstests erfolgen. Im Detail werden dabei die installierten Anwendungen (Webanwendung, Mailserver, Web-Service) beziehungsweise die zugrunde liegenden Trägersysteme (Betriebssystem, Datenbank etc.) überprüft. Im Folgenden sind typische Ansatzpunkte für einen Penetrationstest aufgelistet.

- Netzkoppelelemente (Router, Switches, Gateways).
- Sicherheitsgateway (Paketfilter, Intrusion Detection System, Virenscanner).
- Server (Datenbankserver, Webserver, Fileserver, Speichersysteme).
- Telekommunikationsanlagen.
- Webanwendungen (z.B. Internetauftritt, Vorgangsbearbeitung, Webshop).
- Web-Services (z.B. REST-API, SOAP-API, SOA).
- Clients.
- Drahtlose Netze (zum Beispiel WLAN, Bluetooth).
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen).

Üblicherweise werden Penetrationstests in Blackbox-Tests und Whitebox-Tests unterteilt. Bei einem Blackbox-Test stehen dabei den Penetrationstestern lediglich die Adressinformationen des Zieles zur Verfügung, weitere Informationen werden ihnen nicht mitgeteilt. Mittels der Vorgehensweise Blackbox-Test soll damit der Angriff eines typischen Außentäters mit unvollständigen Kenntnissen über das Zielsystem simuliert werden. Dagegen verfügen die Penetrationstester bei einem Whitebox-Test über umfangreiche, für sie notwendige Informationen über die zu testenden Systeme. Dazu gehören beispielsweise Informationen über IP-Adressen, das interne Netz und die eingesetzte Soft- und Hardware. Diese Angaben werden ihnen zuvor vom Auftraggeber mitgeteilt.
Es ist jedoch fraglich, ob die Unterscheidung zwischen den Vorgehensweisen “Blackbox-Test” und “Whitebox-Test” heute noch sinnvoll ist. Beispielsweise besteht bei einem Blackbox-Test aufgrund nicht vorliegender Informationen ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden zu verursachen. Weiterhin könnten beispielsweise Schwachstellen aufgrund nicht mitgeteilter Informationen übersehen werden.
Zudem besteht die Gefahr, dass im Rahmen eines Blackbox-Tests der Angriff eines informierten Innentäters nicht berücksichtigt wird. Den Penetrationstestern SOLLTEN daher heutzutage alle für die Testdurchführung notwendigen Informationen über die zu testenden Systeme zur Verfügung gestellt werden, um eventuell mit dem Test verbundene Risiken minimieren zu können und eine möglichst vollständige Schwachstellensuche zu ermöglichen. Die Klassifizierung von Penetrationstests in eine weitestgehend automatisierte Schwachstellensuche (“Vulnerability Scan”) sowie eine in großen Teilen manuelle Sicherheitsrevision erscheint daher nach heutigem Kenntnisstand praxisnäher und erfolgsorientierter.
Im Rahmen dieser Ausarbeitung wurde eine Sicherheitsuntersuchung einer öffentlich zugänglichen Webanwendung der ENERTRAG durchgeführt. Die Untersuchung ist im Anhang A zu finden.

4.2.1
Anforderungen an einen Dienstleister

Penetrationstests sind anspruchsvolle und diffizile Aufgaben, die auch Auswirkungen auf den IT-Betrieb haben können. Daher SOLLTE hierfür nur hinreichend qualifiziertes und zuverlässiges Personal mit themenübergreifenden Kenntnissen auf folgenden Gebieten eingesetzt werden.

- Administration von Betriebssystemen und Anwendungen
- Netzwerkprotokolle und Auswertung von Netzwerkverkehr

- Sicherheitsprodukte (zum Beispiel Sicherheitsgateways, Intrusion Detection Systeme)
- Programmiersprachen
- Schwachstellenscanner
- Audit- und Administrationssoftware

Werden externe Dienstleister mit der Durchführung von Penetrationstests beauftragt, so SOLLTE darauf geachtet werden, dass ein qualifizierter und vertrauenswürdiger Dienstleister ausgewählt wird, der entsprechend qualifizierte und zuverlässige Mitarbeiter bereitstellen kann. Weiterhin SOLLTEN Anbieter von Penetrationstests dem Auftraggeber eine strukturierte Methodik zu deren Durchführung vorstellen können, auf deren Basis die jeweilige individuelle Vorgehensweise ausgearbeitet werden kann.

4.2.2 Strukturierung und Vorgehensweise

In einer Vorbereitungsphase MÜSSEN zunächst zwischen dem Auftraggeber und dem Auftragnehmer die Ziele sowie der Umfang des Penetrationstests so genau wie möglich festgelegt werden. Der Penetrationstester SOLLTE hierbei dem Auftraggeber eine strukturierte Vorgehensweise, welche zwischen den Parteien abzustimmen ist, vorstellen. Während des Abstimmungsprozesses SOLLTE beachtet werden, dass unter Umständen Dritte über den geplanten Penetrationstest informiert beziehungsweise daran beteiligt werden MÜSSEN.
In der Regel MÜSSEN beispielsweise die Personalvertretung und der Datenschutzbeauftragte, häufig auch Externe, wie der Internet Service Provider oder der Webhoster, in das Vorhaben einbezogen werden. Zwischen dem Auftraggeber und dem Dienstleister SOLLTEN bestimmte Voraussetzungen bereits im Vorfeld vereinbart werden. Hierzu zählen insbesondere die folgenden Aspekte.

- Vereinbarungen über die Verschwiegenheitspflichten.
- Vereinbarungen über den Einsatz von Hard- und Software.
- Vereinbarungen über die zu testenden IT-Systeme und IT-Anwendungen.
- Festlegung von erlaubten und unerlaubten Aktivitäten der Penetrationstester, um Schäden möglichst zu vermeiden.
- Vereinbarungen über den Umgang mit Datenträgern vor, während und nach Abschluss des Penetrationstests, da die Datenträger zum Beispiel sensible Informationen über die Testergebnisse enthalten können.
- Festlegungen über den Ort der Durchführung sowie zur Auswertung und Berichterstellung für den Penetrationstest.
- Festlegung eines Terminplans einschließlich Wartungsfenster für die Durchführung der Tests.
- Detaillierte Vereinbarungen über den Zugang zum Internet beziehungsweise den Anschluss von Testsystemen an das Internet während der Durchführung und der Auswertung von Penetrationstests.
- Vereinbarungen über Zuständigkeiten und die Erreichbarkeit von Ansprechpartnern sowie zur Notfallvorsorge.

In der sich anschließenden Informationsphase sammeln die Penetrationstester möglichst viele Informationen über das zu testende Objekt. Zur Vorbereitung der Tests werden die gewonnenen Informationen anschließend hinsichtlich potenzieller Schwachstellen ausgewertet. In der eigentlichen Testphase eines Penetrationstests SOLLTEN nach Möglichkeit die Testverfahren vermieden werden, welche ein destruktives Ergebnis für die untersuchten IT-Systeme oder IT-Anwendungen zur Folge haben könnten.
So zielen beispielsweise DoS-Angriffe darauf ab, den Zugriff auf einzelne Dienste, Systeme oder Netzsegmente zu unterbinden. Die Feststellung, ob derartige Attacken möglich

sind, kann jedoch oftmals im Vorfeld durch eine Systemanalyse geklärt werden, sodass solche Angriffe während eines Penetrationstests überflüssig werden.
Sollen dennoch dos-Angriffe oder ähnliche destruktive Angriffe im Rahmen eines Penetrationstests durchgeführt werden, SOLLTE dies außerhalb der produktiven Nutzungszeiten des Systems erfolgen. Gegebenenfalls kann ein derartiger Angriff auch anhand eines Testsystems simuliert werden. Diese Vorgehensweisen SOLLTEN ausdrücklich vereinbart werden.
Erst danach werden aktive Eindringungsversuche unternommen. Dabei MÜSSEN die vereinbarten Wartungsfenster und der Terminplan strikt eingehalten werden. Wenn Änderungen am zeitlichen Ablauf erforderlich sind, MUSS dies auf jeden Fall mit dem Auftraggeber abgestimmt werden. Anderenfalls besteht die erhöhte Gefahr, dass auf der Seite des Auftraggebers bestimmte Aktivitäten der Penetrationstester mit echten Angriffen verwechselt werden. Empfehlenswert ist die vollständige Aufzeichnung und Dokumentation des Penetrationstests.
Um möglichst aussagekräftige Ergebnisse zu erhalten, SOLLTE darauf geachtet werden, dass die Penetrationstests unmittelbar an dem zu testenden IT-System sowie unter Umgehung von vorgeschalteten Komponenten wie zum Beispiel Paketfilter, Web Application Firewall durchgeführt werden. Liegen besondere Gründe vor, den Test mit aktiven vorgeschalteten Sicherheitskomponenten durchzuführen, so ist zu beachten, dass dabei eventuelle Sicherheitsprobleme in der Anwendung selbst unentdeckt bleiben, weil die vorgelagerten Komponenten die Angriffsversuche im Penetrationstest abfangen. Solche unentdeckten Schwachstellen bilden jedoch ein relevantes Risiko, denn häufig können mit einem abgewandelten Angriff die Schutzsysteme ausgehebelt und die Schwachstellen ausgenutzt werden.

4.2.3 Typische Angriffstechniken

Eine typische Methode, um aktive Dienste in einem Netzwerk zu identifizieren, sind Netzwerk- und Portscanns. Dabei werden i.d.R. bestimmte Portbereiche abgefragt, um zu erfahren, unter welchen Ports Dienste erreichbar sind. Seitens der IT-Administration werden solche Abfragen dazu genutzt, um den aktuellen Status der eingesetzten IT-Systeme abzufragen. Allerdings kann ein Angreifer unter Umständen mit Hilfe dieser Informationen vorhandene Schwachstellen auf den einzelnen IT-Systemen identifizieren und basierend auf diesen Informationen, einen Angriff durchführen.
Eine weitere Schwachstelle kann eine mangelhafte Eingabeüberprüfung von Benutzereingaben in ein IT-System sein. Als Eingabeüberprüfung wird das Verfahren bezeichnet, mit dem die Benutzereingaben, die einer Anwendung zur weiteren Bearbeitung übergeben werden, vorher gefiltert, bereinigt oder zurückgewiesen werden. Diese Filterung soll verhindern, dass ein der Anwendung schädlicher Code übergeben werden kann, dessen Verarbeitung zu einem Fehlverhalten führt wie zum Beispiel der Offenlegung vertraulicher Informationen.
Angriffsmethoden, mit denen ein derartiges Fehlverhalten hervorgerufen werden kann, sind zum Beispiel ”Cross-Site Scripting” [24], “Cross-Site Request Forgery” [25], ”SQL-Injection” [26], “OS Injection” [27], “Fuzzing” [28] sowie im Bereich von Web-Services “XML External Entity-Angriffe” [29] oder sogenannte “XML-Bomben” [30]. Wie im Kapitel 2 beschrieben liefert die OWASP Top-Ten[6] eine gute Übersicht der bekanntesten Angriffsmöglichkeiten im Web-Umfeld.
Teilweise lassen sich auch Schwachstellen der verwendeten Protokolle und sonstigen Techniken ausnutzen, um Schaden zu bewirken. Zum Beispiel mittels Angriffen auf veraltete SSL/TLS-Versionen oder etwa durch “XML Signature Wrapping” [31] bei Web-Services.

[6] https://owasp.org/www-project-top-ten/

Eine weitere Kategorie von Angriffen auf Web-Dienste sind Denial-of-Service-Angriffe (DoS). Diese Angriffe zielen darauf ab, einen oder mehrere der zur Verfügung gestellten Dienste außer Betrieb zu setzen. Dies kann unter anderem mittels einer durch vermehrte Anfragen gesteigerten Last, durch ein massiv erhöhtes Datenaufkommen (zum Beispiel E-Mails), aber auch durch gezieltes Ausnutzen möglicher Softwarefehler durchgeführt werden. Ein bekanntes Beispiel für einen DoS-Angriff ist der “Ping of Death” [32].
Als “Information Gathering” [7] wird die Sammlung aller Informationen bezeichnet, welche im weiteren für einen Angriff nützlich sein könnten. Beispiele für solche Informationen sind etwa das verwendete Nummerierungsschema für Verzeichnisse oder Server oder Erkenntnisse über Web-Service-Schnittstellen, die durch WSDL-Scanning gewonnen werden.
Als “Social Engineering” [33] werden beispielsweise fingierte Anrufe oder sonstige Kontaktaufnahmen mit Personen bezeichnet, die das betrachtete IT-System bedienen. Das Ziel ist meist, dadurch vertrauliche Informationen wie zum Beispiel Passwörter zu erhalten.
Unter “War Dialing” [34] wird der automatisierte und systematische Versuch verstanden, Telefonnummern, die in Verbindung mit einem Modem stehen, auszuforschen. Dabei werden die Telefonnummern des Zielsystems angerufen und auf ein antwortendes Modem hin überprüft.
Bei Passwort-Attacken [35] wird die Sicherheit beziehungsweise Stärke von Passwörtern mittels sogenannter Wörterbuchangriffe, Brute-Force-Attacken oder durch Entschlüsselungsversuche getestet.
Eine weitere beliebte Angriffsmethode ist das Ausnutzen von Software-Schwachstellen [36]. Bei diesen Angriffen wird beispielsweise getestet, ob die installierte Software anfällig für bestimmte Exploits ist, fehlerhaft konfiguriert ist, Schwachstellen aufweist oder veraltet ist. Häufig wird auch untersucht, ob etwa bekannte Schwachstellen der Standardinstallation des jeweiligen Produkts im vorliegenden Fall ausgenutzt werden können.
Unter Kryptografischen Angriffen [37] versteht man Angriffe auf den verwendeten Verschlüsselungsmechanismus bzw. des Verschlüsselungsprotokolls sowie der Schlüsselverwaltung.
Im Rahmen von Infrastruktur-Untersuchungen werden unter anderem bauliche Sicherungsmaßnahmen, Zutritts- und Schließeinrichtungen, aber auch die Entsorgung von Material durchleuchtet. Eine Variante hiervon ist das sogenannte “Dumpster Diving” [38], also das Suchen nützlicher Unterlagen oder Datenträger im Abfall (zum Beispiel Papierkörbe, Abfallcontainer).
In der Auswertungs- und Berichtsphase werden die Ergebnisse gesammelt, ausgewertet und in Form eines Berichts zusammengestellt. Alle während des Penetrationstests gewonnenen Informationen sind hierbei entsprechend gesichert aufzubewahren. Der Auftraggeber SOLLTE den Auftragnehmer im Vorfeld dazu verpflichten, alle Aufzeichnungen über den Penetrationstest vollumfänglich an den Auftraggeber zu übergeben beziehungsweise zu vernichten.
Der Bericht MUSS neben einer Auflistung der gefundenen Schwachstellen auch Maßnahmenempfehlungen enthalten, wie mit den entdeckten Schwachstellen umgegangen werden SOLLTE. Empfehlenswert ist hierbei zudem die Erstellung eines Umsetzungsplans für die in dem Bericht aufgeführten Maßnahmenempfehlungen einschließlich einer Priorisierung. Für das Management SOLLTE der Abschlussbericht außerdem eine Zusammenfassung enthalten, in der die wesentlichen Prüfungsergebnisse und ein Überblick über die empfohlene weitere Vorgehensweise dargestellt sind. Der Abschlussbericht MUSS dem IT-Sicherheitsbeauftragten und den verantwortlichen Führungskräften vorgelegt werden.

[7] https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/

Begleitend zu allen Phasen eines Penetrationstests ist eine gemeinsame Dokumentation der einzelnen Vereinbarungen und Ergebnisse durch den Auftraggeber und den Auftragnehmer empfehlenswert.

4.3 Web-Services

Die Anforderungen an einen Web-Service, wie er als APP-02 in der Referenzarchitektur 4 modelliert ist, sind der Web-Anwendung sehr ähnlich und überschneiden sich z.T. mit den Empfehlungen aus Kapitel 4.1. Soweit nicht anders beschrieben, gelten die bereits erläuterten Empfehlungen.

- Einspielen sicherheitsrelevanter Patches: Kapitel 4.1.1.
- Rechtemanagement: Kapitel 4.1.6.
- Dokumentation der Benutzer- und Rechteprofile: Kapitel 4.1.7.
- Dokumentation der Veränderungen eines bestehenden Systems: Kapitel 4.1.8.
- Identifikation von Sicherheitslücken: Kapitel 4.1.9.
- Datenschutzaspekte bei der Protokollierung: Kapitel 4.1.10.
- Schulungen zu Sicherheitsmaßnahmen: Kapitel 4.1.14.
- Konfigurationsänderungen: Kapitel 4.1.15.
- Protokollierung sicherheitsrelevanter Ereignisse: Kapitel 4.1.16.
- Durchführung von Penetrationstests: Kapitel 4.2.

4.3.1 Überwachung

Um den Sicherheitszustand eines Web-Service nachvollziehen zu können, ist es notwendig, diesen kontinuierlich zu überwachen. Ziel einer solchen Überwachung ist es, Verstöße gegen die geltenden Sicherheitsvorschriften zu entdecken, bestehende Sicherheitslücken aufzudecken oder Fehlkonfigurationen, die zu Sicherheitslücken führen können, zu erkennen.
Als Bestandteil des Sicherheitskonzeptes für einen Web-Service MUSS deshalb ein Überwachungskonzept entwickelt werden. Komplexe Systeme wie Web-Services können in der Regel nicht mehr durch einzelne Administratoren überwacht werden, sondern die Kontrolle MUSS automatisch durch entsprechende Systemkomponenten oder Produkte erfolgen. Die Überwachung eines Web-Service MUSS bei Veränderungen entsprechend angepasst werden.
Des Weiteren MÜSSEN in der Planung zur Überwachung eines Web-Service grundsätzlich alle relevanten Komponenten berücksichtigt werden. Daher SOLLTEN im Überwachungskonzept beispielsweise auch Datenbanken und Verzeichnisdienste, abhängige und genutzte Web-Services sowie die relevanten IT-Systeme enthalten sein. Dies ist von besonderer Bedeutung, wenn unterschiedliche Services über einen Enterprise Service Bus (ESB) miteinander verbunden sind.
Wenn Dienste ausfallen, ihre Schnittstellen ändern oder ihr Antwortzeitverhalten verschlechtern, kann das weitreichende Folgen auf eine Vielzahl von abhängigen Systemen haben. Die Verfügbarkeit und Leistung von Web-Services MÜSSEN daher geeignet überwacht werden. Neben der generellen Erreichbarkeit und Aktivität des Web-Service sowie der relevanten Schnittstellen-Dienste und Abhängigkeiten SOLLTEN daher auch Leistungsparameter überwacht werden. Hierzu gehören beispielsweise die folgenden.

- Antwortzeiten von Anfragen.
- Anzahl der Anfragen beziehungsweise Anforderungen.
- Größe von Anforderungen und Antworten oder
- Füllstände von Speichern (zum Beispiel Speicher der JVM, Message-Queues).

Dadurch können zum einen Fehlkonfigurationen oder technisch bedingte Engpässe sowie zum anderen DoS-Angriffe frühzeitig erkannt und zeitnah behandelt werden. Insbesondere bei höheren Anforderungen an die Verfügbarkeit und bei der Verteilung eines Web-Service über mehrere Systeme SOLLTE die Lastverteilung überwacht werden.
Des Weiteren SOLLTEN die Protokolldateien und Systemmeldungen (Notifications) hinsichtlich relevanter Meldungen kontinuierlich ausgewertet werden. Hierzu SOLLTE ein am Schutzbedarf ausgerichtetes Log-Level im jeweiligen Web-Service konfiguriert werden (siehe Kapitel (4.1.16). Für die Überwachung können beispielsweise die folgenden Meldungen relevant sein.

- Fehler- oder Warnmeldungen.
- Meldungen zu Berechtigungsverstößen oder -änderungen (zum Beispiel Vergabe von Administratorberechtigungen).
- Meldungen zur Änderung von sicherheitsrelevanten Einstellungen.
- Meldungen zu ungültigen Nachrichten (z.B. invalides XML oder JSON-Format).
- Fehlermeldungen zu Inkompatibilität von Schnittstellen.

Meldungen mit einer höheren Kritikalität MÜSSEN zu einer Alarmierung eines verantwortlichen Mitarbeiters führen, um eine Reaktion in einem angemessenen Zeitraum sicherzustellen. Hierfür empfiehlt sich der Einsatz eines Alarmierungssystems.
In diesem Zusammenhang SOLLTEN auch die unterschiedlichen Meldungen zu Verstößen gegen die eingesetzten Policies (zum Beispiel WS-Policies, WSSecurityPolicies) berücksichtigt werden. Diese könnten beispielsweise Folgendes beinhalten.

- Verstöße gegen die vordefinierte Nachrichtengröße.
- Verstoß gegen die Verschlüsselungsanforderung an Nachrichten.
- Fehler in der Ver- oder Entschlüsselung von Nachrichteninhalten.
- Fehler in der Signatur von Nachrichteninhalten.
- Fehlerhafte Authentisierung.

Werden aufgrund höherer Vertraulichkeitsanforderungen Verschlüsselungsmaßnahmen eingesetzt (zum Beispiel TLS), SOLLTEN diese hinsichtlich ihrer Funktionalität überwacht werden. Gerade durch die automatisierte Funktion eines Web-Service besteht die Gefahr, dass Fehler in der Verschlüsselung nicht rechtzeitig bemerkt werden. Ansatzpunkte für eine Überwachung der Verschlüsselung sind beispielsweise die folgenden.

- Aktualität und Gültigkeit des Zertifikats des Web-Service.
- Aktualität und Gültigkeit der Zertifikate von anfragenden Diensten.
- Fehler- oder Warnmeldungen beim Aufbau von verschlüsselten Verbindungen (zum Beispiel Warnmeldungen bei veralteten SSL-Versionen)

Um Bedrohungen und Schwachstellen rechtzeitig erkennen zu können, ist es erforderlich, Schwellwerte zu definieren sowie Trends aus den überwachten Werten abzuleiten, zum Beispiel für den belegten Speicherplatz, die Systemauslastung oder die genutzte Bandbreite. Anhand der Schwellwerte und jeweils kritischen Trendrichtungen SOLLTEN im Rahmen des Überwachungskonzepts Handlungsanweisungen definiert werden.

4.4 Betrieb von Datenbanken

Die Anforderungen an den sicheren Betrieb einer Datenbank, wie in der Referenzarchitektur in Abbildung 4 als APP-03 beschrieben, überschneiden sich z.T mit den Empfehlungen aus Kapitel 4.3 sowie Kapitel 4.1. Soweit nicht anders beschrieben gelten die folgenden bereits erläuterten Empfehlungen.

- Dokumentation der Benutzer und Rechteprofile: Kapitel 4.1.7.
- Dokumentation der Veränderungen eines bestehenden Systems: Kapitel: 4.1.8.

4.4.1 Kontrolle der Wirksamkeit der Benutzer-Trennung am IT-System

Mittels Protokollauswertung oder durch Stichproben ist in angemessenen Zeitabständen zu überprüfen, ob die Benutzer von IT-Systemen sich regelmäßig nach Aufgabenerfüllung abmelden oder ob mehrere Benutzer unter einer Kennung arbeiten. Sollte festgestellt werden, dass tatsächlich mehrere Benutzer unter einer Kennung arbeiten, sind sie auf die Verpflichtung zum Abmelden nach Aufgabenerfüllung hinzuweisen. Gleichzeitig SOLLTE der Sinn dieser Maßnahme erläutert werden, die im Interesse des einzelnen Benutzers liegt. Stellt sich heraus, dass die An- und Abmeldevorgänge zu zeitintensiv sind und trotz Aufforderung nicht akzeptiert werden, SOLLTEN alternative Maßnahmen diskutiert werden wie zum Beispiel die folgenden.

- Das IT-System kann für bestimmte Zeitintervalle einem Benutzer zugeordnet werden, so dass in dieser Zeit andere Benutzer das IT-System nicht nutzen DÜRFEN. Dies setzt voraus, dass der Arbeitsprozess dementsprechend zeitlich variabel ist.
- Es können zusätzliche IT-Systeme angeschafft werden, mit denen die quasiparallele Arbeit an einem IT-System vermieden werden kann. Wenn diese Geräte weggeschlossen werden, wenn sie benutzt wurden, kann auch auf eine An- und Abmeldung für die Nutzungsintervalle verzichtet werden.
- Statt zeitaufwendigen mehrstufigen Authentisierungsverfahren könnten automatisierte Authentisierungsverfahren wie beispielsweise über RFID-basierte Token oder biometrische Verfahren eingesetzt werden.
- Wenn sich die Datenbestände der einzelnen Benutzer separieren lassen (beispielsweise Benutzer A bearbeitet die Daten A-L, Benutzer B die Daten M-Z), so SOLLTEN dafür unterschiedliche Zugriffsrechte eingeräumt werden.

4.4.2 Inferenzprävention

Zum Schutz personenbezogener und anderer vertraulicher Daten eines Datenbanksystems ist grundsätzlich jedem Benutzer nur der Zugriff auf diejenigen Daten zu gestatten, die für seine Tätigkeiten notwendig sind. Alle anderen Informationen, die sich zusätzlich in der Datenbank befinden, sind vor ihm zu verbergen. Zu diesem Zweck MÜSSEN die Zugriffsberechtigungen auf Tabellen bis hin zu deren Feldern definiert werden können. Dies kann mittels Verwendung von Views und Grants durchgeführt werden. Damit ist es einem Benutzer nur möglich, die für ihn bestimmten Daten einzusehen und zu verarbeiten. Stellt er Datenbankabfragen, die auf andere Informationen zugreifen wollen, werden diese vom DBMS zurückgewiesen.
Im Zusammenhang mit statistischen Datenbanken, die Daten über Personengruppen, Bevölkerungsschichten oder ähnliches enthalten, treten dagegen andere Schutzanforderungen auf. In einer statistischen Datenbank unterliegen die einzelnen, personenbezogenen Einträge dem Datenschutz, statistische Informationen sind jedoch allen Benutzern zugänglich. Hier gilt es zu verhindern, dass aus Kenntnissen über die Daten einer Gruppe auf die Daten eines individuellen Mitglieds dieser Gruppe geschlossen werden kann. Es MUSS außerdem verhindert werden, dass durch das Wissen der in der Datenbank gespeicherten Informationen bzw. der Ablagestrukturen der Daten in der Datenbank die Anonymität dieser Daten durch entsprechend formulierte Datenbankabfragen umgangen werden kann (z.B. wenn die Ergebnismenge einer Datenbankabfrage nur einen Datensatz beinhaltet). Diese Problematik wird Inferenzproblem, der Schutz vor solchen Techniken Inferenzprävention genannt.

Auch wenn die Daten einer statistischen Datenbank anonymisiert sind, kann durch Inferenztechniken der Personenbezug zu bestimmten Datensätzen wiederhergestellt werden. Eine Zurückweisung bestimmter Anfragen (z.B. Anfragen mit nur einem oder wenigen Ergebnistupeln) reicht im allgemeinen nicht aus, da auch die Verweigerung einer Antwort durch das DBMS Informationen beinhalten kann. Durch das Erstellen verschiedener Statistiken kann die Anonymität der Daten ebenfalls verloren gehen. Ein solcher indirekter Angriff zielt darauf ab, aus mehreren Statistiken Rückschlüsse auf die persönlichen Daten eines einzelnen Individuums ziehen zu können. Eine Schutzmaßnahme ist in diesem Fall, die Freigabe von so genannten sensitiven Statistiken nicht zu erlauben, was als unterdrückte Inferenzprävention bezeichnet wird. Eine weitere Möglichkeit ist die Verzerrung solcher Statistiken durch kontrolliertes Runden (gleiche Statistiken sind gleich zu runden) oder die Beschränkung auf statistisch relevante Teilmengen mit der Auflage, dass gleiche Anfragen immer Bezug auf die gleichen Teilmengen nehmen. Dieses Verfahren wird als verzerrende Inferenzprävention bezeichnet. Werden weitergehende Anforderungen an die Vertraulichkeit der Daten gestellt, ist deren Verschlüsselung erforderlich.

4.4.3 Zugangskontrolle einer Datenbank

Die Datenbank-Software MUSS über geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer verfügen, um eine wirkungsvolle Zugangskontrolle zu gewährleisten. Die Vergabe von Zugangsberechtigungen hat nach festgelegten Regeln zu erfolgen. Generell SOLLTE für normale Benutzer der Zugang zu einer Produktionsdatenbank über einen interaktiven SQL-Interpreter unterbunden werden. Auf solche Datenbanken SOLLTE ausschließlich ein indirekter Zugang über die entsprechenden Anwendungen möglich sein. Die einzige Ausnahme bilden hier Datenbankkennungen zu Administrationszwecken.
Remote-Zugänge zu Datenbanken SOLLTEN äußerst restriktiv gehandhabt werden. Ist diese Art des Zugangs nicht zwingend erforderlich, so sind diese zu unterbinden. Ansonsten SOLLTE nur denjenigen Benutzern ein Remote-Zugang ermöglicht werden, die diesen auch tatsächlich benötigen. Andere Benutzer DÜRFEN NICHT in der Lage sein, sich selbst einen Remote-Zugang zu verschaffen. Keinesfalls DARF ein Remote-Zugang ohne Angabe einer gültigen Benutzer- Kennung und Eingabe eines Passwortes möglich sein.
Bei erhöhten Sicherheitsanforderungen SOLLTE geprüft werden, ob eine starke Authentisierung, die über Benutzername und Passwort hinausgeht, erforderlich ist. Hier kommt beispielsweise der Einsatz von Chipkarten oder sogenannten Tokens in Frage.

4.4.4 Zugriffskontrolle einer Datenbank

Um einen wirkungsvollen Schutz der Vertraulichkeit und Integrität der Daten einer Datenbank zu erreichen, MÜSSEN eine Reihe von Maßnahmen umgesetzt werden. Neben einer Zugangskontrolle der Datenbank, die in Kapitel 4.4.3 beschrieben wird, sind dies im wesentlichen die folgenden Möglichkeiten der Zugriffskontrolle.
Es SOLLTE eine logische Zuordnung der Datenbankobjekte, also der Tabellen, Indizes, Datenbankprozeduren, etc. zu den Anwendungen erfolgen, die diese Objekte benutzen. Die daraus entstehenden Gruppen von Datenbankobjekten werden je Anwendung den eigens hierfür einzurichtenden Kennungen zugeordnet. Damit können die Zugriffsberechtigungen der Datenbankobjekte so eingestellt werden, dass nur über diese speziellen Kennungen eine Modifikation der Objekte stattfinden kann. Greifen mehrere Anwendungen auf dieselben Datenbankobjekte zu, SOLLTEN diese als eigene Gruppe isoliert werden.

Werden beispielsweise die Daten zweier Anwendungen A und B in der Datenbank verwaltet, so sind zwei Datenbankkennungen ”AnwA” und “AnwB” anzulegen. Alle Datenbankobjekte, die eindeutig der Anwendung A zugeordnet werden können, werden mit der Datenbankkennung “AnwA” angelegt und verwaltet. Analog wird mit den Datenbankobjekten von Anwendung B verfahren. Ein Beispiel für ein zentrales Datenbankobjekt, das von beiden Anwendungen benutzt wird, wäre eine Tabelle, die alle ansteuerbaren Drucker beinhaltet. Datenbankobjekte dieser Kategorie SOLLTEN nicht einer Kennung der Anwendungen (“AnwA” oder “AnwB”) zugeordnet werden, stattdessen SOLLTEN solche Datenbankobjekte unter einer eigenen Kennung (z.B. Druck) zusammengefasst und mit dieser zentralen Kennung verwaltet werden.
Diese speziellen Kennungen sind nicht personenbezogen. Stattdessen erhalten eigens hierfür autorisierte Personen (z.B. der Datenbankadministrator oder der Administrator der zugehörigen Anwendung) das Passwort der benötigten Kennung, falls Modifikationen an den Datenbankobjekten vorgenommen werden MÜSSEN.
Durch eine Definition von Views und Prozeduren können spezielle Benutzer- Sichten auf die Daten erzeugt werden, so dass die Daten der Datenbank nach bestimmten Kriterien sichtbar gemacht bzw. unsichtbar gehalten werden. Über einen View oder eine Prozedur wird explizit festgelegt, welche Felder aus einer oder mehreren Tabellen einem Benutzer in welcher Reihenfolge angezeigt werden. Durch spezielle Bedingungen können hierbei die Daten gefiltert und durch spezifische Beschränkungen in ihrem Umfang begrenzt werden. Durch die restriktive Vergabe von Zugriffsrechten auf solche Views und Prozeduren können vertrauliche Daten vor unberechtigtem Zugriff geschützt werden.
Durch Trennung von Daten und Funktionalitäten, hier die Trennung der Views und Prozeduren von den echten Daten durch Speicherung in einer eigenständigen Datenbank, kann die Sicherheit zusätzlich erhöht werden. Der Benutzer oder die Anwendung greift ausschließlich auf die Views und Prozeduren in der ausgelagerten Datenbank zu. Erst diese Views und Prozeduren greifen auf die in der Datenbank abgelegten Daten zu. In der ausgelagerten Datenbank werden die Zugriffsrechte der Benutzer und Anwendungen zusammengefasst.
Hierbei können Zugriffsrechte (Grants) auf Tabellen, Views, etc. oder sogar auf einzelne Felder einer Tabelle vergeben werden. Diese Rechte sind immer an bestimmte Benutzer, Rollen oder Benutzergruppen gebunden. Vorzuziehen ist hierbei die klare Trennung zwischen Zugangsrechten von Benutzern (meist über Kennung und Passwort) einerseits und Zugriffsrechten von Benutzergruppen und Rollen auf DB-Objekte andererseits. Die Koppelung von Benutzern zu DB-Objekten geschieht dann über die Zuordnung einzelner Benutzer zu den mit den notwendigen Zugriffsrechten ausgestatteten Benutzergruppen oder Rollen. Es können Zugriffsberechtigungen lesender (read), ändernder (update), löschender (delete), neu einfügender (insert) oder neu erstellender (create) Art unterschieden werden. Bei Prozeduren kommt die Ausführungsberechtigung (execute) hinzu. Die Schritte zur Vergabe von Zugriffsberechtigungen SOLLTEN im Datenbankkonzept präzise beschrieben sein. Grundsätzlich SOLLTEN nur die wirklich erforderlichen Zugriffsberechtigungen vergeben werden. Anderenfalls besteht die Gefahr, dass der Überblick über die aktuellen Zugriffsrechte verloren geht und zusätzliche Sicherheitslücken entstehen können. Insbesondere SOLLTE die vom DBMS zur Verfügung gestellte Möglichkeit, Rechte an alle zu vergeben (GRANT ... TO PUBLIC), nicht genutzt werden.
Im allgemeinen ist es nur dem Besitzer eines Datenbankobjektes erlaubt, Zugriffsberechtigungen an andere Benutzer weiterzugeben. Einige Datenbanksysteme stellen jedoch die Möglichkeit zur Verfügung, dass der Besitzer eines Datenbankobjektes auch das Recht, Zugriffsrechte weiterzugeben, an andere Benutzer vergeben kann. Von dieser Möglichkeit SOLLTE nur in begründeten Ausnahmefällen Gebrauch gemacht werden, da der Besitzer des Datenbankobjektes auf diese Weise die Kontrolle über den Zugriff auf die Daten bzw. die Datenbankobjekte verliert.
Anwendungen SOLLTEN einen restriktiven Zugriff auf die Daten unterstützen, d.h. in Abhängigkeit der Benutzer-Kennung und der Gruppenzugehörigkeit SOLLTEN nur diejenigen Funktionalitäten und Daten zur Verfügung gestellt werden, die ein Benutzer für

die Ausführung seiner Aufgaben benötigt. Eine Form der DB-seitigen Realisierung einer solchen Anwendung ist hier die Verwendung von sogenannten Stored Procedures. Stored Procedures sind Abfolgen von SQL-Anweisungen, die in der Datenbank voroptimiert gespeichert werden. Beim Aufruf einer Stored Procedure MÜSSEN nur ihr Name und eventuelle Parameter angegeben werden, um die dahinterstehenden Anweisungen auszuführen. Dies hat zum einen den Vorteil, dass nicht die gesamten Anweisungen zum Datenbank-Server übertragen werden MÜSSEN, was bei komplexeren Operationen die Netzbelastung vermindert.
Zum anderen kann das Datenbanksystem die Anweisungen in einer optimierten, vorcompilierten Form ablegen, so dass sie bei Aufruf schneller ausgeführt werden. Die restriktivste Form der Rechtevergabe ist die Vergabe von Zugriffsrechten auf Stored Procedures statt auf Tabellen oder Views. Wenn Zugriffsrechte nur auf Stored Procedures vergeben werden, können die Benutzer nur die von den Datenbankverantwortlichen ausgewählten Operationen ausführen. Nachfolgend einige Beispiele.

- In Microsoft Access können verschiedene Berechtigungen vergeben werden, die sich entweder auf die Datenbank selbst (Öffnen/Ausführen, Exklusiv, Verwalten) oder auf die Tabellen und Abfragen beziehen (Daten lesen, Daten aktualisieren, Daten löschen, Daten einfügen). Diese Berechtigungen können dann unterschiedlichen Benutzern oder Benutzergruppen zugeordnet werden. Standardmäßig sind bei Microsoft Access die Gruppen “Administratoren” und “Benutzer” eingerichtet, wobei die Gruppe “Benutzer” die Berechtigungen “Daten lesen” und “Daten aktualisieren” für Tabellen und Abfragen sowie die Berechtigung “Öffnen/Ausführen” für Datenbanken enthält. Für eine detailliertere Kontrolle der Zugriffsrechte können eigene Gruppen definiert werden, an die unterschiedliche Berechtigungen vergeben werden können.
- In einer Oracle-Datenbank kann mit den Kommandos CREATE ROLE und GRANT die Gruppe „Abteilung_1“ erstellt und die Berechtigung erteilt werden, z.B. eine Verbindung zur Datenbank herzustellen (connect), eine Session zu eröffnen (create Session) und Auswahlabfragen auf bestimmte Tabellen durchzuführen (select). Indem existierende Datenbank-Benutzer der Gruppe “Abteilung_1” zugeordnet werden, erhalten diese Benutzer alle Berechtigungen der zugeordneten Benutzergruppe. In diesem Beispiel könnte ein ausschließlich der Gruppe “Abteilung_1” zugeordneter Benutzer nur auf die der Gruppe zugeordneten Tabellen und hier ausschließlich lesend (select) aber nicht modifizierend (insert, delete, update, etc.) zugreifen.
- Eine Stored Procedure unter Oracle mit PL/SQL-Anweisungen hat einen Eingabeparameter, der die Artikelnummer angibt. Die Stored Procedure durchsucht alle zur Berechnung der Ausgabeparameter benötigten Tabellen und gibt unter anderem den Artikelpreis zurück. Benutzer erhalten über die Zugriffsrechtevergabe ein Nutzungsrecht nur auf die Stored Procedure, jedoch keinerlei Rechte auf die entsprechenden Tabellen. Damit werden z.B. auch zeitaufwendige Suchoperationen durch eine Auswahlberechtigung direkt auf die zugehörigen Tabellen verhindert.

4.4.5 Gewährleistung der Datenbankintegrität

Die Integritätssicherung und -überwachung einer Datenbank soll die Korrektheit der zugehörigen Daten bzw. einen korrekten Zustand der Datenbank gewährleisten. Die folgenden Techniken sind zur Vermeidung inkorrekter Daten bzw. Zustände innerhalb einer Datenbank zu beachten.

Zugriffskontrolle Damit ist der Schutz der betreffenden Datenbank vor unautorisiertem Zugriff mittels der Vergabe von Zugriffsrechten gemeint, wie in Kapitel 4.4.4 beschrieben. Damit wird dem manipulativen Ändern von Daten bzw. Datenbankobjekten (wie z.B. Tabellen) vorgebeugt. Verantwortlich für die Umsetzung der Zugriffskontrolle ist

der Datenbankadministrator. Auf eine detaillierte Ausführung wird an dieser Stelle verzichtet und stattdessen auf die Empfehlungen aus Kapitel 4.4.4 verwiesen.

Synchronisationskontrolle Die Synchronisationskontrolle dient der Verhinderung von Inkonsistenzen, die durch einen parallelen Zugriff auf denselben Datenbestand entstehen können. Es gibt dazu verschiedene Techniken, wie z.B. das Sperren von Datenbankobjekten (Locking) oder die Vergabe von Zeitstempeln (Time- stamps). Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen, insofern als das ein zusätzlicher Mechanismus zur Verfügung gestellt werden MUSS, der über die Möglichkeiten des DBMS hinausgeht. Auf eine detaillierte Ausführung wird verzichtet, da im allgemeinen jedes DBMS eine Synchronisationskontrolle durchführt. Vom Einsatz eines DBMS, welches dies nicht leisten kann, wird dringend abgeraten.

Integritätskontrolle Hierunter fällt die Vermeidung semantischer Fehler bzw. semantisch unsinniger Zustände der Datenbank durch Einhaltung und Überwachung der geforderten Integritätsbedingungen. Diese können sich auf einzelne Relationen beziehen oder mehrere Relationen miteinander in Beziehung setzen (referentielle Integrität). Beispiele sind die Angabe eines Primärschlüssels für eine Relation, die Definition von Wertebereichen zu den einzelnen Attributen oder die Formulierung spezieller Bedingungen mittels einer assertion-Klausel. Dies kann durch das DBMS automatisch mittels eines Monitors überprüft werden, der z.B. durch die Verwendung von Triggern oder Stored Procedures realisiert werden kann. Damit sind prinzipiell beliebige Transaktionen möglich, jedoch werden diejenigen vom DBMS zurückgewiesen, die die Datenbank-Konsistenz verletzen würden. Verantwortlich für die Umsetzung sind die Verantwortlichen der IT-Anwendungen respektive der fachliche Administrator, falls es sich um eine Umsetzung der Integritätsbedingungen in Form von Relationen, Primärschlüsseln oder allgemeinen Datenbankobjekten handelt. Im Rahmen der Konzeption einer IT-Anwendung sind folgende Punkte zu erstellen.

- Ein Datenmodell, welches neben den Datenbankobjekten auch deren Beziehungen untereinander abbildet.
- Ein Fachkonzept, welches unter anderem Bedingungen beschreibt, unter denen Daten manipuliert werden DÜRFEN.

Im Rahmen der Realisierung einer IT-Anwendung sind die folgenden Punkte zu beachten.

- Die konkrete Umsetzung des in der konzeptionellen Phase definierten Datenmodells MUSS festgelegt werden. Hierzu gehört die Definition und Anlage von Tabellen, Indizes, Wertebereichen usw.
- Die Definition von Triggern oder Stored Procedures erfolgt im Rahmen der Realisierung des Fachkonzepts. Trigger und Stored Procedures können dabei sowohl innerhalb der Anwendung (in den Programmen), als auch der Datenbank (für Tabellen) Verwendung finden. Trigger, die auf Datenbankebene eingesetzt werden, wirken unabhängig von darüberliegenden Anwendungen und sind aus diesem Grund zentral zu verwalten. Als Beispiel sei hier ein Trigger “Update” für eine Tabelle erläutert: Immer wenn ein Datensatz der Tabelle geändert wird, dann sind die für den Trigger definierten Anweisungen auszuführen. Eine dieser Anweisungen kann der Aufruf einer Stored Procedure sein.

Im Rahmen von Anwendungen kann eine Integritätssicherung durch einen geeigneten Einsatz von Commit bzw. Rollback für das Betätigen bzw. Widerrufen von Transaktionen realisiert werden.

4.4.6 Aufteilung von Administrationstätigkeiten

Um einen geordneten Betrieb von Datenbanksystemen zu ermöglichen, sind Administratoren zu bestimmen. Diesen obliegt neben allgemeinen Administrationsarbeiten insbesondere die Benutzerverwaltung einschließlich der Verwaltung der Zugriffsrechte. Zusätzlich sind sie für die Sicherheitsbelange der betreuten Datenbanksysteme zuständig. Neben der Ernennung eines Administrators und eines Vertreters und der Auswahl eines vertrauenswürdigen Administrators und Vertreters sind speziell für Datenbanksysteme folgende Dinge zu beachten. Es SOLLTEN grundsätzlich zwei verschiedene Administrator-Rollen für die beiden folgenden Bereiche unterschieden werden.

- Die fachlich übergreifende Administration der Datenbank-Software.
- Die Administration der anwendungsspezifischen Belange.

Diese beiden Aufgaben SOLLTEN von verschiedenen Personen durchgeführt werden, um eine Trennung der anwendungsspezifischen und fachlich übergreifenden Administration einer Datenbank zu erreichen. Der grundsätzliche Betrieb des DBMS, die Durchführung der Datensicherungen oder die Archivierung von Datenbeständen sind beispielsweise Bestandteil der fachlich übergreifenden Datenbankadministration.
Bei der anwendungsspezifischen Administration werden dagegen die Erfordernisse der einzelnen Anwendungen an die Datenbank bearbeitet. Dies kann z.B. die Verwaltung der zugehörigen Datenbankobjekte, die Unterstützung der Benutzer bei Problemen bzw. Fragen oder die Verwaltung der entsprechenden Datenbankkennungen beinhalten. Letzteres ist allerdings nur dann möglich, wenn die Verwaltung der Datenbankkennungen je Anwendung über ein entsprechendes Berechtigungskonzept durch die Datenbank-Software unterstützt wird, also von den fachlich übergreifenden Berechtigungen getrennt werden kann.
Der fachlich übergreifende Administrator richtet die für die anwendungsspezifischen Belange zuständigen Administratorkennungen mit den zugehörigen Berechtigungen ein. Dazu gehört insbesondere das Recht, Datenbanken anzulegen. Die Rechtevergabe für die einzelnen Benutzer SOLLTE dagegen für jede anwendungsspezifische Datenbank getrennt durchgeführt werden und zwar vom jeweils zuständigen anwendungsspezifischen Administrator.

4.4.7 Kontrolle der Protokolldateien

Die in einem Datenbanksystem mögliche Protokollierung bzw. Auditierung ist in einem sinnvollen Umfang zu aktivieren. Werden zu viele Ereignisse protokolliert, wird die Performance der Datenbank negativ beeinflusst und die Protokolldateien wachsen stark an. Es MUSS also immer zwischen dem Bedürfnis, möglichst viele Informationen zur Sicherheit der Datenbank zu sammeln, und der Möglichkeit, diese Informationen zu speichern und auszuwerten, abgewogen werden. Dabei sind insbesondere folgende Vorkommnisse von Interesse.

- Anmeldezeiten und -dauer der Benutzer,
- Anzahl der Verbindungen zur Datenbank,
- fehlgeschlagene bzw. abgewiesene Verbindungsversuche,
- Auftreten von Deadlocks innerhalb des Datenbanksystems,
- I/O-Statistik für jeden Benutzer,
- Zugriffe auf die Systemtabellen,
- Erzeugung neuer Datenbankobjekte und
- Datenmodifikationen (eventuell mit Datum, Uhrzeit und Benutzer).

Die Protokollierung sicherheitsrelevanter Ereignisse ist als Sicherheitsmaßnahme allerdings nur dann wirksam, wenn die protokollierten Daten auch ausgewertet werden. Daher sind die Protokolldateien in regelmäßigen Abständen durch einen Revisor auszuwerten. Ist es organisatorisch oder technisch nicht möglich, einen unabhängigen Revisor mit der Auswertung der Protokolldateien zu betrauen, ist eine Kontrolle der Tätigkeiten des Administrators nur schwer möglich.
Weiterhin ist bei der Protokollierung sicherheitsrelevanter Ereignisse sowie bei der Prüfung (Monitoring) der Protokolldateien Folgendes zu beachten. Für die Überprüfung der Protokolldateien sind diese grundsätzlich in eine andere Umgebung zu kopieren. Geeignete Tools SOLLTEN dabei genutzt werden. Die Verantwortlichkeiten für die Protokollierung und die Verantwortlichkeiten für die zu protokollierenden Aktivitäten MÜSSEN getrennt werden. Bei der Protokollierung sicherheitsrelevanter Ereignisse SOLLTEN Änderungen nur im Vier-Augen-Prinzip möglich sein. Die Protokollierung ist zudem vor den folgenden Fällen zu schützen.

- Deaktivierung.
- Änderungen der zu protokollierenden Ereignistypen.
- Änderung der Protokolldaten (Inhalt).
- Datenverlust bei Protokoll-Medien, z.B. durch Überschreiben, falsches Beschreiben, falsche Lagerung.

Die Protokolldaten MÜSSEN auf dem Produktivsystem regelmäßig gelöscht werden, um ein übermäßiges Anwachsen der Protokolldateien zu verhindern. Sie DÜRFEN allerdings nur dann gelöscht werden, wenn die Protokolldateien vorher ausgewertet und kontrolliert wurden. Unter Umständen MÜSSEN die Protokolldaten archiviert werden. Die Archivierung oder gegebenenfalls auch die Löschung der Protokolldateien kann manuell oder automatisch geschehen, falls entsprechende Werkzeuge zur Verfügung stehen. Bei Auffälligkeiten ist das Sicherheitsmanagement zu unterrichten.
Weiterhin ist der Zugriff auf die Protokolldateien strikt zu beschränken. Einerseits MUSS verhindert werden, dass Angreifer ihre Aktionen durch nachträgliche Änderung der Protokolldateien verbergen können, andererseits könnten über die gezielte Auswertung von Protokolldateien Leistungsprofile der Benutzer erstellt werden. Deshalb DÜRFEN beispielsweise Änderungen überhaupt nicht vorgenommen werden und lesender Zugriff DARF nur den Revisoren gestattet werden.
Bei der Konzeption der Vorgehensweise für die Protokollierung und Auswertung der Protokolldaten MÜSSEN frühzeitig der Datenschutzbeauftragte und die Personalvertretung beteiligt werden. Um die Auswertung der Protokolldaten zu vereinfachen, können vom Datenbank- Administrator zusätzliche Tools eingesetzt werden, die eine automatisierte Überwachung durchführen. Solche Produkte können beispielweise die Protokolldateien von Datenbanksystemen nach vorgegebenen Mustern auswerten und bei Bedarf einen Alarm erzeugen.

4.4.8
Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung

Wird ein IT-System oder eine IT-Anwendung von mehreren Benutzern verwendet und besitzen die einzelnen Benutzer unterschiedliche Zugriffsrechte auf dort gespeicherte Daten oder Programme, so kann der erforderliche Schutz mittels einer Zugriffskontrolle nur dann erreicht werden, wenn jeder Benutzer sich nach Aufgabenerfüllung am IT-System oder der IT-Anwendung abmeldet. Ist es einem Dritten möglich, an einem IT-System oder in einer IT-Anwendung unter der Identität eines anderen weiterzuarbeiten, so ist jegliche sinnvolle Zugriffskontrolle unmöglich. Daher sind alle Benutzer zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden. Aus technischen Gründen (z.B. damit alle offenen Dateien geschlossen werden) SOLLTEN auch dann Regelungen für die Abmeldung von IT-Systemen und IT-Anwendungen

getroffen werden, wenn keine Zugriffskontrolle realisiert ist. Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen. Bei längerer Abwesenheit SOLLTE die Bildschirmsperre automatisch aktiviert werden.
Einige IT-Systeme und IT-Anwendungen bieten die Möglichkeit, einen Zeitraum vorzugeben, nach dessen Ablauf ein Benutzer bei Inaktivität automatisch vom System abgemeldet wird. Es SOLLTE überlegt werden, ob dieses Verfahren benutzt wird, da es auch zu Datenverlusten führen kann. Eine automatische Abmeldung kann z.B. bei PC-Pools mit starkem Publikumsverkehr zum Einsatz kommen, da hier ein angemeldeter Benutzer den Arbeitsplatz mit Hilfe der Bildschirmsperre unberechtigterweise blockieren kann.
Je nach Arbeitsplatzumgebung ist abzuwägen, welche Vorkehrungen für kurzfristige Abwesenheiten von Benutzern zu treffen sind. So SOLLTE eine automatische Aktivierung der Bildschirmsperre bei Mehr-Benutzer-Systemen schneller erfolgen als bei solchen für einen Benutzer, also z.B. bereits nach 5 Minuten.

4.4.9
Sperren und Löschen nicht benötigter Datenbank-Accounts

Wenn ein neu einzurichtender Benutzer seinen Datenbank-Account nur für einen befristeten Zeitraum benötigt, SOLLTE dieser auch nur befristet eingerichtet werden, falls die Datenbank eine solche Möglichkeit zur Verfügung stellt. Es kann vorteilhaft sein, Accounts grundsätzlich nur befristet einzurichten und in regelmäßigen Abständen (z.B. jährlich) bei Bedarf zu verlängern. Darüber hinaus SOLLTE die Datenbankadministration schnellstmöglich über das endgültige Ausscheiden eines Benutzers informiert werden. Spätestens am letzten Arbeitstag des Benutzers ist dessen Account zu sperren.
Auch wenn Benutzer in ein anderes Aufgabengebiet, einen anderen Zuständigkeitsbereich oder andere Projekte wechseln, MÜSSEN die dafür nicht mehr benötigten Datenbank-Accounts gesperrt oder die Zugriffsrechte entsprechend angepasst werden. Weiterhin SOLLTE regelmäßig geprüft werden, ob vorhandene Datenbank-Accounts tatsächlich benötigt werden. Insbesondere SOLLTEN hierbei auch nicht benötigte Standard-Accounts gesperrt werden.

4.4.10
Sicherstellung einer konsistenten Datenbankverwaltung

Die Datenbankverwaltung steht im Zentrum des Betriebskonzepts eines Datenbanksystems DBS, auf dessen Grundlage unter anderem die konsistente Datenbankverwaltung sichergestellt werden soll. Im Betriebskonzept MÜSSEN alle für den Betrieb des DBS wichtigen Prozesse mit fest definierten Ausgangspunkten, Durchführungsreihenfolgen und Zielen sowie die zur Durchführung der Prozesse berechtigten Rollen mit ihren Rechten und Pflichten definiert sein. Im weiteren Verlauf des Projekts MÜSSEN darüber hinaus den definierten Rollen reale Personen zugeordnet werden.
In der Rollenbeschreibung werden die Aufgaben, Zugriffsrechte und Befugnisse der Rollen beschrieben, die zur Durchführung bestimmter Funktionen notwendig sind. Im DBMS sind die definierten Rollen als Benutzergruppen einzurichten, denen die rollenspezifischen Rechte zuzuordnen sind. Den Benutzergruppen werden gemäß Rollenprofil die zuständigen Benutzer über ihre Benutzerkennung zugeordnet. Besonders zu beachten sind nachfolgende Hinweise.

- Der Systemadministrator ist ein spezieller Benutzer in der Rechteverwaltung des Datenbanksystems, der bereits nach der Installation des DBMS zur Verfügung steht. Dieser Benutzer unterliegt prinzipiell keinerlei Beschränkungen bei der Nutzung des Datenbanksystems, wodurch ein Risiko für Fehler oder Missbrauch besteht. Diese Kennung DARF nur von dem kleinen Kreis der System-Administratoren für explizit fest-

gelegte Administrationsaufgaben, wie die Einrichtung von Datenbank-Administratoren für einzelne Datenbanken, genutzt werden.

- Die Benutzergruppen der Datenbank-Administratoren für einzelne Datenbanken und somit auch die jeweils zugeordneten Benutzer unterliegen prinzipiell keinerlei Beschränkungen bei Nutzung und Manipulation der Datenbanken in ihrem Zuständigkeitsbereich, wodurch ein generelles Gefahrenpotenzial besteht. Die Rechte, die für diese Aufgaben notwendig sind, MÜSSEN daher wie der Personenkreis, der mit diesen Rechten ausgestattet wird, klar definiert und dokumentiert sein.
- In vielen Fällen arbeiten die Administratoren auch als Benutzer auf einer Datenbank, da sie neben ihrer Administratorentätigkeit Benutzeraufgaben wahrnehmen oder die Datenbank für die Ablage und Verwaltung von Dokumentationen im Administrationsumfeld nutzen. In diesem Fall ist für sie, neben der Administratorenkennung, eine normale Benutzerkennung anzulegen, die für solche Arbeiten mit der Datenbank genutzt wird. Die Administratorenkennung DARF nur für Administrationstätigkeiten genutzt werden.
- Die Zuordnung eines Benutzers zu mehreren Benutzergruppen SOLLTE genau geplant werden, da der Benutzer die Summe der Berechtigungen aller Benutzergruppen erhält, denen er zugeordnet ist.

Zusätzlich SOLLTE durch eine klare Aufgabenteilung, verbindliche Regelungen sowie Absprachen zwischen den Administratoren sichergestellt werden, dass Administratoren keine inkonsistenten oder unvollständigen Eingriffe vornehmen. Dabei SOLLTEN folgende Bedingungen erfüllt sein.

- Die Art und Weise der Durchführung von Änderungen sowie deren Dokumentation ist festzulegen.
- Art, Umfang und Grund der Änderungen sind zu beschreiben.
- Änderungen an Datenbankobjekten oder Daten sind prinzipiell durch den Verantwortlichen der IT-Anwendung genehmigungspflichtig. Handelt es sich dabei um ein zentrales Datenbankobjekt, so erfordert eine Änderung die Zustimmung aller Verantwortlichen der betroffenen IT-Anwendungen.
- Der Zeitpunkt der geplanten Änderungen ist festzulegen und bekannt zu geben.
- Vor der Durchführung von Änderungen MUSS die Datenbank komplett gesichert werden.
- Für den laufenden Betrieb SOLLTE ein Kontrollintervall festgelegt werden, in dem die Dokumente/Protokolle auf Aktualität und Korrektheit überprüft werden (siehe auch Kapitel 4.4.11).

Um Gefährdungen der Datenbankintegrität und Inkonsistenzen einzelner Datensätze zu vermeiden, SOLLTEN alle Datenbankobjekte einer Anwendung unter die ausschließliche Verwaltung einer eigens für die jeweilige Anwendung eingerichteten Benutzergruppe gestellt werden. Dieser Benutzergruppe DÜRFEN ausschließlich Anwender zugeordnet werden, die direkte Zugriffsrechte auf die Datenbankobjekte der betreffenden Anwendung zu ihrer Aufgabenerfüllung benötigen. Außerdem SOLLTE der für die jeweilige Anwendung zuständige Datenbankadministrator Mitglied dieser Benutzergruppe sein.

4.4.11
Regelmäßiger Sicherheitscheck der Datenbank

Der Datenbankadministrator SOLLTE regelmäßig, jedoch mindestens einmal monatlich einen Sicherheitscheck des DBS durchführen, der durch das Betriebskonzept geregelt sein SOLLTE. In Abhängigkeit der Prüfungsergebnisse SOLLTEN entsprechende Maßnahmen ergriffen werden, um Abweichungen von den Vorgaben des Betriebskonzepts abzustellen. Diese Maßnahmen und die Zuständigkeiten für die Umsetzung SOLLTEN ebenfalls im Betriebskonzept festgelegt sein. Folgende Aspekte SOLLTEN im Rahmen

des Sicherheitschecks mindestens überprüft werden, wobei die mit (*) markierten Punkte meist durch entsprechende Skripte automatisiert werden können.

- Werden die im Betriebskonzept vorgegebenen Nachweise (z.B. Dokumentation von Änderungen) korrekt erstellt?
- Sind die erforderlichen und geplanten Sicherungs- und Sicherheitsmechanismen aktiv und greifen sie auch?
- Gibt es Datenbank-Benutzer mit leicht zu ermittelndem oder keinem Passwort? (*)
- Gibt es Benutzer, die die ihnen zugewiesenen Rechte nicht mehr für ihre Aufgabenerfüllung benötigen?
- Wer DARF bzw. kann außer dem Datenbank-Administrator auf die Dateien der Datenbank-Software bzw. auf die Dateien der Datenbank auf Betriebssystemebene zugreifen? (*)
- Wer hat außer dem Datenbank-Administrator Zugriff auf die System-Tabellen der Datenbanken?
- Wer DARF mit einem interaktiven SQL-Editor auf die Datenbank zugreifen?
- Welche Benutzer-Kennungen haben modifizierende Zugriffsrechte auf die Datenbankobjekte der Anwendungen? (*)
- Welche Benutzer-Kennungen haben lesende und / oder modifizierende Zugriffsrechte auf die Daten der Anwendungen? (*)
- Welche Benutzer besitzen die gleichen Rechte wie der Datenbank-Administrator? (*)
- Verfügt das Datenbanksystem über ausreichend freie Ressourcen? (*)

4.4.12 Durchführung einer Überwachung

Um die Verfügbarkeit, die Datenbankintegrität und die Vertraulichkeit der Daten gewährleisten zu können, ist eine regelmäßige und in angemessen definierten Überwachungszeiträumen durchzuführende Datenbanküberwachung erforderlich. Dabei zu beachtende Aspekte, die im folgenden kurz erläutert werden, sind unter anderem die Datenfragmentierung innerhalb der Datenbank, das aktuelle Datenvolumen und dessen Veränderung hinsichtlich der vorhandenen Ressourcen (Füllgrad) sowie die Auslastung der Datenbank.
Die Datenbank ist in regelmäßigen Zeitabständen hinsichtlich einer möglichen Fragmentierung zu überprüfen, um gegebenenfalls Maßnahmen, wie z.B. eine Reorganisation der Datenbank, planen und durchführen zu können. Die Speicherplatzverwaltung in einem DBMS geschieht in der Regel in Form von Blöcken fester Größe, d.h. eine Veränderung (meist Vergrößerung) des Speicherplatzes erfolgt nur in Blöcken. Datensätze werden dabei auf eine minimale Anzahl von Blöcken verteilt abgespeichert. Prinzipiell werden Daten hinzugefügt, indem zuerst freie Blöcke belegt und wenn nötig zusätzlich neue Blöcke angelegt werden. Beim Löschen werden die zugehörigen Blöcke wieder freigegeben und stehen für neue Daten zur Verfügung.
Um einer zu starken bzw. zu raschen Fragmentierung vorzubeugen, erlauben einige Datenbankmanagementsysteme durch Definition bestimmter Parameter bereits beim Anlegen der Tabellen, eine bestimmte Menge zusammenhängender Blöcke zu reservieren. Damit steigt bei gleichem Datenvolumen der Füllgrad. Die Datenbankdateien SOLLTEN regelmäßig hinsichtlich ihres Datenvolumen und Füllgrades überwacht werden. Dabei wird regelmäßig überprüft, ob sich das Datenvolumen zusammen mit dem Füllgrad im vorgegebenen Rahmen verändert. Ist das Wachstum größer als erwartet, kann es unter Umständen zu Speicherengpässen kommen. Aus den Beobachtungen SOLLTEN Maßnahmen, wie z.B. eine Erweiterung der Speicherkapazitäten, abgeleitet werden.
Sei im Folgenden ein Beispiel für die Datenverwaltung einer Oracle-Datenbank angeführt. Bei einer Oracle-Datenbank wird jeder Tabelle eine feste Anzahl von Extents (im Sprachgebrauch von Oracle: logische Größeneinheit) zugeordnet. Die Daten einer Tabelle werden in mindestens einem Extent abgelegt. Sobald die Kapazität eines Extents

ausgeschöpft ist, legt das DBMS automatisch ein weiteres Extent an. Beim Erstellen einer Tabelle können dabei folgende Werte definiert werden.

- Größe des ersten und nachfolgenden Extents in Bytes.
- Wachstum aller weiteren Extents in Prozent, wobei diese Zahl in Relation zur Größe des zweiten Extents steht.
- Maximale Anzahl an Extents, die für die Tabelle angelegt werden DÜRFEN.
- Reservierte Blöcke für spätere Änderungen in Prozent.

Wenn durch Anlage weiterer Extents der freie Speicherbereich innerhalb eines Tablespaces zu gering wird, MUSS ein neuer Tablespace hinzugefügt werden. Eine Verringerung der Anzahl der Tablespaces ist nur durch vollständige Reorganisation möglich. Darüber hinaus ist die Auslastung der Datenbank regelmäßig zu prüfen, insbesondere im Hinblick auf die eingestellten Obergrenzen. Welche Informationen für eine konkrete Datenbanküberwachung relevant sind, hängt von deren spezieller Funktionsweise, also von der eingesetzten Datenbank-Standardsoftware ab. Dementsprechend sind auch individuelle Maßnahmen einzuleiten, die die Datenbankkonfiguration dahingehend modifizieren, dass sie den Anforderungen hinsichtlich Zugriffsgeschwindigkeiten, durchzuführender Transaktionen usw. gerecht wird. Eine Automatisierung der Datenbanküberwachung kann in vielen Fällen mit Hilfe von Skripten durchgeführt werden. Eine Voraussetzung ist allerdings, dass die Informationen in auswertbarer Form von der eingesetzten Datenbank- Software zur Verfügung gestellt werden.

4.4.13 Verschlüsselung

In Abhängigkeit von der Art der in einer Datenbank gespeicherten Informationen und den sich daraus ergebenden Anforderungen an deren Vertraulichkeit und Integrität kann es notwendig werden, diese Daten zu verschlüsseln. Dabei kann zwischen einer Online- und einer Offline-Verschlüsselung unterschieden werden.

- Bei einer Online-Verschlüsselung werden die Daten während des laufenden Betriebs ver- und entschlüsselt, ohne dass die betroffenen Benutzer davon etwas merken. Dafür können Tools eingesetzt werden, mit denen entweder auf Betriebssystemebene die gesamte Festplatte verschlüsselt wird, oder solche, mit denen nur die Anwendungsdaten der Datenbank verschlüsselt werden.
- Bei einer Offline-Verschlüsselung werden die Daten erst nach ihrer Bearbeitung verschlüsselt und vor ihrer Weiterverarbeitung wieder entschlüsselt. Dies wird im Allgemeinen mit Tools durchgeführt, die nicht in das Datenbanksystem integriert sind, und kann insbesondere für Datensicherungen oder Datenübertragungen sinnvoll sein. Dabei ist zu beachten, dass genügend Platz auf der Festplatte vorhanden ist, da die Ver- bzw. Entschlüsselung nur dann erfolgreich ausgeführt werden kann, wenn auf der Festplatte genügend Platz für das Original und die verschlüsselte Version der Datenbank verfügbar ist.

Darüber hinaus besteht die Möglichkeit, Daten weiterhin im Klartext in der Datenbank abzuspeichern, beim Zugriff über ein Netz jedoch eine verschlüsselte Datenübertragung zu realisieren. Dies kann z.B. durch die Secure Network Services der Oracle SQL*Net [8] Produktfamilie durchgeführt werden.
Welche Daten mit welchem Verfahren zu verschlüsseln sind, ist am besten bereits bei der Auswahl der Datenbank-Standardsoftware festzustellen. Dabei SOLLTEN die Anforderungen hinsichtlich der Verschlüsselung von Datenbeständen mit den entsprechen-

[8] https://www.orafaq.com/wiki/SQL*Net

den Leistungsmerkmalen der Datenbank-Software verglichen werden. Als Mindestanforderung SOLLTE sie in jedem Fall sicherstellen, dass die Passwörter der Benutzer-Kennungen der Datenbank verschlüsselt abgelegt sind.
Falls die Anforderungen durch keine der am Markt verfügbaren Datenbank- Standardsoftware abgedeckt werden können, SOLLTE man den Einsatz von Zusatzprodukten prüfen, um die entsprechende Sicherheitslücke zu schließen. Falls auch keine Zusatzprodukte erhältlich sind, MUSS ein Konzept für die Umsetzung einer Verschlüsselungsstrategie erstellt werden, das im Unternehmen bzw. in der Behörde umgesetzt wird.

4.4.14
Integration eines Datenbank-Servers in ein Sicherheitsgateway

Bei der Aufstellung von Datenbank-Servern zum Zugriff aus einem nicht-vertrauenswürdigen Netz sind zwei Haupt-Anwendungsfälle zu unterscheiden.

1. Zugriff auf die Daten der Datenbank über ein Web-Frontend.
2. Direkter Zugriff auf die Daten der Datenbank (z.B. mittels SQL)

Beide Anwendungsfälle werden in den folgenden beiden Abschnitten beschrieben.
Der Webserver und der Datenbank-Server SOLLTEN in unterschiedlichen DMZ stehen, damit bei einer Kompromittierung des Webservers ein Schutz des Datenbank- Servers durch einen Proxy des Application Level Gateways (ALG) besteht. Der Schutz durch den Proxy ist allerdings nur gering, beispielsweise wird der TCP/IP-Stack des Datenbank-Servers geschützt. Zudem können Angriffe auf Basis von TCP/IP-Header-Daten verhindert werden. Falls keine besonderen Sicherheitsanforderungen bestehen, so kann der Server auch in der gleichen DMZ wie der Webserver aufgestellt werden. Der Aufbau und die Kommunikationsbeziehungen sind in diesem Fall wie folgt.

- Der Zugriff vom Internet aus erfolgt ausschließlich per HTTPS auf den Webserver. Die Zugriffe werden durch das ALG entsprechend abgesichert.
- Eine auf dem Webserver laufende Anwendung setzt die Anfrage in entsprechende Datenbankabfragen um, führt diese Abfragen auf der Datenbank aus und bereitet die Ergebnisse entsprechend auf.
- Die Administration des Datenbankrechners, des Datenbanksystems und die Pflege der Daten in der Datenbank erfolgen über entsprechend abgesicherte Verbindungen aus dem internen Netz.

Der Client im nicht-vertrauenswürdigen Netz kann ausschließlich an den Webserver über Webseiten Anfragen stellen, ein direkter Zugriff auf die Datenbank selbst ist nicht möglich.
Bei diesem Aufbau ist es über die Absicherung auf der Transportebene hinaus wichtig, dass die Anwendung auf dem Webserver, welcher die Anfragen und Ergebnisse aufbereitet, entsprechend sicher programmiert ist und keine Möglichkeiten für Angriffe auf die Datenbank (beispielsweise SQL Injection) bietet. Falls über das Web-Frontend sogar direkt Datenbankanfragen in der betreffenden Datenbanksprache (beispielsweise SQL) formuliert werden können, MUSS der Zugriff auf das Web-Frontend nur über HTTPS erfolgen.
Soll auf die Datenbank direkt aus dem nicht-vertrauenswürdigen Netz heraus zugegriffen werden, so SOLLTE der Server in einer eigenen DMZ aufgestellt werden. Da nur wenige Proxies für Datenbankprotokolle existieren, ist der Einsatz eines TCP- oder UDP-Relays oftmals unumgänglich.
Da sich, wegen der fehlenden Sicherheitsproxies, für Datenbankabfrage-Protokolle kaum mittels Sicherheitsproxies kontrollieren lassen, ist die zuerst vorgestellte Lösung mit einem Web-Frontend in der Regel die sichere Variante.

Je nach dem Schutzbedarf der Daten in der Datenbank wird dringend empfohlen, nicht die “Echtdatenbank” für den externen Zugriff freizugeben, sondern nur eine Kopie der Daten auf einer separaten Datenbank, die in entsprechenden Intervallen mit der “Echtdatenbank” synchronisiert wird.

5
Zusammenfassung

Es wurde eine Übersicht von relevanten Normen, Gremien und Standards gegeben die sich mit dem Thema Sicherheit in der IT befassen. Bei der Recherche ist schnell deutlich geworden, dass der ITG die umfassendsten und konkretesten Leitlinien und Empfehlungen für IT-Systeme bietet. Darüber hinaus liefert es ein systematisches Vorgehen um beliebige IT-Systeme für eine Sicherheitsbetrachtung zu modellieren und zu untersuchen. Besonders Hilfreich für eine Institution ist die vergleichsweise geringe Einstiegshürde da es möglich ist erst ein niedriges Sicherheitsziel mit vergleichsweise geringem Aufwand zu verfolgen und iterativ das Sicherheitsniveau zu erhöhen. Ebenfalls liefert der ITG Hinweise welches Sicherheitsniveau bzw. Empfehlungen für Zertifizierungen wie z.B. ISO/IEC 27001 relevant sind.
Nach der Modellierung wurden für die drei Hauptkomponenten eines VK (Web-Anwendung, Web-Service und Datenbanken) Handlungsempfehlungen zum Betrieb formuliert. Durch die ähnliche technische Charakteristik zwischen Web-Anwendung und Web-Service überschneiden sich viele Empfehlungen und es gibt Empfehlungen allgemeiner Natur welche für eine Vielzahl von IT-Systemen im allgemeinen gelten. Zusammengefasst basieren viele Empfehlungen auf grundlegendem Management von Zuständigkeiten und Sichtbarkeitsgrenzen von Informationen zwischen IT-Systemen aber auch den Personen, welche damit in Kontakt bzw. Interaktion treten. Ein weiterer wichtiger Punkt ist die korrekte Einhaltung und Umsetzung von Regeln sowie Wahrung der Datenintegrität. Für ein IT-System ist es maßgeblich ob es nicht nur für den Standardfall entwickelt wurde sondern auch in Grenzsituationen bzw. Sonderfällen korrekt funktioniert. Häufig sind es eben diese Sonderfälle, welche wenn sie nicht korrekt vom IT-System abgedeckt sind, eine Sicherheitslücke darstellen. Hervorzuheben ist hier das Security-by-Design Prinzip welches bereits vor der Implementierung einer Anwendung und vor der Konzipierung einer IT-Architektur, Sicherheitsaspekte in den ersten Überlegungenn postuliert. Wenn ein IT-System von Beginn an Sicherheitsaspekte berücksichtigt (wie z.B. ein Nutzermanagement mit Rechteverwaltung) ist es vergleichsweise einfach ein hohes Sicherheitsniveau (und ggf. Zertifizierung) zu erreichen. Falls in der Entwicklung eines IT-System, Sicherheitsaspekte bloß eine untergeordnete Rolle gespielt haben, ist der Aufwand, der getrieben werden muss um ein gewisses Sicherheitsniveau zu erreichen ggf. nicht mehr tragbar.
Auf Ebene der Personen, welche mit einem sicherheitsrelevantem IT-System arbeiten ist die Sensibilisierung für sicherheitsaspekte sowie regelmäßige Schulungen besonders wichtig.
Im Rahmen der praktischen Sicherheitsanalyse wurden Teile der Webanwendung der PowerTrade Platform untersucht. Es wurden die potentiellen Schwachstellen beschrieben und mit Hilfe von der CWE kategorisiert. Ob es sich hierbei um reale Schwachstellen handelt muss im Nachgang an diese Untersuchung durch Enertrag bewertet werden.

Anhang A
Sicherheitsanalyse der Powertrade Plattform der ENERTRAG

Fraunhofer
IEE

FRAUNHOFER-INSTITUT ENERGIEWIRTSCHAFT UND ENERGIESYSTEMTECHNIK

SICHERHEITSANALYSE VON „ENERTRAG-POWERTRADE“

Inhalt

1
Allgemeines und Randbedingungen

Im Rahmen des Projektes WindNODE wurde in Abstimmung mit Enertrag eine Sicherheitsanalyse der Webanwendung der PowerTrade-Plattform durchgeführt. Bei der Analyse wurde darauf Wert gelegt, dass das laufende System nicht beeinträchtigt wird, da das Test- und Produktivsystem sich die gleiche Datenbank teilen.
In Kapitel 2 werden die gefundene potentielle Schwachstellen dargestellt und beschrieben. Ob es sich hierbei wirklich im eine Schwachstelle des betrachteten Systems handelt, muss durch Enertrag entsprechend bewertet werden.
Für die Durchführung wurde ein Gast-Account mit eingeschränkten Rechten genutzt, welcher für jeden Internet-Nutzer zugänglich ist. Die Gast-Anmeldung ist über einen Link auf der Enertrag Firmen-Webseite möglich, demnach kann aktuell jeder diesen Zugang nutzen und die potentiellen Schwachstellen ausnutzen.
Dieser Nutzer hat zum jetzigen Zeitpunkt initial Zugriff auf 15 Energieanlagen und kann für diese Anlagen verschiedene Informationen abrufen. Möglichkeiten zum Daten schreiben hat der Nutzer sehr wenig, dadurch sind einige Angriffsvarianten erstmal ausgeschlossen (z.B. Stored-Cross-Site-Scripting).
Die gefundenen Schwachstellen wurde anhand der Common Weakness Enumeration (CWE) kategorisiert. Dies ist eine von der Community entwickelte Liste mit dem Ziel eine gemeinsame Sprache für Sicherheitsschwachstellen zu schaffen.
Die Idee hinter dieser ersten Sicherheitsanalyse war es mit so wenig wie möglich Informationen einen erfolgreichen Angriff darzustellen.

2 Durchführung der Sicherheitsanalyse

2.1 CWE-200: Information Exposure

2.1.1 Reporting - Abfragen von Anlagen-Informationen

Durch Manipulation des Request zum Darstellen der »Datenstromvorgänge für Energieanlagen« ist es möglich mehr Anlagen zu sehen, als initial für den Benutzer möglich waren.

URL:
https://powersystem.enertrag.com/PyReportsExt/Reporting/PerformanceReport2#DatenstromAnlage

Request:
POST
https://powersystem.enertrag.com/PyReportsExt/Reporting/PerformanceReport2/DatenstromAnlage HTTP/1.1
Host: powersystem.enertrag.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: de,en-US;q=0.7,en;q=0.3
Referer:
https://powersystem.enertrag.com/PyReportsExt/Reporting/PerformanceReport2
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 163
Cookie: culture=de-DE; ASP.NET_SessionId=oes3brbcvzynfwd04sq2ndzm; pyweb.20171207085018=[…]
Connection: keep-alive
Cache-Control: max-age=0

{"ids":[78,342,343,344,345,346,347,348,349,350,353,354,355,356,357],"from":"2014-12-31T23:00:00.000Z","to":"2017-07-31T21:59:59.000Z","units":-1,"culture":"de-DE"}

Erklärung:
Der Request wird durch einen lokalen Proxy abgefangen und somit sind die »ids« für den Client frei wählbar. Für den Angriff wurden die Zahlen 1 bis 70 ergänzt. Das Ergebnis sieht man in Abbildung 1. Diese Energieanlagen waren für den Benutzer vorher nicht sichtbar.
Hinweis:
Eine Anfrage mit die IDs von 1 bis 2000 wurde nach mehreren Minuten ohne Ergebnis abgebrochen. Dies könnte für einen Angreifer ein Indiz dafür sein, dass mit dieser Anfrage – unter zusätzlicher Anpassung eines größeren Zeitbereichs – ein Denial of Service Angriff gestartet werden kann.

2.1.2 PowerChart

Durch Manipulation des Request zum Darstellen der »Leistungskurven« ist es möglich mehr Anlagen zu sehen, als initial für den Benutzer möglich waren.

URL:
https://powersystem.enertrag.com/PyReportsExt/Reporting/ChartReports

Request:
POST https://powersystem.enertrag.com/PyReportsExt/Reporting/ChartReports HTTP/1.1
Host: powersystem.enertrag.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Referer: https://powersystem.enertrag.com/PyReportsExt/Reporting/ChartReports
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Cookie: culture=de-DE; ASP.NET_SessionId=oes3brbcvzynfwd04sq2ndzm; pyweb.20171207085018=[…]
Connection: keep-alive
Upgrade-Insecure-Requests: 1

SelectedEaID=1&Von=09.01.2018&Bis=11.01.2018

Erklärung:
Der Request wird durch einen lokalen Proxy abgefangen und somit ist das Feld »SelectedEaID« für den Client frei wählbar. Für den Angriff wurden die Zahl 1 gesetzt. Abbildung 2 zeigt das Ergebnis einer manipulierten Anfrage. Die Kennlinie war für diesen Benutzer vorher nicht sichtbar.

Datenstromvorgänge für Energieanlagen

Status

Automatisch Geschlossen

Ziehen Sie eine Spaltenüberschrift hierher, um nach dieser Spalte zu gruppieren

Energieanlage	Gerät	Feld	Feldbereich	Status	Nachricht	Bearbeiter	Bemerkung	Klassifizierung	Anzahl von Erreignissen	Erste Zeitpunkt	Letzte Zeitpunkt
M5 Mittelweg 5	PC PT Nechlin	NE Nechlin	Mittelweg	Geschlossen	Fehlende Werte				17	01.06.2016 11:00	08.06.2016 11:45
K5 Kastanienweg 5	PC PT Nechlin	NE Nechlin	Kastanienweg	Geschlossen	Fehlende Werte				2	06.06.2016 08:40	08.06.2016 11:45
M4 Mittelweg 4	PC PT Nechlin	NE Nechlin	Mittelweg	Geschlossen	Fehlende Werte				1	06.06.2016 14:40	08.06.2016 11:45
E3 Erdmannsweg 3	PC PT Nechlin	NE Nechlin	Erdmannsweg	Geschlossen	Fehlende Werte				2	06.06.2016 08:10	08.06.2016 11:45
E2 Erdmannsweg 2	PC PT Nechlin	NE Nechlin	Erdmannsweg	Geschlossen	Fehlende Werte				1	06.06.2016 14:40	08.06.2016 11:45
M2 Mittelweg 2	PC PT Nechlin	NE Nechlin	Mittelweg	Geschlossen	Fehlende Werte				1	08.06.2016 08:50	08.06.2016 11:45
M3 Mittelweg 3	PC PT Nechlin	NE Nechlin	Mittelweg	Geschlossen	Fehlende Werte				1	08.06.2016 08:50	08.06.2016 11:45
B1 Bummlersruh 1	PC ENERCON Scada Nechlin	NE Nechlin	Bummlersruh	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:45
B2 Bummlersruh 2	PC ENERCON Scada Nechlin	NE Nechlin	Bummlersruh	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:45
K1 Kastanienweg 1	PC ENERCON Scada Nechlin	NE Nechlin	Kastanienweg	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:24
K2 Kastanienweg 2	PC ENERCON Scada Nechlin	NE Nechlin	Kastanienweg	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:24
K3 Kastanienweg 3	PC ENERCON Scada Nechlin	NE Nechlin	Kastanienweg	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:45
K4 Kastanienweg 4	PC ENERCON Scada Nechlin	NE Nechlin	Kastanienweg	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:45
M1 Mittelweg 1	PC ENERCON Scada Nechlin	NE Nechlin	Mittelweg	Geschlossen	Fehlende Werte				2	07.06.2016 13:38	08.06.2016 11:24
Z6 Zum UW 6	PC PT Nechlin	UM Uckermark	Zum UW	Geschlossen	Fehlende Werte				1	08.06.2016 09:50	08.06.2016 11:20

Einträge 1 - 27 von 27

Abbildung 1 Ergebnis nach Manipulation des ids-Feldes

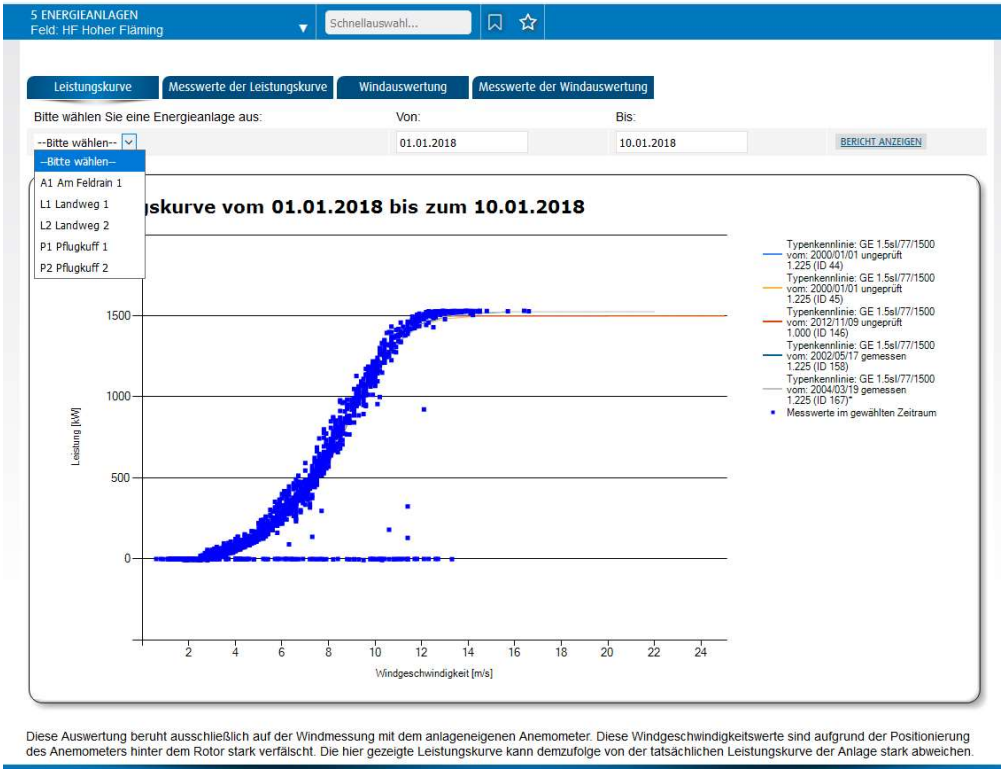
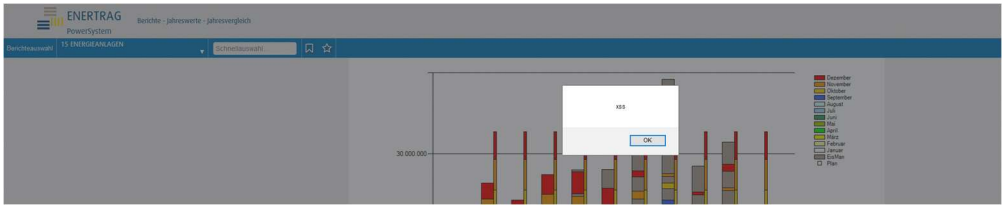


Abbildung 2 Kennlinie einer bestimmten Anlage

2.2 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

2.2.1 Filternamen

Für die Auswahl bestimmter Energieanlagen kann man einen frei wählbaren Filternamen (»Bookmark«) vergeben. Die Eingaben werden bei der späteren Auslieferung der Webseite nicht HTTP »output encoded«, somit befindet sich der Text später identisch in der Webseite. Als Name wurde »<script>alert('xss')</script>« gewählt. Im Anschluss an das Abschicken des Request wird die Seite neu geladen und das JavaScript-Tag ausgeführt. Dies wird ebenfalls ausgeführt, wenn man den Filternamen per Maus-Klick aktiviert. Die Alert-Box stellt hierbei nur ein Beispiel für einen erfolgreichen Angriff dar. Mögliche Angriffsvarianten sind Webseiten-Defacement oder auch Entführen der Benutzer-Session.



2.3 CWE-209: Information Exposure Through an Error Message

Im Falle von ungültigen Request werden unnötigerweise Systeminformation über die Fehlermeldungen dem Angreifer mitgeteilt. Für einen Angreifer sind dies hilfreiche Informationen um mehr Informationen über das System zu erlangen und weitere Angriffe vorzubereiten. Bei der PowerTrade-Plattform ist dies auch möglich:

[Technische Einzelheiten]

<pre class="errorText">System.ArgumentException: Ein ungültiges Array wurde übergeben. Erwartet wurde ",". (12): {"ids":[342',343,344,345,346,347,348,349,350],"from":"2015-06-30T22:00:00.000Z","to":"2017-07-31T21:59:59.000Z","units":0,"culture":"de-DE"}

bei System.Web.Script.Serialization.JavaScriptObjectDeserializer.DeserializeList(Int32 depth)

bei System.Web.Script.Serialization.JavaScriptObjectDeserializer.DeserializeInternal(Int32 depth)

bei System.Web.Script.Serialization.JavaScriptObjectDeserializer.DeserializeDictionary(Int32 depth)

bei System.Web.Script.Serialization.JavaScriptObjectDeserializer.DeserializeInternal(Int32 depth)

bei System.Web.Script.Serialization.JavaScriptObjectDeserializer.BasicDeserialize(String input, Int32 depthLimit, JavaScriptSerializer serializer)

bei System.Web.Script.Serialization.JavaScriptSerializer.Deserialize(JavaScriptSerializer serializer, String input, Type type, Int32 depthLimit)

bei PyWebApp.Util.CustomJsonValueProviderFactory.GetDeserializedObject(ControllerContext controllerContext)

bei PyWebApp.Util.CustomJsonValueProviderFactory.GetValueProvider(ControllerContext controllerContext)

bei System.Web.Mvc.ValueProviderFactoryCollection.GetValueProvider(ControllerContext controllerContext)

bei System.Web.Mvc.ControllerBase.get_ValueProvider()

bei System.Web.Mvc.ControllerActionInvoker.GetParameterValue(ControllerContext controllerContext, ParameterDescriptor parameterDescriptor)

bei System.Web.Mvc.ControllerActionInvoker.GetParameterValues(ControllerContext controllerContext, ActionDescriptor actionDescriptor)

bei System.Web.Mvc.Async.AsyncControllerActionInvoker.<>c__DisplayClass21.<BeginInvokeAction>b__19(AsyncCallback asyncCallback, Object asyncState)</pre>

2.4 CWE-602: Client-Side Enforcement of Server-Side Security

Durch Abfangen von Request und Manipulation des Zeitbereichs kann ein größerer Zeitbereich abgefragt und angezeigt werden als nur allein durch die Webseite möglich wäre. Die Abbildung 3 soll dies darstellen.

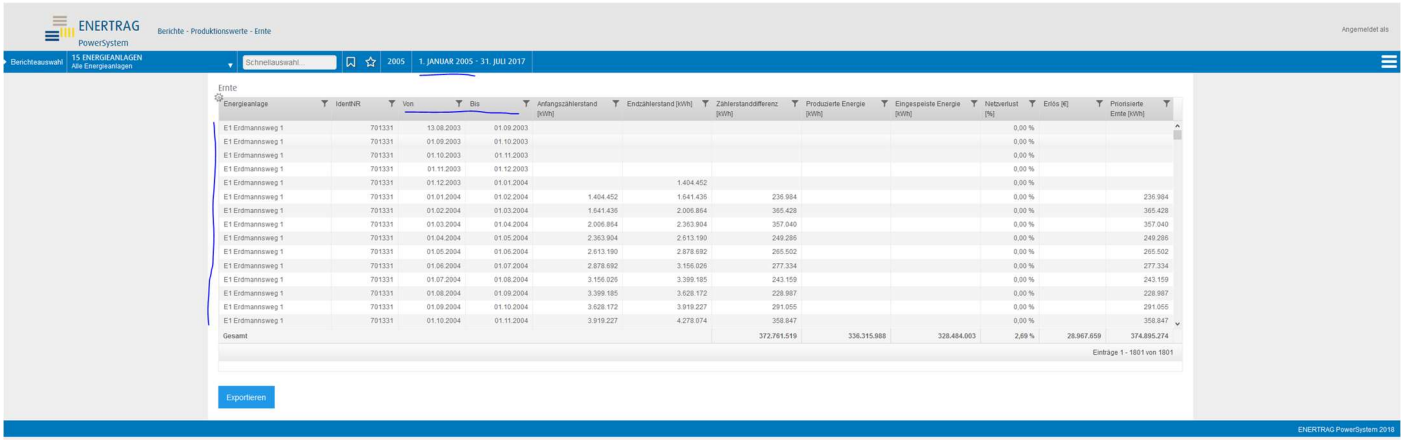


Abbildung 3 Manipulation des Zeitbereichs

3 Fazit

Im Rahmen der Sicherheitsanalyse wurden Teile der Webanwendung der PowerTrade Platform untersucht. In Kapitel 2 wurden die potentiellen Schwachstellen beschrieben und mit Hilfe von der CWE kategorisiert. Ob es sich hierbei um reale Schwachstellen handelt muss im Nachgang an diese Untersuchung durch Enertrag bewertet werden. Ein Penetrationstest ist am Ende des Entwicklungsprozesses angesiedelt und betrachtet nur spezielle Aspekte. Dieser Test erhebt daher kein Anspruch auf Vollständigkeit und war auch lediglich als erste Vorstufe gedacht.

Literaturverzeichnis

[1] P. Klimaabkommen, “Ubereinkommen von Paris,” 2015, https://www.bmu.de/fileadmin/Daten_BMU/Download_PDF/Klimaschutz/paris_abkommen_bf.pdf.

[2] N. Höhne, M. Hagemann, and H. Fekete, “Zwei neue Klimaschutzziele für Deutschland,” 2020.

[3] J. Albersmann, D. Bahn, I. Baum, S. Farin, T. Fecht, R. Reuter, and T. Stiefelhagen, “Virtuelle Kraftwerke als wirkungsvolles Instrument für die Energiewende,” *PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft*, 2012.

[4] BSI, “Die lage der IT-Sicherheit in Deutschland 2020,” *Bundesamt für Sicherheit in der Informationstechnik*, 2020.

[5] D. Bundestag, “Gesetzt zur Stärkung der Sicherheit in der Informationstechnik des Bundes,” *Bundesgesetzblatt Bonn*, p. 2821, 2009.

[6] BSI, “ICS-Security-Kompendium,” *Bundesamt für Sicherheit in der Informationstechnik*, 2013.

[7] VGB PowerTech e.V., “IT-Sicherheit für Erzeugungsanlagen,” *Verlag technisch-wissenschaftlicher Schriften*, 2014.

[8] V. e.V., “VHPready 4.0 - Virtual Power Plant Communication Path between Control Center and Distributed Energy Resource,” *Industry Alliance VHPready e.V.*, 2017.

[9] V. Hammer, *Zentrale Bausteine der Informationssicherheit*. Web-Site-Verlag, 2014.

[10] C. Wiemers, “Informationssicherheit erhöhen mit dem modernisierten IT-Grundschutz: Ein Überblick,” *Bundesamt für Sicherheit in der Informationstechnik*, 2017.

[11] BSI, “BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS),” *Bundesamt für Sicherheit in der Informationstechnik*, 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.html.

[12] ——, “BSI-Standard 200-2 IT-Grundschutz-Methodik,” *Bundesamt für Sicherheit in der Informationstechnik*, 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.html.

[13] ——, “BSI-Standard 200-3 Risikoanalyse auf Basis von IT-Grundschutz,” *Bundesamt für Sicherheit in der Informationstechnik*, 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html.

[14] Deutschland, Ed., *Notfallmanagement: BSI-Standard 100-4 zur Business Continuity*, version 1.0 ed., ser. Praxiswissen Professionals. Köln: Bundesanzeiger, 2009, oCLC: 254622228.

[15] J. Nagel, *Energie-und Ressourceninnovation: Wegweiser zur Gestaltung der Energiewende*. Carl Hanser Verlag GmbH Co KG, 2017.

[16] K. Irlbeck, Maximilian, “Die E-Energy Referenzarchitektur,” 2015.

[17] J. Hartmann, “IT-Sicherheit virtueller Kraftwerke,” Master’s thesis, Hochschule Hannover, 2018.

[18] 50Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, and TransnetBW GmbH, “Mindestanforderungen an die Informationstechnik des Reservenanbieters zur Erbringung von Regelreserve,” https://www.regelleistung.net/ext/static/srl/it, 2020.

[19] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, “Leitfaden zum Einspeisemanagement,” https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/ErneuerbareEnergien/Einspeisemanagement/einspeisemanagement-node.html, 2018.

[20] I.-G. Kompendium, “Bundesamt für Sicherheit in der Informationstechnik (BSI),” *BSI*, 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium.

[21] D. L. Mills *et al.*, “Network time protocol (NTP),” *Internet RFC 958, Network Information Center*, 1985.

[22] BSI, “Ein Praxis-Leitfaden für IS-Penetrationstests,” *Bundesamt für Sicherheit in der Informationstechnik*, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.html.

[23] ——, “Ein Praxis-Leitfaden für den IS-Webcheck,” *Bundesamt für Sicherheit in der Informationstechnik*, 2020, https://www.bsi.bund.de.

[24] J. Grossman, S. Fogie, R. Hansen, A. Rager, and P. D. Petkov, *XSS attacks: cross site scripting exploits and defense*. Syngress, 2007.

[25] M. S. Siddiqui and D. Verma, “Cross site request forgery: A common web application weakness,” in *2011 IEEE 3rd International Conference on Communication Software and Networks*. IEEE, 2011, pp. 538–543.

[26] J. Clarke-Salt, *SQL injection attacks and defense*. Elsevier, 2009.

[27] G. Hoglund and G. McGraw, *Exploiting software: How to break code*. Pearson Education India, 2004.

[28] J. Neystadt, “Automated penetration testing with white-box fuzzing,” *Microsoft, February*, 2008.

[29] S. Herzog, “Xml external entity attacks (xxe),” *Retrieved October*, vol. 13, p. 2013, 2010.

[30] A. Bonguet and M. Bellaiche, “A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing,” *Future Internet*, vol. 9, no. 3, p. 43, 2017.

[31] M. McIntosh and P. Austel, “XML signature element wrapping attacks and countermeasures,” in *Proceedings of the 2005 workshop on Secure web services*, 2005, pp. 20–27.

[32] F. Yihunie, E. Abdelfattah, and A. Odeh, “Analysis of ping of death DoS and DDoS attacks,” in *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2018, pp. 1–4.

[33] K. Beckers and S. Pape, “A serious game for eliciting social engineering security requirements,” in *2016 IEEE 24th International Requirements Engineering Conference (RE)*. IEEE, 2016, pp. 16–25.

[34] P. S. Ryan, “War, peace, or stalemate: Wargames, wardialing, wardriving, and the emerging market for hacker ethics,” *Va. JL & Tech.*, vol. 9, p. 1, 2004.

[35] M. Raza, M. Iqbal, M. Sharif, and W. Haider, “A survey of password attacks and comparative analysis on methods for secure authentication,” *World Applied Sciences Journal*, vol. 19, no. 4, pp. 439–444, 2012.

[36] A. A. Younis, Y. K. Malaiya, and I. Ray, “Using attack surface entry points and reachability analysis to assess the risk of software vulnerability exploitability,” in *2014 IEEE 15th International Symposium on High-Assurance Systems Engineering*. IEEE, 2014, pp. 1–8.

[37] E. Biham, “New types of cryptanalytic attacks using related keys,” *Journal of Cryptology*, vol. 7, no. 4, pp. 229–246, 1994.

[38] J. Long, *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*. Syngress, 2011.