UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

FB 4
Informatik

Entwurf eines Common Criteria-Schutzprofils für Router zur Abwehr von Online-Überwachung

Tobias Kippert
Anastasia Meletiadou
Rüdiger Grimm

Nr. 5/2009

Arbeitsberichte aus dem Fachbereich Informatik

Universität Koblenz-Landau • Campus Koblenz • Universitätsstraße 1 • 56070 Koblenz
Telefon +49 261 287-0 • http://www.uni-koblenz.de

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Zöbel

Kontaktdaten der Verfasser

Tobias Kippert, Anastasia Meletiadou, Rüdiger Grimm
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: kippert@uni-koblenz.de; nancy@uni-koblenz.de, grimm@uni-koblenz.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1

PP-Einführung

1.1 PP-Referenz

PP-Titel:	Vorgeschlagenes Common Criteria-Schutzprofil für Router zur Abwehr von Online-Überwachung
PP-Version:	1.0
Autor:	Tobias Kippert
Datum:	30. April 2009
CC-Version:	3.1 Release 2

1.2 EVG-Übersicht

Bei dem für dieses Schutzprofil (engl. „Protection Profile“ im Folgenden PP genannt) herangezogenen Evaluationsgegenstand (im Folgenden EVG genannt) handelt es sich um einen Router, der einen Schutz gegen Online-Überwachung bietet. Der EVG-Typ ist hierbei ein handelsüblicher Internet-Router, der in Privathaushalten und kleineren Firmen eingesetzt wird. Der EVG umfasst den gesamten Router, so dass sowohl die Hardwarekomponenten als auch die Softwarekomponenten betrachtet werden. Es ist dabei irrelevant, ob es ein Modell mit integriertem Breitband-Modem ist oder ob dieses separat angeschlossen ist.
Der EVG dient zum Anschluss mehrerer Client-Rechner über ein LAN (Local Area Network) oder über WLAN (Wireless LAN). Um dieses zu realisieren verfügt der EVG über Network Address Translation (NAT). Darüber hinaus kann der EVG über eine integrierte Firewall abgesichert werden, in der Port-Filterungen definiert werden können. Dieses sind die Hauptbestandteile des EVG, die für die gemeinsame Nutzung eines Breitbandanschlusses durch mehrere Clients notwendig sind. Manche Router werden zusätzlich mit

Funktionen für Telefonie ausgestattet. Diese sind jedoch für den betrachteten EVG irrelevant und werden daher nicht berücksichtigt.
In diesem PP werden funktionale Sicherheitsanforderungen für einen EVG aufgestellt, die den Gefahren der Online-Überwachung entgegenwirken sollen. So sollen die grundlegende Analyse, die Einbringung einer Remote Forensic Software (RFS) und die darauf aufbauende Durchführung der Online-Überwachung eines Zielsystems verhindert werden.
Zur Analyse eines Zielsystems zählen unter anderem folgende Punkte:

- Das verwendete Betriebssystem mit Angaben über Hersteller, Version und Patch-Stand
- Der Internet-Zugang mit Informationen über Provider und Zugangsart (Einwahl oder DSL)
- Auf dem Zielsystem eingesetzte Schutzsoftware wie Virenscanner, Personal Firewall, Spywareprogramme, Verschlüsselungssoftware mit den jeweiligen Versionsständen
- Aktuelle Sicherheitskonfiguration, die unter anderem Aufschluss darüber gibt, welche Rechte der angemeldete Nutzer auf dem Zielsystem hat und wie die Schutzsoftware konfiguriert ist
- Benutzte Kommunikationsdienste mit verwendeter Software und Versionsangaben wie zum Beispiel Browser oder E-Mail-Client

Die Infiltration einer Online-Überwachung kann auf unterschiedliche Weise erfolgen.

Automatische Hintergrund-Installation Die RFS gelangt durch die Installation eines Trojaners auf einen Computer. Dieser Trojaner kann entweder durch einen Internet-Download oder über externe Datenträger auf den Computer gelangen. Der Benutzer unterstützt hierbei unbewusst den Installationsvorgang.

Manuelle Installation Hierfür ist ein physischer Zugriff auf den Computer, der online überwacht werden soll, notwendig, wobei die RFS installiert wird. Dieser Zugriff erfolgt durch den Angreifer selbst.

Entfernte manuelle Installation Die Online-Überwachung kann auf Grund einer Schwachstelle im System durchgeführt werden. Auch bei dieser Angriffsmethode agiert der Angreifer selbst.

Die RFS hat laut [BMI, 2007] und [BMI2, 2007] folgende Leistungsmerkmale:

- Durchführung einer Systemanalyse zur Gewinnung von Informationen über Betriebssystem, installierte Programme, Leistungsmerkmale, Benutzeraccounts, etc. sowie den Zugriff auf Systemeinstellungen des Computers.
- Erstellung einer Verzeichnisübersicht mit anschließender Durchsuchung der Verzeichnisse sowie Volltextsuche nach Stichworten.

- Erkennung von externen Datenspeichern und Durchsuchung dieser. Die externen Datenspeicher können sowohl direkt an Clients angeschlossen sein, als auch über das lokale Netzwerk zugreifbar sein.
- Herunterladen von ausgewählten Dokumenten.
- Mitschneiden von Tastaturanschlägen mit Hilfe eines Tastatur-Loggers.
- Selbstständige Entfernung der RFS bei Beendigung der Maßnahme durch eine Deaktivierung per Remotezugriff sowie Löschung entstandener Spuren.
- Automatische Deaktivierung nach einer bestimmten Zeit (meist richterlich vorgegeben).

Der EVG soll mit Hilfe dieses PPs so abgesichert werden können, dass eine Online-Überwachung nicht möglich ist. Hierfür können folgende generelle Sicherheitserwartungen an den EVG aufgestellt werden:

- Der EVG prüft Passwörter auf deren Sicherheit
- Der EVG schützt vor der Gefahr des Abhörens von Datenverkehr
- Der EVG kontrolliert den Zugang zum internen Netzwerk
- Der EVG kontrolliert den Zugang zum EVG-Konfigurationsmenü

In diesem PP werden funktionale Sicherheitsanforderungen aufgestellt, so dass der EVG gegen die oben dargestellte Funktionsweise und die damit verbundenen Maßnahmen abgesichert werden kann.

1.3 EVG-Umgebung

Der EVG wird in ein Netzwerk eingebunden, wie es beispielhaft in Abbildung 1.1 dargestellt ist. Der EVG ist über einen Breitband-Internetanschluss mit einem Internet Service Provider (ISP) verbunden. An den EVG können Clients angeschlossen werden, die zusammen ein internes Netzwerk bilden. Diese Clients können entweder per LAN-Kabel oder per WLAN-Verbindung an den EVG angeschlossen werden. An die Clients können zur Erweiterung des Speichers bzw. zur Portabilität von Daten externe Festplatten angeschlossen werden. Die Clients werden von Benutzern bedient. Diese Benutzer kommunizieren mit den Clients über den EVG mit dem Internet. Ein oder mehrere Benutzer können administrative Rollen übernehmen. Hierfür können sie mit einem Client auf das Konfigurationsmenü des Routers zugreifen, um Einstellungen am EVG vorzunehmen.
Die Komponenten dieser EVG-Umgebung können jeweils auf der Grundlage anderer PPs entwickelt sein. Beispielhaft hierfür wäre ein PP für Webbrowser.

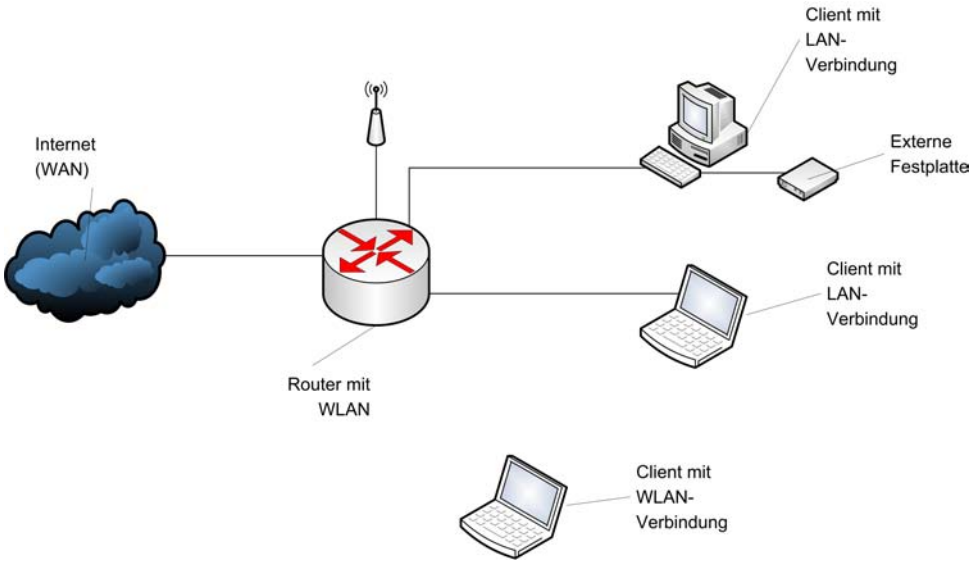

Abbildung 1.1: EVG-Umgebung.

1.4 Abkürzungen und Glossar

Client an ein Netzwerk angeschlossener Rechner

DHCP Dynamic Host Configuration Protocol

EAL Evaluation Assurance Level

EVG Evaluationsgegenstand (=TOE)

EVG-Konfigurationsmenü Konfigurationsmenü eines Routers, in dem Einstellungen vorgenommen werden

Externes Netzwerk z.B. Internet, WAN

Instant Messaging-Dienst Dienst zur Übertragung von Textnachrichten zwischen zwei Teilnehmern

Internes Netzwerk LAN bzw. WLAN (=Lokales Netzwerk)

IP-Adresse Eindeutige Adresse eines Internetanschlusses (extern) bzw. eines Clients (intern)

IP-Konfiguration Konfiguration zur Anbindung an ein lokales Netzwerk; enthält IP-Adresse, Gateway, DNS-Server, Subnetzmaske

ISP Internet Service Provider

LAN Local Area Network

Lokales Netzwerk Mehrere Clients, die über ein Gateway (Router) mit dem WAN verbunden sind. Ihre IP-Adressen liegen im gleichen von der Subnetzmaske festgelegten Adressraum.

NAT Network Address Translation

PP Protection Profile (=Schutzprofil)

RFS Remote Forensic Software

SAR Security Assurance Requirements

SFP Security Functional Policies

SFR Security Functional Requirements

SSID Service Set Identifier, Kennung eines WLAN

ST Security Target

TOE Target Of Evaluation (=EVG)

TSF TOE Security Functions

WAN Wide Area Network, Netzwerk über große Distanzen, z.B. Internet

WLAN Wireless Local Area Network, kabelloses LAN

WPA / WPA2 Wi-Fi Protected Access (2), Verschlüsselungsmethoden für WLAN

Kapitel 2

Postulate zur Übereinstimmung

Dieses PP postuliert Übereinstimmung mit CC Version 3.1 Release 2.

Dieses PP ist CC Part 2 **conformant**.

Die in Teil 2 der CC in englischer Sprache definierten funktionalen Anforderungen wurden nach bestem Wissen ins Deutsche übersetzt. Bezogen auf die Konformität zu Teil 2 der CC gilt im Zweifelsfall die englische Originalfassung.

Dieses PP ist CC Part 3 **conformant**.

Dieses PP ist EAL 3 **conformant**.

Dieses PP verlangt **strict conformance**.

Kapitel 3

Definition des Sicherheitsproblems

Bei der Definition des Sicherheitsproblems werden die Sicherheitsaspekte der Umgebung, in welcher der EVG eingesetzt werden soll, und die Sicherheitsaspekte des EVG beschrieben. Hierzu zählen die Bedrohungen, die sich sowohl gegen den EVG selbst als auch gegen die Umgebung richten, die Anforderungen an die organisatorische Sicherheitspolitik, die Richtlinien für die Sicherheit definieren, und die Annahmen, die für die Umgebung des EVG gelten müssen und für den Einsatz des EVG vorausgesetzt werden.
Für die Beschreibung des Sicherheitsproblems werden grundlegend die zu schützenden Werte (Assets) und Subjekte definiert:

- Zu schützende Werte
  - Authentifikationsdaten
    - Clients
    - WLAN
    - EVG-Konfigurationsmenü
  - Gespeicherte Daten auf Clients
  - Konfigurationsdaten im EVG-Konfigurationsmenü
  - im lokalen Netzwerk und über das Internet gesendeter Datenverkehr
  - Zugang zum internen Netzwerk nur für erlaubte Clients
- Subjekte
  - Benutzer eines Clients
  - Benutzer mit Administrationsrechten für EVG
  - Angreifer
    - Angreifer im lokalen Netzwerk
    - Angreifer im externen Netzwerk
    - Angreifer ohne Netzwerkmitgliedschaft
    - Angreifer mit physischem Zugriff auf Client

3.1 Bedrohungen

Bei einer Bedrohungsanalyse wurden die Bedrohungen gegen die zu schützenden Werte ermittelt. Bedrohungen werden durch ihren Urheber, die Angriffe und die angegriffenen Werte beschrieben.
Für die folgende Beschreibung von Bedrohungen werden Kriterien zur Definition einer Bedrohung benutzt:

Motivation Beschreibt das Ziel des Angriffes.

Ausgenutzte Schwachstelle Die ausgenutzte Schwachstelle beschreibt die möglichen Zugangspunkte eines Angriffes.

Angegriffener Wert Der angegriffene Wert bezieht sich auf die in der Einleitung zu diesem Kapitel definierten zu schützenden Werte.

Angreifermethode Ein Angriff wird als direkt bezeichnet, wenn der Angreifer durch dessen erfolgreiche Ausführung sein endgültiges Ziel erreicht.

Gelegenheit Ein Angriff wird als aktiv bezeichnet, wenn der Angriffszeitpunkt durch den Angreifer bestimmt werden kann, indem er aktiv ins Geschehen eingreift. Reines Mitlesen von Nachricht gilt als passiver Angriff.

Die Bedrohungen werden mit einem vorangestellten **T.** bezeichnet. Das T steht hierbei für das englische „Threat“ , was auf deutsch Bedrohung bedeutet.

T.Protokoll Sicherheitsrelevante Ereignisse werden nicht protokolliert.

Motivation Angriffsversuche bleiben unentdeckt.

Ausgenutzte Schwachstelle Firewall, EVG-Firmware, EVG-Konfiguration

Angegriffener Wert alle zu schützenden Werte

Angreifermethode indirekt

Gelegenheit aktiv

T.Abhören Über das WLAN ausgesandter Datenverkehr kann mitgelesen werden.

Motivation Angreifer möchte sensible Daten aus dem Datenverkehr mitlesen. So können zum Beispiel Passwörter erlangt werden oder ganze Kommunikationen belauscht werden.

Ausgenutzte Schwachstelle WLAN, EVG-Firmware, EVG-Konfiguration

Angegriffener Wert Gespeicherte Daten auf Clients, Datenverkehr

Angreifermethode direkt

Gelegenheit passiv

T.SSID Einem Angreifer wird wegen sichtbarer Ausstrahlung des WLAN-Namens (SSID) bzw. durch Auswahl einer Standard-SSID ein Angriff auch das WLAN erleichtert. Durch die Auswahl einer Standard-SSID kann eventuell auf das Passwort für das EVG-Konfigurationsmenü geschlossen werden.

Motivation Der Angreifer kann das WLAN-Netz lokalisieren und auffinden. Darauf aufbauend kann er weitere Angriffe durchführen.

Ausgenutzte Schwachstelle WLAN, EVG-Konfiguration

Angegriffener Wert Authentifikationsdaten WLAN

Angreifermethode indirekt

Gelegenheit passiv

T.KonfExt Das Konfigurationsmenü des EVG kann aus dem externen Netzwerk (WAN) über die externe IP-Adresse des Routers erreicht und aufgerufen werden. Diese Möglichkeit erweitert die Angriffsmöglichkeiten, da ein Angreifer im externen Netzwerk bei Kenntnis der IP-Adresse des Routers ortsunabhängig Angriffsversuche auf das EVG-Konfigurationsmenü starten kann. Die Möglichkeit zur Konfiguration des EVG aus dem internen Netzwerk ist ausreichend, weil Änderungen der Router-Eigenschaften von außerhalb des internen Netzwerkes hier als nicht zwingend notwendig angesehen werden.

Motivation Angreifer im externen Netzwerk (WAN) wollen sich Zugang zum EVG-Konfigurationsmenü verschaffen, um Einstellungen zu ändern, so dass sie zum Beispiel Zugang zum internen Netzwerk über WLAN erlangen.

Ausgenutzte Schwachstelle EVG-Konfigurationsmenü, Firewall

Angegriffener Wert Authentifikationsdaten EVG-Konfigurationsmenü, Konfigurationsdaten im EVG-Konfigurationsmenü

Angreifermethode direkt

Gelegenheit aktiv

T.KonfInt Unautorisierte Benutzer können im internen Netzwerk das EVG-Konfigurationsmenü aufrufen.

Motivation Einstellungen können im EVG-Konfigurationsmenü verändert werden, so dass sie nicht mehr der geforderten Sicherheit entsprechen.

Ausgenutzte Schwachstelle EVG-Firmware, EVG-Konfigurationsmenü

Angegriffener Wert Authentifikationsdaten EVG-Konfigurationsmenü, Konfigurationsdaten im EVG-Konfigurationsmenü

Angreifermethode direkt

Gelegenheit aktiv

T.DHCP Unautorisierte Clients im internen Netzwerk (LAN oder WLAN) bekommen durch den EVG automatisch Konfigurationsdaten zugewiesen.

Motivation So angeschlossene Clients sind Mitglieder des internen Netzwerkes.

Ausgenutzte Schwachstelle EVG-Konfiguration

Angegriffener Wert Exklusivität des Zugangs zum internen Netzwerk

Angreifermethode indirekt

Gelegenheit passiv

T.NAT Ein sich im internen Netzwerk befindlicher Client kann aus dem externen Netzwerk (WAN) direkt adressiert und erreicht werden.

Motivation Angreifer können Zielsystem direkt angreifen.

Ausgenutzte Schwachstelle EVG-Konfiguration, Firewall

Angegriffener Wert Gespeicherte Daten auf Clients

Angreifermethode direkt

Gelegenheit aktiv

T.Firewall Der EVG besitzt keine Firewall oder diese ist nicht aktiviert.

Motivation EVG filtert keine Zugriffe aus dem externen Netzwerk (WAN) zum internen Netzwerk.

Ausgenutzte Schwachstelle EVG-Firmware, EVG-Konfiguration, Firewall

Angegriffener Wert Exklusivität des Zugangs zum internen Netzwerk

Angreifermethode indirekt

Gelegenheit passiv

T.Backdoor Es existiert eine Backdoor, die werkseitig in die Software oder Hardware des EVG eingebaut wurde, um eine Online-Überwachung zu ermöglichen bzw. zu vereinfachen.

Motivation Es werden bereits werkseitig Vorbereitungen für eine Online-Überwachung getroffen.

Ausgenutzte Schwachstelle nicht relevant, jeder Teil des EVG kann grundsätzlich für eine Backdoor missbraucht werden

Angegriffener Wert Authentifikationsdaten WLAN, Authentifikationsdaten EVG-Konfigurationsmenü, Konfigurationsdaten im Konfigurationsmenü, Datenverkehr, Exklusivität des Zugangs zum internen Netzwerk

Angreifermethode indirekt

Gelegenheit passiv

3.2 Organisatorische Sicherheitspolitik

Die organisatorische Sicherheitspolitik gibt die Politiken und Regeln an, die der EVG und seine Umgebung erfüllen müssen. Sie werden von der Organisation, in der sich der EVG und seine Umgebung befinden, festgelegt. Die Regeln der organisatorischen Sicherheitspolitik werden mit einem vorangestellten **P.** bezeichnet. Das P steht hierbei für das englische „Policy“ , was auf deutsch Richtlinie bedeutet.

P.Update Die Firmware des EVG muss ständig auf den aktuellen Stand gebracht werden.

P.sicherePW Der EVG akzeptiert nur ein sicheres Passwort für das Konfigurationsmenü. Das Passwort muss auf seine Sicherheit überprüft und darf nur bei bestandener Prüfung akzeptiert werden.

3.3 Annahmen

Die Definition von Annahmen beinhaltet die Beschreibung der Voraussetzungen an die EVG-Umgebung, die stets erfüllt sein müssen. Diese Annahmen betreffen alle Maßnahmen, die etwas zur IT-Sicherheit beitragen, aber nicht vom EVG erfüllt werden können. Aus diesem Grund werden sie an die EVG-Umgebung gerichtet. Ohne die Annahmen ist die EVG-Sicherheitsleistung beeinträchtigt, und somit ist jede einzelne Annahme eine Voraussetzung für die Wirksamkeit der Sicherheitsfunktionen. Die Annahmen werden mit einem vorangestellten **A.** bezeichnet. Das A steht hierbei für das englische „Assumption“ was auf deutsch Annahme bedeutet.

A.OSAuth Die Clients werden bei Nichtbenutzung immer vor fremden Zugriff geschützt oder ganz ausgeschaltet. Dieses kann durch ein Passwort oder durch ein biometrisches Merkmal geschehen. Auch die Benutzung eines Clients überhaupt kann nur durch vorherige Authentifikation erfolgen.

A.UserSensib Mit den Authentifikationsdaten wird sorgsam umgegangen. Unter den autorisierten Benutzern wird verbreitet, dass es sich bei den Authentifikationsdaten um sensible Daten handelt, und dass diese Daten geschützt werden müssen.

A.ZugriffEVG Der EVG ist so aufzustellen, dass nur autorisierte Benutzer physischen Zugang zu ihm haben. Unautorisierte Personen dürfen niemals physischen Zugriff auf den EVG haben.

A.ZugriffLAN Die LAN-Ports des EVG bzw. die in den Räumlichkeiten verlegten LAN-Anschlussdosen sind nur autorisierten Benutzern zugänglich. Die Benutzer müssen erkennen, dass diese Anschlüsse geschützt und beobachtet werden müssen.

A.Updateclient Auf jedem eingesetzten Client im System ist aktuelle Sicherheitssoftware installiert. Unter Sicherheitssoftware wird hier ein Programm gegen Viren und eine Personal Firewall verstanden. Die Konfiguration dieser Software ist korrekt erfolgt. Alle Dateien werden von der Sicherheitssoftware untersucht und fortlaufend kontrolliert. Die Sicherheitssoftware wird durch Updates immer auf dem aktuellsten Stand gehalten.

A.FreigabeAuth Im internen Netzwerk freigegebene Ordner dürfen nur autorisierten Benutzern zur Verfügung stehen. Der Schutz durch ein Authentifizierungsmerkmal wie ein Passwort wird verlangt.

A.extDatenträger Den Benutzern muss klar sein, dass von externen Datenträgern wie CDs, DVDs, USB-Sticks, etc. eine potentielle Gefahr ausgeht. Diese dürfen nicht leichtgläubig benutzt werden. Auch die Herkunft der Datenträger muss vertrauenswürdig sein. Die Benutzer müssen hierfür sensibilisiert werden.

A.Downloads Downloads aus dem Internet dürfen nur von vertrauenswürdigen Servern erfolgen. Auch das Herunterladen und Ausführen von Dateianhängen an E-Mails darf nur bei geprüfter Vertrauenswürdigkeit erfolgen. Dasselbe gilt für zugeschickte Dateien über Instant Messaging-Dienste. Die Benutzer müssen hierfür sensibilisiert werden.

A.ISP Die Anbindung des EVG an ein WAN wird als sicher angesehen. Der ISP behandelt Daten über die Einwahl ins Internet und über das Kommunikationsverhalten vertraulich und gibt sie nicht an Dritte weiter. Der ISP sorgt dafür, dass sein eigenes Netzwerk sicher ist.

A.BackdoorClient Es werden von Herstellern von Software und Hardware, die der Client verwendet, keine Backdoors fabrikseitig eingebaut, so dass hierdurch eine Durchführung einer Online-Überwachung ermöglicht bzw. erleichtert wird. Hierzu zählen auch Updates und Patches.

A.Admin Nur qualifizierte Personen administrieren den EVG.

A.AdminModus Der Betrieb der Clients erfolgt nicht in einem ständigen Administratormodus. Eine Installation eines Programmes darf nicht ohne explizite Zustimmung des Benutzers erfolgen.

Kapitel 4

Sicherheitsziele

Die Sicherheitsziele sind präzise und abstrakte Formulierungen, die sich auf die beabsichtigte Lösung des Sicherheitsproblems beziehen. Hierbei werden die Sicherheitsziele in Sicherheitsziele für den EVG und in Sicherheitsziele für die EVG-Umgebung unterteilt. Um alle Bedrohungen, organisatorischen Sicherheitspolitken und Annahmen abzudecken, muss jede von ihnen mit mindestens einem Sicherheitsziel verknüpft sein. Diesen Nachweis bringt die Erklärung der Sicherheitsziele.

4.1 Sicherheitsziele für den EVG

Die Sicherheitsziele für den EVG können nur mit den Bedrohungen und den organisatorischen Sicherheitspolitken verknüpft werden. Sie beziehen sich direkt auf den EVG. Die Sicherheitsziele für den EVG werden mit einem **O.** bezeichnet. Dieses steht für das englische „Objective“ , was auf deutsch Ziel bedeutet.

O.KonfExt Das EVG-Konfigurationsmenü lässt sich nur aus dem internen Netzwerk aufrufen. Ein Aufrufversuch aus dem externen Netzwerk wird verhindert.

O.KonfPW Das EVG-Konfigurationsmenü ist durch ein sicheres, individuelles Passwort geschützt. Dieses wird entweder zufällig ab Werk eingestellt, oder der Benutzer muss dieses bei erstmaliger Konfiguration des EVG selbst vergeben. Hierbei muss darauf geachtet werden, dass es sich um ein sicheres Passwort handelt. Damit sichergestellt wird, dass nur sichere Passwörter verwendet werden, prüft der EVG diese auf ihre Sicherheit. Ein sicheres Passwort besteht aus einer Mischung von Ziffern und Buchstaben und hat mindestens acht Zeichen. Die Einstellung eines unsicheren Passwortes wird verweigert.

O.Firewall Der EVG blockiert unzulässigen, nicht explizit freigegebenen Datenverkehr aus dem externen Netzwerk durch eine Firewall. Die EVG-Firewall ist nach sicherheitsrelevanten Aspekten konfiguriert. Unter sicherheitsrelevanten Aspekten ist hier zu verstehen, dass nur erlaubte Kommunikation explizit freigegeben wird. Hierzu zählen erlaubte Ports, die für die jeweiligen IP-Adressen der Clients individuell

angepasst werden, so dass sichergestellt wird, dass nur erwünschte Kommunikationsflüsse erlaubt werden.

O.Abhören Der EVG verhindert das unautorisierte Abhören des WLAN-Datenverkehrs. (Hinweis: Für die Verschlüsselung und Authentizität könnte WPA oder WPA2 eingesetzt werden. Die Größe des kryptografischen Schlüssels liegt zwischen 8 und 63 Zeichen.)

O.WLANSSID Der EVG unterbindet die Ausstrahlung des Namen des WLAN (SSID).

O.IPKonf Der EVG bedient angeschlossene Clients nur bei statischer IP-Konfigu-ration. Jeder Client muss die IP-Konfiguration kennen und sich eine der Subnetzmaske entsprechenden IP-Adresse statisch zuweisen.

O.Intern Der EVG verschleiert die internen IP-Adressen der angeschlossenen Clients, so dass diese nicht aus dem externen Netzwerk direkt adressiert werden können.

O.Backdoor Alle Funktionen des EVG müssen vom Benutzer transparent einsehbar sein. Hierzu muss eine vollständige Dokumentation der EVG-Funktio-nen für den Benutzer erfolgen.

O.Protokoll Der EVG erkennt sicherheitsrelevante Ereignisse und protokolliert diese. Die Protokollierung muss zur Transparenz der EVG-Funktionen beitragen.

O.Update Der EVG muss eine Update-Funktion anbieten.

4.2 Sicherheitsziele für die EVG-Umgebung

Die Sicherheitsziele für die EVG-Umgebung können mit den Bedrohungen, den organisatorischen Sicherheitspolitiken und den Annahmen verknüpft werden. Sie beziehen sich nur auf die EVG-Umgebung. Die Sicherheitsziele für die EVG-Umgebung werden mit **OE.** bezeichnet. Dieses steht für die englischen Wörter „Objective“ und „Environment“ die auf deutsch Ziel und Umgebung bedeuten.

OE.OSAuth Das Betriebssystem der Clients bietet die Möglichkeit den Client mit einem Passwort oder durch Nachweis eines biometrischen Merkmals vor Fremdbenutzung abzusichern.

OE.UserSensib Die Benutzer müssen für den empfindlichen Umgang mit Authentifikationsdaten sensibilisiert werden. Generell müssen die Benutzer über mögliche Gefahren aufgeklärt werden.

OE.ZugriffEVG Die Umgebung muss den physischen Zugriff auf den EVG beobachten und verhindern.

OE.ZugriffLAN Die Umgebung muss den physischen Zugriff zu den LAN-Ports beobachten und für unautorisierte Personen verhindern.

OE.Updateclient Das Betriebssystem und die Sicherheitssoftware auf den Clients entsprechen immer dem aktuellsten Sicherheitsstandard. Dies wird durch regelmäßige Updates und Patches sichergestellt. (Hinweis: Das Update des EVG wird durch O.Update abgedeckt.)

OE.FreigabeAuth Netzwerkfreigaben müssen mit einem Passwort geschützt werden, so dass sie nur durch vorherige Authentifikation zugreifbar werden.

OE.extDatenträger Benutzer müssen vor der Benutzung externer Datenträger (USB-Sticks, CDs, DVDs, etc.) diese auf ihre Sicherheit und Herkunft prüfen und dürfen diese gegebenenfalls nicht verwenden.

OE.Downloads Benutzer müssen vor dem Download von Servern diese auf ihre Sicherheit und Vertrauenswürdigkeit prüfen und dürfen diese gegebenenfalls nicht verwenden.

OE.ISP Der ISP hat die Daten der Kunden vertraulich zu behandeln und sein Netzwerk gegen feindliche Angriffe abzusichern.

OE.BackdoorClient Die verwendete Hardware und Software der Clients verfügt nicht über absichtlich eingebaute Sicherheitslücken.

OE.Admin Ein EVG-Administrator verfügt über eine angemessene Qualifikation und verwaltet Einstellungen im EVG und seiner Umgebung nur zu Gunsten der Sicherheit.

OE.AdminModus Die Clients werden mit einem Benutzer ohne Administratorrechte ausgeführt. Bei Veränderungen am System muss der Benutzer entweder vorübergehend in den Administratormodus wechseln oder muss die Veränderungen explizit zulassen.

4.3 Erklärung der Sicherheitsziele

Die Erklärung der Sicherheitsziele weist nach, dass alle in der Sicherheitsumgebung definierten Aspekte durch die Sicherheitsziele identifiziert werden, zurückverfolgbar sind und durch diese abdeckbar sind. Sowohl für jedes Sicherheitsziel für den EVG als auch für jedes Sicherheitsziel für die EVG-Umgebung wird angegeben, welche Bedrohungen abgewehrt, welche organisatorischen Sicherheitspolitiken beachtet und welche Annahmen abgedeckt werden. Der Zusammenhang zwischen dem Sicherheitsproblem und den Sicherheitszielen verdeutlicht Abbildung 4.1 [CCT1, 2006].
Nach den Erklärungen für die einzelnen Bereiche des Sicherheitsproblems werden jeweils in tabellarischer Form die Nachweise erbracht, dass jede Bedrohung, jede organisatorische Sicherheitspolitik und jede Annahme von mindestens einem Sicherheitsziel adressiert wird und jedes Sicherheitsziel mindestens eine Bedrohung, eine organisatorische Sicherheitspolitik oder eine Annahme adressiert.

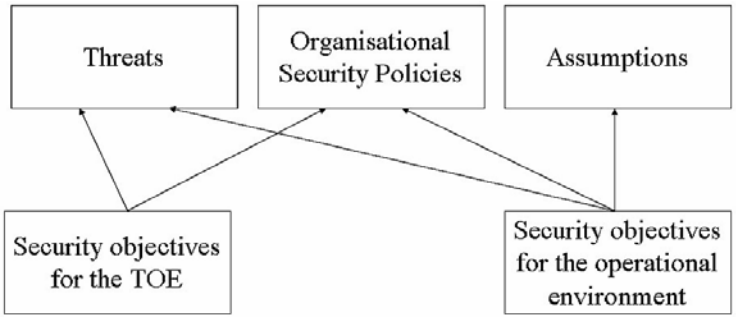

Abbildung 4.1: Sicherheitsprobleme und Sicherheitsziele [CCT1, 2006].

4.3.1 Abwehr der Bedrohungen durch den EVG

T.Protokoll Die Bedrohung wird durch das Ziel O.Protokoll abgewehrt. Alle sicherheitsrelevanten Aktionen werden somit protokolliert. Außerdem wird die Abwehr durch folgendes Ziel der IT-Umgebung unterstützt:

- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.Abhören Die Bedrohung wird durch die Ziele O.Abhören und O.WLANSSID abgewehrt. Das WLAN ist damit unsichtbar und durch einen Verschlüsselungsmechanismus geschützt. Außerdem wird die Abwehr durch folgendes Ziel der IT-Umgebung unterstützt:

- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.SSID Die Bedrohung wird durch das Ziel O.WLANSSID abgewehrt. Das WLAN ist damit für unautorisierte Clients unsichtbar. Außerdem wird die Abwehr durch folgendes Ziel der IT-Umgebung unterstützt:

- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.KonfExt Die Bedrohung wird durch das Ziel O.KonfExt abgewehrt. Das EVG-Konfigurationsmenü ist damit nicht aus dem externen Netzwerk erreichbar. Außerdem wird die Abwehr durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.UserSensib (da hierdurch sichergestellt ist, dass die IP-Adresse des EVG nicht Dritten mitgeteilt wird),
- OE.ISP (da davon ausgegangen wird, dass Dritten die IP-Adresse des EVG nicht mitgeteilt wird),
- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.KonfInt Die Bedrohung wird durch die Ziele O.IPKonf und O.KonfPW abgewehrt. Das EVG-Konfigurationsmenü ist damit mit einem sicheren Passwort vor dem Zugriff von unautorisierten Personen geschützt und unbefugte Clients erlangen nicht

automatisch die notwendige Netzwerkkonfiguration. Das Ziel O.Protokoll sorgt für die Protokollierung sicherheitsrelevanter Ereignisse. Außerdem wird die Abwehr durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.UserSensib (da hierdurch sichergestellt ist, dass Befugte über die Gefahren des Zugangs zu LAN-Ports oder zum EVG durch Dritte aufgeklärt sind),
- OE.ZugriffLAN (da so sichergestellt wird, dass die Umgebung den physischen Zugriff auf die LAN-Ports des EVG verhindert),
- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.DHCP Die Bedrohung wird durch das Ziel O.IPKonf abgewehrt. Den angeschlossenen Client werden so nicht automatisch die IP-Einstellungen mitgeteilt, sondern diese müssen manuell im Client konfiguriert werden. Die Anmeldung von Clients wird mit O.Protokoll protokolliert. Außerdem wird die Abwehr durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.ZugriffLAN (da hierdurch sichergestellt ist, dass kein unbefugter Client unbemerkt an das interne Netzwerk des EVG angeschlossen wird),
- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.NAT Die Bedrohung wird durch die Ziele O.Firewall und O.Intern abgewehrt. Angriffsversuche auf interne Clients werden durch die Firewall des EVG geblockt, und der Datenverkehr wird nicht an Clients weitergeleitet. Eine direkte Adressierung der internen Clients ist nicht möglich. Das Ziel O.Protokoll sorgt für die Protokollierung sicherheitsrelevanter Ereignisse. Außerdem wird die Abwehr durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.ISP (da davon ausgegangen wird, dass Dritten nicht die IP-Adresse des EVG mitgeteilt wird),
- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.Firewall Das Ziel O.Firewall wehrt die Bedrohung ab. Der EVG verfügt so über eine korrekt konfigurierte Firewall. Außerdem wird die Abwehr durch die folgenden Ziele der IT-Umgebung unterstützt:

- OE.Admin (da so sichergestellt ist, dass alle Konfigurationen im EVG korrekt und nach höchster Sicherheitsgrundlage erstellt sind).

T.Backdoor Die Bedrohung wird durch das Ziel O.Backdoor abgewehrt. Hierbei wird es durch das Ziel O.Protokoll unterstützt. Es wird sichergestellt, dass sich keine werkseitig eingebaute Backdoor im EVG befindet, da die Funktionen des EVG für den Benutzer transparent sind. Dieses wird auch durch eine entsprechende Protokollierung gewährleistet.

Abbildung 4.2 zeigt die Zuordnung der Bedrohungen zu den Sicherheitszielen, und dass jede Bedrohung mindestens von einem Sicherheitsziel abgewehrt wird.

	T.Protokoll	T.Abhören	T.SSID	T.KonfExt	T.KonfInt	T.DHCP	T.NAT	T.Firewall	T.Backdoor
O.Protokoll	X				X	X	X		X
O.Abhören		X							
O.WLANSSID		X	X						
O.KonfExt				X					
O.KonfPW					X				
O.IPKonf					X	X			
O.Intern							X		
O.Firewall							X	X	
O.Backdoor									X
O.Update									
OE.OSAuth									
OE.UserSensib				X	X				
OE.ZugriffEVG									
OE.ZugriffLAN					X	X			
OE.Updateclient									
OE.FreigabeAuth									
OE.extDatenträger									
OE.Downloads									
OE.ISP				X			X		
OE.BackdoorClient									
OE.Admin	X	X	X	X	X	X	X	X	
OE.AdminModus									

Abbildung 4.2: Zuordnung Bedrohungen - Sicherheitsziele.

4.3.2 Durchsetzung der organisatorischen Sicherheitspolitiken

P.Update Die organisatorische Sicherheitspolitik wird durch die Erfüllung des folgenden Sicherheitszieles für den EVG realisiert:

- O.Update (da hierdurch sichergestellt ist, dass die Firmware des EVG stets auf den Sicherheitsstand gebracht wird).

P.sicherePW Das Ziel O.KonfPW erfüllt die organisatorische Sicherheitspolitik. Hierdurch wird sichergestellt, dass nur ein sicheres Passwort zur Absicherung des Konfigurationsmenüs verwendet wird. Das gewählte Passwort wird überprüft und bei mangelnder Sicherheit nicht akzeptiert. Die organisatorische Sicherheitspolitik wird durch die Erfüllung der folgenden Ziele der IT-Umgebung unterstützt:

- OE.UserSensib (da die Benutzer wissen, dass sie vorsichtig mit Passwörtern umgehen müssen),
- OE.Updateclient (da hierdurch sichergestellt ist, dass die Mechanismen zur Überprüfung auf sichere Passwörter stets aktuell sind).

Abbildung 4.3 zeigt die Zuordnung der organisatorischen Sicherheitspolitiken zu den Sicherheitszielen, und dass jede organisatorische Sicherheitspolitik mindestens von einem Sicherheitsziel durchgesetzt wird.

	P.Update	P.sicherePW
O.Protokoll		
O.WLANEncr		
O.WLANSSID		
O.KonfExt		
O.KonfPW		X
O.IPKonf		
O.Intern		
O.Firewall		
O.Backdoor		
O.Update	X	
OE.OSAuth		
OE.UserSensib		X
OE.ZugriffEVG		
OE.ZugriffLAN		
OE.Updateclient	X	X
OE.FreigabeAuth		
OE.extDatenträger		
OE.Downloads		
OE.ISP		
OE.BackdoorClient		
OE.Admin		
OE.AdminModus		

Abbildung 4.3: Zuordnung organisatorische Sicherheitspolitiken - Sicherheitsziele.

4.3.3 Abdeckung der Annahmen

Die Abdeckung der Annahmen durch Sicherheitsziele der Umgebung erklärt sich von selbst. Es wurden daher auch jeweils gleiche Bezeichner gewählt. Abbildung 4.4 zeigt die Zuordnung der Annahmen zu den Sicherheitszielen.

	A.OSAuth	A.UserSensib	A.ZugriffEVG	A.ZugriffLAN	A.Updateclient	A.FreigabenAuth	A.extDatenträger	A.Downloads	A.ISP	A.BackdoorClient	A.Admin	A.AdminModus
OE.OSAuth	X											
OE.UserSensib		X										
OE.ZugriffEVG			X									
OE.ZugriffLAN				X								
OE.Updateclient					X							
OE.FreigabeAuth						X						
OE.extDatenträger							X					
OE.Downloads								X				
OE.ISP									X			
OE.BackdoorClient										X		
OE.Admin											X	
OE.AdminModus												X

Abbildung 4.4: Zuordnung Annahmen - Sicherheitsziele.

Kapitel 5

Erweiterte Komponenten-Definitionen

Da dieses Schutzprofil CC Teil 2 konformant ist, werden keine weiteren Komponenten definiert.

Kapitel 6

IT-Sicherheitsanforderungen

Die IT-Sicherheitsanforderungen sind eine Übersetzung der Sicherheitsziele für den EVG in eine standardisierte Sprache. Die so festgelegten funktionalen EVG-Sicherheitsanforderungen stellen im Falle ihrer Erfüllung sicher, dass der EVG seine Sicherheitsziele erfüllen kann. Die Sicherheitsanforderungen enthalten sowohl Anforderungen an das Vorhandensein des gewünschten Verhaltens als auch Anforderungen an die Abwesenheit unerwünschten Verhaltens.
Abbildung 6.1 [CCT1, 2006] verdeutlicht den Zusammenhang zwischen dem Sicherheitsproblem, den Sicherheitszielen und den Sicherheitsanforderungen. Neben den funktionalen EVG-Anforderungen werden in diesem Kapitel auch die Anforderungen an die Vertrauenswürdigkeit des EVG genannt und erklärt.
Für die Beschreibung der funktionalen Sicherheitsanforderungen werden folgende Si-

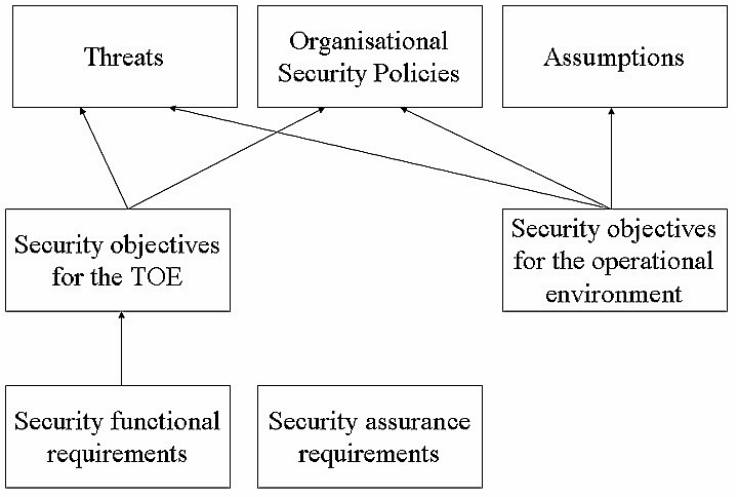

Abbildung 6.1: Zusammenhänge bis Sicherheitsanforderungen [CCT1, 2006].

cherheitsattribute definiert:

kein Zugriff auf EVG-Konfigurationsmenü aus WAN Ein Zugriff auf das EVG-Konfigurationsmenü ist grundsätzlich nicht aus dem externen Netzwerk möglich.

Passwort des EVG-Konigurationsmenüs Das EVG-Konfigurationsmenü ist nur durch die Eingabe des richtigen Passwortes zugänglich.

Kenntnis der WLAN-SSID Die Clients müssen die WLAN-SSID kennen, damit sie sich per WLAN mit dem EVG verbinden können.

Kenntnis der IP-Konfiguration Die Clients müssen die richtige IP-Konfiguration kennen, damit sie sich mit dem EVG verbinden können.

6.1 Funktionale EVG-Sicherheitsanforderungen

Die Darstellung der funktionalen EVG-Sicherheitsanforderungen erfolgt durch die funktionalen Anforderungen an den EVG in Form funktionaler Komponenten, die in einem Katalog in Teil 2 der Common Criteria [CCT2, 2007] aufgeführt sind. Abbildung 6.2 gibt eine Übersicht über die ausgewählten Komponenten, die hier ausführlich beschrieben werden.

Komponente	Beschreibung
FAU: Sicherheitsprotokollierung	
FAU_GEN.1	Generierung der Protokolldaten
FAU_SAR.1	Durchsicht der Protokollierung
FAU_SAR.2	Eingeschränkte Durchsicht der Protokollierung
FCS: Kryptografische Unterstützung	
FCS_CKM.1	Generierung kryptografischer Schlüssel
FCS_COP.1	Kryptografischer Betrieb
FDP: Schutz der Benutzerdaten	
FDP_ACC.1	Teilweise Zugriffskontrolle
FDP_ACF.1	Zugriffskontrolle basierend auf Sicherheitsattributen
FDP_IFC.1	Teilweise Informationsflusskontrolle
FDP_IFF.1	Einfache Sicherheitsattribute
FDP_IFF.5	Keine unerwünschten Informationsflüsse
FDP_ITT.1	Einfacher Schutz des internen Transfers
FDP_UCT.1	Einfache Vertraulichkeit des Datenaustausches
FDP_UIT.1	Einfache Integrität des Datenaustausches
FIA: Identifikation und Authentifizierung	
FIA_AFL.1	Authentifikationsfehler-Behandlung
FIA_SOS.1	Verifikation von Geheimnissen
FIA_UAU.2	Benutzerauthentifizierung vor jeglicher Aktion
FIA_UID.2	Benutzeridentifikation vor jeglicher Aktion
FMT: Sicherheitsmanagement	
FMT_MSA.1	Management der Sicherheitsattribute
FMT_MSA.2	Sichere Sicherheitsattribute
FMT_SMF.1	Spezifikation der Managementfunktionen
FMT_SMR.1	Sicherheitsrollen
FPR: Datenschutz	
FPR_UNL.1	Unverkettbarkeit
FPT: Schutz der EVG-Sicherheitsfunktionen	
FPT_STM.1	Verlässliche Zeitstempel
FTA: EVG-Zugriff	
FTA_TAH.1	EVG-Zugriffshistorie
FTA_TSE.1	EVG-Sitzungseinrichtung
FTP: Vertrauenswürdiger Pfad/Kanal	
FTP_TRP.1	Vertrauenswürdiger Pfad

Abbildung 6.2: Übersicht über die ausgewählten funktionalen Sicherheitsanforderungen.

FAU: Sicherheitsprotokollierung

FAU_GEN.1 Generierung der Protokolldaten
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FPT_STM.1 Verlässliche Zeitstempel

FAU_GEN.1.1
Die TSF muss in der Lage sein, für folgende protokollierbaren Ereignisse eine Protokollaufzeichnung zu generieren:

a Starten und Beenden der Protokollierungsfunktionen

b Alle protokollierbaren Ereignisse für den Protokollierungsgrad [Auswahl: Minimal] und

c [Zuweisung: weitere speziell festgelegte protokollierbare Ereignisse: FDP_ITT.1 Basic, FDP_UCT.1 Basic, FDP_UIT.1 Basic, FIA_UAU.2 Basic, FTA_TSE.1 Basic, FTP_TRP.1 Basic]

FAU_GEN.1.2
Die TSF muss innerhalb jeder Aufzeichnung mindestens die folgenden Informationen speichern:

a Datum und Uhrzeit des Ereignisses, Art des Ereignisses, Identität des Subjekts und das Ergebnis (Erfolg oder Misserfolg) des Ereignisses; und

b basierend auf den Definitionen der im PP/ST eingebundenen protokollierbaren Ereignissen, für jede Art von Protokollierungsereignissen [Zuweisung: sonstige protokollierungsrelevante Information].

FAU_SAR.1 Durchsicht der Protokollierung
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FAU_GEN.1 Generierung der Protokolldaten

FAU_SAR.1.1
Die TSF muss für den [Zuweisung: Administrator] die Fähigkeit bereitstellen, [Zuweisung: alle Protokollinformationen] aus den Protokollaufzeichnungen zu lesen.

FAU_SAR.1.2
Die TSF muss die Protokollaufzeichnungen in einer für die Interpretation der Informationen durch den Benutzer geeigneten Art und Weise bereitstellen.

FAU_SAR.2 Eingeschränkte Durchsicht der Protokollierung
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FAU_SAR.1 Durchsicht der Protokollierung

FAU_SAR.2.1
Die TSF soll allen Benutzern den Lesezugriff auf die Protokolldaten verweigern, außer den Benutzern, die explizite Leseerlaubnis besitzen.

FCS: Kryptografische Unterstützung

FCS_CKM.1 Generierung kryptografischer Schlüssel

Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FCS_COP.1 Kryptografischer Betrieb, FCS_CKM.4 Vernichtung kryptografischer Schlüssel

FCS_CKM.1.1
Die TSF soll unter Einhaltung eines festgelegten Algorithmus zur Erstellung von kryptografischen Schlüsseln [Zuweisung: zufällige Auswahl von Buchstaben und Ziffern] und einer festgelegten Größe eines kryptografischen Schlüssels [Zuweisung: zwischen 8 und 63 Zeichen] in der Lage sein, kryptografische Schlüssel zu generieren, die Folgendes erfüllen:
Einsetzbar für die WLAN-Verschlüsselung mit den Verschlüsselungsmethoden WPA oder WPA2.

FCS_COP.1 Kryptografischer Betrieb

Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FCS_CKM.1 Generierung kryptografischer Schlüssel, FCS_CKM.4 Vernichtung kryptografischer Schlüssel

FCS_COP.1.1
Die TSF soll [Zuweisung: die Verschlüsselung des WLAN-Signals] im Einklang mit einem festgelegten kryptografischen Algorithmus [Zuweisung: WPA, WPA2] und einer festgelegten Größe des kryptografischen Schlüssels [Zuweisung: zwischen 8 und 63 Zeichen] realisieren, so dass Folgendes gilt:
Abhörsichere Übertragung des Datenstromes per WLAN.

FDP: Schutz der Benutzerdaten

FDP_ACC.1 Teilweise Zugriffskontrolle

Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen

FDP_ACC.1.1
Die TSF soll die [Zuweisung: Zugriffskontroll-SFP] für [Zuweisung: kein Zugriff für Clients aus WAN auf Konfigurationsmenü; nur Zugriff für Administratoren auf Konfigurationsmenü aus lokalem Netzwerk; nur Zugriff auf lokales Netzwerk per WLAN bei Kenntnis der WLAN-SSID; nur Zugriff auf lokales Netzwerk bei Kenntnis der erforderlichen IP-Konfiguration] durchsetzen.

FDP_ACF.1 Zugriffskontrolle basierend auf Sicherheitsattributen
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FDP_ACC.1 Teilweise Zugriffskontrolle, FMT_MSA.3 Initialisierung statischer Attribute

FDP_ACF.1.1
Die TSF müssen die [Zuweisung: Zugriffskontroll-SFP] für Objekte basierend auf Folgendes durchsetzen: [Zuweisung: kein Zugriff für Clients aus WAN auf Konfigurationsmenü: Sperre der direkten Erreichbarkeit des Konfigurationsmenüs aus dem WAN; nur Zugriff für Administratoren auf Konfigurationsmenü aus lokalem Netzwerk: Administrator-Passwort; nur Zugriff auf lokales Netzwerk per WLAN bei Kenntnis der WLAN-SSID: nicht sichtbare Ausstrahlung der WLAN-SSID; nur Zugriff auf lokales Netzwerk bei Kenntnis der erforderlichen Konfiguration: Kenntnis der IP-Konfigurationen].

FDP_ACF.1.2
Die TSF müssen die folgenden Regeln durchsetzen, um festzustellen, ob eine Operation zwischen kontrollierten Subjekten und kontrollierten Objekten zulässig ist: [Zuweisung: Sperre von unerlaubten Zugängen; Überprüfung der Anmeldeprozeduren].

FDP_ACF.1.3
Die TSF sollen Subjekten zu Objekten explizit Zugang gewähren, basierend auf den folgenden zusätzlichen Regeln: [Zuweisung: keine weiteren Regeln].

FDP_ACF.1.4
Die TSF sollen Subjekten zu Objekten explizit den Zugang verweigern, basierend auf den folgenden zusätzlichen Regeln: [Zuweisung: keine weiteren Regeln].

FDP_IFC.1 Teilweise Informationsflusskontrolle
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FDP_IFF.1 Einfache Sicherheitsattribute
FDP_IFC.1.1
Die TSF sollen die [Zuweisung: Informationsflusskontroll-SFP] durchsetzen. [Zuweisung: das Konfigurationsmenü darf aus dem WAN nicht adressiert werden können; der Informationsfluss vom und zum EVG, sowohl aus dem WAN als auch von den Clients kommend, muss die EVG-Firewall passieren und wird dort auf zulässigen und nicht zulässigen Informationsfluss kontrolliert und gegebenenfalls blockiert].

FDP_IFF.1 Einfache Sicherheitsattribute
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle, FMT_MSA.3 Initialisierung statischer Attribute

FDP_IFF.1.1
Die TSF muss die [Zuweisung: Informationsflusskontroll-SFP] basierend auf den folgenden Subjekten und Informationssicherheitsattributen durchsetzen: [Zuweisung: Das Konfigurationsmenü darf von Client im WAN nicht adressiert werden können. Diese

Einschränkung wird durch das Attribut IP-Adresse beschränkt. Der Informationsfluss vom und zum EVG, sowohl aus dem WAN als auch von den Clients kommend, muss die EVG-Firewall passieren und wird dort auf zulässigen und nicht zulässigen Informationsfluss kontrolliert und gegebenenfalls blockiert. Diese Einschränkungen werden durch die Attribute IP-Adressen und Internet-Ports beschränkt].

FDP_IFF.1.2
Die TSF soll einen Informationsfluss zwischen einem kontrollierten Subjekt und einer kontrollierten Information über einer kontrollierten Operation erlauben, falls die folgenden Regeln gelten: [Zuweisung: Für das Sicherheitsattribut IP-Adresse gilt, dass beim Zugriff auf das Konfigurationsmenü des EVG nur interne IP-Adressen erlaubt sind. Für die Sicherheitsattribute, die die EVG-Firewall betreffen, muss gelten, dass nur gültige Kombinationen aus IP-Adressen und Internet-Ports für eine Datenübertragung genutzt werden dürfen. Diese Absender- bzw. Ziel-IP-Adressen und die zugelassenen Internet-Ports müssen einmalig vom EVG-Administrator festgelegt werden. Hierbei muss dieser die erlaubten Wege freigeben und die unerlaubten Wege blockieren].

FDP_IFF.1.3
Die TSF soll [Zuweisung: keine weiteren Informationsflusskontroll-SFP-Regeln] durchsetzen.

FDP_IFF.1.4
Die TSF soll explizit den Informationsfluss basierend auf folgenden Regeln erlauben: [Zuweisung: Das EVG-Konfigurationsmenü kann von jedem Client im internen Netzwerk durch Eingabe der IP-Adresse des EVG erreicht werden. Der in der EVG-Firewall definierte erlaubte Kommunikationsfluss zwischen IP-Adressen über freigegebene Internet-Ports wird explizit erlaubt. Hierbei muss darauf geachtet werden, dass nur die Internet-Ports geöffnet werden, die auch wirklich nur für die gewünschte Datenübertragungen nötig sind. Als Standard-Freigaben für die Internet-Ports gelten die Port-Nummern 25 (SMTP), 80 (HTTP), 108-110 (POP3), 220 (IMAP) und 443 (HTTPS). Weitere Freigaben von Internet-Ports müssen sorgfältig vom Administrator geprüft werden.].

FDP_IFF.1.5
Die TSF soll explizit den Informationsfluss basierend auf folgenden Regeln verbieten: [Zuweisung: Jeder Informationsfluss, der nicht den Regeln der expliziten Erlaubnisse angehört, muss verboten werden.].

FDP_IFF.5 Keine unerwünschten Informationsflüsse
Hierarchisch zu: FDP_IFF.4 Teilweise Beseitigung der unerwünschten Informationsflüsse
Abhängigkeiten: FDP_IFC.1 Teilweise Informationsflusskontrolle

FDP_IFF.5.1
Die TSF muss sicherstellen, dass keine unerwünschten Informationsflüsse zur Umgehung der [Zuweisung: Informationsflusskontroll-SFP] existieren.

FDP_ITT.1 Einfacher Schutz des internen Transfers
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FDP_ACC.1 Teilweise Zugriffskontrolle, FDP_IFC.1 Teilweise Informationsflusskontrolle

FDP_ITT.1.1
Die TSF soll die [Zuweisung: Zugriffskontroll-SFP und die Informationsflusskontroll-SFP] durchsetzen, um [Zuweisung: die Enthüllung und die Veränderung] der Benutzerdaten zu verhindern, wenn sie zwischen physikalisch getrennten Teilen des EVG übertragen werden.

FDP_UCT.1 Einfache Vertraulichkeit des Datenaustausches
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal oder FTP_TRP.1 Vertrauenswürdiger Pfad] [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle]

FDP_UCT.1.1
Die TSF muss die [Zuweisung: Zugriffskontroll-SFP und die Informationsflusskontroll-SFP] durchsetzen, um in der Lage zu sein, Benutzerdaten vor nicht autorisierter Preisgabe geschützt zu [Auswahl: übertragen und empfangen].

FDP_UIT.1 Einfache Integrität des Datenaustausches
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] [FTP_ITC.1 Inter-TSF Vertrauenswürdiger Kanal oder FTP_TRP.1 Vertrauenswürdiger Kanal]

FDP_UIT.1.1
Die TSF muss die [Zuweisung: Zugriffskontroll-SFP und die Informationsflusskontroll-SFP] durchsetzen, um in der Lage zu sein, Benutzerdaten geschützt vor [Auswahl: Modifizierung, Einfügen] zu [Auswahl: übertragen und empfangen].

FDP_UIT.1.2
Die TSF muss in der Lage sein, beim Empfang der Benutzerdaten festzustellen, ob ein [Auswahl: Modifizieren, Einfügen] stattgefunden hat.

FIA: Identifikation und Authentifizierung

FIA_AFL.1 Authentifikationsfehler-Behandlung
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FIA_UAU.1 Zeitpunkt der Authentifikation

FIA_AFL.1.1
Die TSF soll erkennen, wenn [Auswahl: [Zuweisung: drei(3)]] erfolglose Authentifizierungsversuche erfolgt sind bei der [Zuweisung: Anmeldung am EVG-

Konfigurationsmenü].

FIA_AFL.1.2
Wenn die definierte Anzahl erfolgloser Authentifizierungsversuche [Auswahl: erreicht] ist, soll die TSF [Zuweisung: den Zugang zum EVG-Konfigurationsmenü für fünf(5) Minuten sperren].

FIA_SOS.1 Verifikation von Geheimnissen
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.
FIA_SOS.1.1
Die TSF soll einen Mechanismus zur Verfügung stellen, der verifiziert, dass Geheimnisse übereinstimmen mit: [Zuweisung: der Schlüssel zur Verschlüsselung des WLAN besteht aus einer Auswahl von Ziffern und Buchstaben mit einer Länge von acht (8) bis dreiundsechzig (63) Zeichen; das Passwort für das EVG-Konfigurationsmenü besteht aus einer Auswahl von Ziffern und Buchstaben und ist mindestens acht (8) Zeichen lang; der Name der ausgestrahlten WLAN-SSID sollte kein Name sein, der leicht zu erraten ist].

FIA_UAU.2 Benutzerauthentifizierung vor jeglicher Aktion
Hierarchisch zu: FIA_UAU.1 Zeitpunkt der Authentifizierung
Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FIA_UAU.2.1
Die TSF muss erfordern, dass jeder Benutzer erfolgreich authentifiziert wurde, bevor diesem jegliche andere TSF-vermittelte Aktionen erlaubt werden.

FIA_UID.2 Benutzeridentifikation vor jeglicher Aktion
Hierarchisch zu: FIA_UID.1 Zeitpunkt der Identifikation
Abhängigkeiten: keine Abhängigkeiten.

FIA_UID.2.1
Die TSF muss erfordern, dass sich jeder Benutzer identifiziert, bevor für diesen jegliche andere TSF-vermittelte Aktionen erlaubt werden.

FMT: Sicherheitsmanagement

FMT_MSA.1 Management der Sicherheitsattribute
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_SMR.1 Sicherheitsrollen, FMT_SMF.1 Spezifikation der Managementfunktionen

FMT_MSA.1.1
Die TSF muss die [Zuweisung: Zugriffskontroll-SFP und die Informationsflusskon-troll-SFP] zur Beschränkung der Fähigkeit zum [Auswahl: Ändern der Default-Einstellungen, Abfragen, Modifizieren, Löschen] der Sicherheitsattribute auf [Zuweisung: Administratoren].

FMT_MSA.2 Sichere Sicherheitsattribute
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: [FDP_ACC.1 Teilweise Zugriffskontrolle oder FDP_IFC.1 Teilweise Informationsflusskontrolle] FMT_MSA.1 Management der Sicherheitsattribute, FMT_SMR.1 Sicherheitsrollen

FMT_MSA.2.1
Die TSF müssen sicherstellen, dass nur sichere Werte für Sicherheitsattribute akzeptiert werden.

FMT_SMF.1 Spezifikation der Managementfunktionen
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.

FMT_SMF.1.1
Die TSF soll dazu in der Lage sein, die folgenden Managementfunktionen auszuführen [Zuweisung: Ändern des Passwortes für das EVG-Konfigurationsmenü, Ändern der WLAN-SSID, Ändern des Verschlüsselungsstrings für die WLAN-Verschlüsselung, Ändern der Einstellungen in der Firewall, Auswahl der Protokollfunktionen, Aktualisieren der EVG-Firmware].

FMT_SMR.1 Sicherheitsrollen
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: FIA_UID.1 Zeitpunkt der Identifikation

FMT_SMR.1.1
Die TSF muss die Rollen [Zuweisung: Administrator, Client] erhalten.

FMT_SMR.1.2
Die TSF müssen Benutzer mit Rollen verknüpfen können.

FPR: Datenschutz

FPR_UNL.1 Unverkettbarkeit
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.

FPR_UNL.1.1
Die TSF soll sicherstellen, dass [Zuweisung: Benutzer, Angreifer, andere Clients] nicht in der Lage sind herauszufinden, dass [Zuweisung: mehrere Datenübertragungen] [Auswahl: von ein und demselben Client ausgehen].

FPT: Schutz der EVG-Sicherheitsfunktionen

FPT_STM.1 Verlässliche Zeitstempel
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.

FPT_STM.1.1
Die TSF sollen einen verlässlichen Zeitstempel bereitstellen.

FTA: EVG-Zugriff

FTA_TAH.1 EVG-Zugriffshistorie
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.

FTA_TAH.1.1
Nach erfolgreicher Sitzungseinrichtung muss die TSF dem Benutzer [Auswahl: Datum, Zeit, Client-IP-Adresse] der letzten erfolgreichen Sitzungseinrichtung anzeigen.
[Verfeinerung: gilt nur für den Zugriff auf das EVG-Konfigurationsmenü]

FTA_TAH.1.2
Nach erfolgreicher Sitzungseinrichtung muss die TSF dem Benutzer [Auswahl: Datum, Zeit, Client-IP-Adresse] des letzten misslungenen Versuchs einer Sitzungseinrichtung und die Anzahl misslungener Versuche seit der letzten erfolgreichen Sitzungseinrichtung anzeigen.

FTA_TAH.1.3
Die TSF muss sicherstellen, dass die Informationen der Zugriffshistorie nicht von der Benutzerschnittstelle gelöscht werden, ohne dem Benutzer die Möglichkeit zur Durchsicht der Informationen zu geben.

FTA_TSE.1 EVG-Sitzungseinrichtung
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.

FTA_TSE.1.1
Die TSF muss in der Lage sein, eine Sitzungseinrichtung wegen [Zuweisung: falscher Schlüssel für WLAN-Verschlüsselung, Zugriff auf das EVG-Konfigura-tionsmenü aus dem WAN, falsche IP-Konfiguration] abzulehnen.

FTP: Vertrauenswürdiger Pfad/Kanal

FTP_TRP.1 Vertrauenswürdiger Pfad
Hierarchisch zu: keine anderen Komponenten.
Abhängigkeiten: keine Abhängigkeiten.

FTP_TRP.1.1
Die TSF muss einen Kommunikationspfad zwischen sich und [Auswahl: entfernten] Benutzern bereitstellen, der logisch von den anderen Kommunikationspfaden getrennt ist und eine gesicherte Identifikation der Endpunkte und Schutz der kommunizierten Daten vor [Auswahl: Modifikation, Offenlegung] bietet.

FTP_TRP.1.2
Die TSF muss [Auswahl: entfernten Benutzern] erlauben, eine Kommunikation über den vertrauenswürdigen Pfad einzuleiten.

FTP_TRP.1.3
Die TSF muss den Gebrauch des vertrauenswürdigen Pfades für [Zuweisung: eine Verbindung eines Clients über WLAN, für eine Verbindung zum EVG-Konfigura-tionsmenü] erfordern.

6.2 Anforderungen an die Vertrauenswürdigkeit des EVG

Für die Anforderungen an die Vertrauenswürdigkeit, die vom EVG erfüllt werden müssen, wurden die Komponenten der EAL-Stufe 3 (EAL3) ausgewählt. In Abbildung 6.3 werden die Komponenten der Stufe EAL3 aufgeführt. [CCT3, 2007]

6.3 Erklärung der Sicherheitsanforderungen

Die Erklärung der Sicherheitsanforderungen liefert den Nachweis, dass die Auswahl der funktionalen Sicherheitsanforderungen an den EVG geeignet ist, die Sicherheitsziele an den EVG zu erfüllen. Dabei werden die funktionalen Sicherheitsanforderungen auf die Sicherheitsziele zurückverfolgt. Darüber hinaus werden in diesem Kapitel die Abhängigkeiten der funktionalen Sicherheitsanforderungen an den EVG dargelegt und die Auswahl der Anforderungen an die Vertrauenswürdigkeit des EVG erklärt.

6.3.1 Erklärung der funktionalen Sicherheitsanforderungen an den EVG

Im Folgenden wird die Eignung zur Abdeckung aller Sicherheitsziele an den EVG nachgewiesen.

O.KonfExt Durch die Komponenten FDP_ACC.1 und FDP_ACF.1 wird die Zugriffskontroll-SFP durchgesetzt, so dass kein Zugriff auf das EVG-Konfigurationsmenü von einem Client im WAN möglich ist. Unterstützt werden sie dabei von

Vertrauenswürdigkeitsklasse	Vertrauenswürdigkeitskomponenten
ADV: Entwicklung	ADV_ARC.1 Sicherheitsarchitektur-Beschreibung
	ADV_FSP.3 Funktionale Spezifikation mit kompletter Zusammenfassung
	ADV_TDS.2 Architektonisches Design
AGD: Handbücher	AGD_OPE.1 Benutzerhandbuch
	AGD_PRE.1 Vorbereitungsprozeduren
ALC: Lebenszyklus-Unterstützung	ALC_CMC.3 Autorisationskontrollen
	ALC_CMS.3 Implementationsdarstellung Abdeckung Konfigurationsmanagement
	ALC_DEL.1 Auslieferungsprozeduren
	ALC_DVS.1 Identifikation von Sicherheitsmaßnahmen
	ALC_LCD.1 Entwicklerbestimmtes Lebenszyklusmodell
ASE: Security Target Evaluation	ASE_CCL.1 Postulate zur Übereinstimmung
	ASE_ECD.1 Erweiterte Komponentendefinition
	ASE_INT.1 ST Einleitung
	ASE_OBJ.2 Sicherheitsziele
	ASE_REQ.2 abgeleitete Sicherheitsanforderungen
	ASE_SPD.1 Definition des Sicherheitsproblems
	ASE_TSS.1 EVG Spezifikationszusammenfassung
ATE: Tests	ATE_COV.2 Analyse der Testabdeckung
	ATE_DPT.1 Test: Grundaufbau
	ATE_FUN.1 Funktionales Testen
	ATE_IND.2 Unabhängiges Testen - Stichproben
AVA: Schwachstellenbewertung	Schwachstellenanalyse

Abbildung 6.3: Anforderungen an die Vertrauenswürdigkeit des EVG.

den Komponenten FDP_IFC.1, FDP_IFF.1 und FDP_IFF.5, die den unerwünschten Informationsfluss auf das EVG-Konfigurationsmenü aus dem WAN unterbinden. Die Sitzungseinrichtung aus dem WAN für das EVG-Konfigurationsmenü wird zusätzlich durch Komponente FTA_TSE.1 verboten.

O.KonfPW Die Zugriffskontroll-SFP für den Zugriff auf das Konfigurationsmenü des EVG werden durch die Komponenten FDP_ACC.1 und FDP_ACF.1 erfüllt. FIA_AFL.1 behandelt den Fall der dreimaligen Falscheingabe des Passwortes für das EVG-Konfigurationsmenü. Dieses Passwort muss vordefinierten Richtlinien entsprechen (FIA_SOS.1). Komponente FIA_UAU.2 verlangt die Authentifizierung mit einem Passwort. Durch die Komponenten FMT_MSA.1 und FMT_MSA.2 werden die Zugriffskontroll-SFP durchgesetzt, indem nur dem Administrator definierte Handlungen erlaubt werden und dass nur sichere Werte für Sicherheitsattribute akzeptiert werden. Die Funktionen, für die der Administrator Befugnis zur Einstellung bzw. zur Änderung hat, werden in FMT_SMF.1 beschrieben. FMT_SMR.1 definiert den Administrator als Rolle. Die Anmeldeversuche am EVG-Konfigurations-menü werden protokolliert, und misslungene Versuche werden dem Administrator beim nächsten Anmelden angezeigt (FTA_TAH.1). Die Kommunikation von einem Client zum EVG-Konfigurationsmenü erfolgt dabei immer über einen vertrauenswürdigen Pfad, der in der Komponente FTP_TRP.1 gefordert wird.

O.FirewallBlock Die dem Protokollierungsgrad entsprechenden Protokolldaten werden durch die Komponente FAU_GEN.1 erfasst. Diese Daten können vom Administrator, und zwar nur von ihm, eingesehen werden (FAU_SAR.1 und FAU_SAR.2). Durch die Komponenten FDP_IFC.1, FDP_IFF.1 und FDP_IFF.5 wird die Informationsflusskontroll-SFP durchgesetzt, da der Datenverkehr durch die EVG-Firewall auf unzulässigen Datenverkehr untersucht wird und gegebenenfalls blockiert wird. Die Datenübertragung wird generell nur Clients gestattet, die sich vorher durch den Beweis durch Kenntnis der Sicherheitsattribute am EVG identifiziert haben (FIA_UID.2). Hierbei handelt es sich um die Kenntnis des richtigen WLAN-Schlüssels (bei WLAN-Nutzung) und die Kenntnis der richtigen IP-Konfiguration. Die Einstellungen für die EVG-Firewall werden durch die Komponente FMT_SMF.1 ermöglicht.

O.FirewallKorrekt Die dem Protokollierungsgrad entsprechenden Protokolldaten werden durch Komponente FAU_GEN.1 erfasst. Diese Daten können vom Administrator, und zwar nur von ihm, eingesehen werden (FAU_SAR.1 und FAU_SAR.2). Durch die Komponenten FDP_IFC.1, FDP_IFF.1 und FDP_IFF.5 wird die Informationsflusskontroll-SFP durchgesetzt, da der Datenverkehr durch die EVG-Firewall auf unzulässigen Datenverkehr untersucht wird und gegebenenfalls blockiert wird. Die Datenübertragung wird generell nur Clients gestattet, die sich vorher durch den Beweis durch Kenntnis der Sicherheitsattribute am EVG identifiziert haben (FIA_UID.2). Hierbei handelt es sich um die Kenntnis des richtigen WLAN-Schlüssels (bei WLAN-Nutzung) und die Kenntnis der richtigen IP-Konfiguration. Die Einstellungen für die EVG-Firewall werden durch die Komponente FMT_SMF.1 ermöglicht.

O.Abhören Das vom EVG ausgestrahlte WLAN soll mit einem Schlüssel verschlüsselt werden. Dieser kann nach der Komponente FCS_CKM.1 im EVG generiert werden. FCS_COP.1 verlangt dann den Einsatz dieses Schlüssels zur Absicherung des WLAN-Datenstromes. Die Zugriffskontroll-SFP und die Informationsflusskontroll-SFP werden von Komponente FDP_UCT.1 durchgesetzt. Der eingesetzte Schlüssel entspricht dabei den nach FIA_SOS.1 geforderten Ansprüchen. Der Schlüssel wird bei jedem Verbindungsaufbau mit dem WLAN verifiziert (FIA_UAU.2). FMT_MSA.2 stellt sicher, dass der generierte Schlüssel einen sicheren Wert darstellt. Die Einrichtung dieser WLAN-Verschlüsselung übernehmen die Komponenten FMT_MSA.1 und FMT_SMF.1. Die Verbindung über das WLAN wird für einen Client nur gestattet, wenn der Schlüssel übereinstimmt (FTA_TSE.1), so dass dann ein vertrauenswürdiger Pfad aufgebaut werden kann (FTP_TRP.1).

O.WLANSSID Die Zugriffskontrolle für die Verbindung mit dem WLAN wird durch die Komponente FDP_ACC.1 realisiert. Dabei basiert sie auf den von der Komponente FDP_ACF.1 beschriebenen Sicherheitsattributen. Die Verifikation der Geheimnisse WLAN-Schlüssel und SSID übernimmt die Komponente FIA_SOS.1. Die Komponenten FMT_MSA.1, FMT_MSA.2 und FMT_SMF.1 legen die Richtlinien für die Einrichtung der SSID fest.

O.IPKonf Die dem Protokollierungsgrad entsprechenden Protokolldaten werden durch die Komponente FAU_GEN.1 erfasst. Diese Daten können vom Administrator, und

zwar nur von ihm, eingesehen werden (FAU_SAR.1 und FAU_SAR.2). Die Komponenten FDP_ACC.1 und FDP_ACF.1 definieren die Zugriffskontrolle, so dass nur Clients Zugang zum internen Netzwerk bekommen, wenn sie die richtige IP-Konfiguration kennen. Die Kenntnis über die IP-Konfiguration ist für die Benutzerauthentifizierung FIA_UAU.2 geeignet. Die IP-Konfiguration wird in der Komponente FMT_SMF.1 erledigt. Bei falscher Authentifizierung des Clients wird keine Sitzung zum EVG hergestellt (FTA_TSE.1).

O.Intern Die dem Protokollierungsgrad entsprechenden Protokolldaten werden durch die Komponente FAU_GEN.1 erfasst. Diese Daten können vom Administrator, und zwar nur von ihm, eingesehen werden (FAU_SAR.1 und FAU_SAR.2). Die internen IP-Adressen der angemeldeten Clients werden im EVG im Rahmen von Network Address Translation auf die dem EVG zugewiesene externe IP-Adresse abgebildet. So ist ein Datenstrom nicht auf den genauen Urheber im internen Netzwerk zurückverfolgbar (FPR_UNL.1).

O.Backdoor Alle ausgewählten funktionalen Sicherheitsanforderungen müssen so implementiert werden, wie sie definiert wurden. Eine Backdoor wird so ausgeschlossen. Ergänzend zu den anderen aufgeführten Komponenten wird hier durch die Komponente FDP_ITT.1 der interne Datentransfer geschützt, und durch die Komponente FDP_UIT.1 wird die einfache Datenintegrität des Datenaustausches gefordert.

O.Protokoll Die dem Protokollierungsgrad entsprechenden Protokolldaten werden durch die Komponente FAU_GEN.1 erfasst. Diese Daten können vom Administrator, und zwar nur von ihm, eingesehen werden (FAU_SAR.1 und FAU_SAR.2). Das Protokoll wird durch verlässliche Zeitstempel nach FPT_STM.1 ergänzt. FTA_TAH.1 definiert die protokollierbare EVG-Zu-griffshistorie.

O.Update Die Updatefunktion des EVG ist eine Managementfunktion und wird durch die Komponente FMT_SMF.1 erfasst.

Die Abbildung 6.4 beweist, dass alle Sicherheitsziele für den EVG von mindestens einer funktionalen Sicherheitsanforderung abgedeckt wird. Auch wird gezeigt, dass jede Komponente von einem Sicherheitsziel effektiv adressiert wird.

6.3.2 Abhängigkeiten der funktionalen Sicherheitsanforderungen an den EVG

Die von den gewählten SFR abhängigen Komponenten werden in der Abbildung 6.5 aufgeführt. Falls es bei den Abhängigkeiten mehrere Möglichkeiten gibt, so wird in der Auflösung die gewählte Alternative angegeben. Bereits durch die Wahl entsprechender Komponenten aufgelöste Abhängigkeiten werden mit „Done“ bezeichnet.

	O.KonfExt	O.KonfPW	O.Firewall	O.WLANEner	O.WLANSSID	O.IPKonf	O.Intern	O.Backdoor	O.Protokoll	O.Update
FAU_GEN.1			X			X	X	X	X	
FAU_SAR.1			X			X	X	X	X	
FAU_SAR.2			X			X	X	X	X	
FCS_CKM.1				X				X		
FCS_COP.1				X				X		
FDP_ACC.1	X	X			X	X		X		
FDP_ACF.1	X	X			X	X		X		
FDP_IFC.1	X		X					X		
FDP_IFF.1	X		X					X		
FDP_IFF.5	X		X					X		
FDP_ITT.1								X		
FDP_UCT.1				X				X		
FDP_UIT.1								X		
FIA_AFL.1		X						X		
FIA_SOS.1		X		X	X			X		
FIA_UAU.2		X		X		X		X		
FIA_UID.2			X					X		
FMT_MSA.1		X		X	X			X		
FMT_MSA.2		X		X	X			X		
FMT_SMF.1		X	X	X	X	X		X		X
FMT_SMR.1		X						X		
FPR_UNL.1							X	X		
FPT_STM.1								X	X	
FTA_TAH.1		X						X	X	
FTA_TSE.1	X			X		X		X		
FTP_TRP.1		X		X				X		

Abbildung 6.4: Abdeckung der Sicherheitsziele an den EVG.

6.3.3 Erklärung der Anforderungen an die Vertrauenswürdigkeit des EVG

Die Anforderungen an die Vertrauenswürdigkeit wurden entsprechend der EAL-Stufe 3 (EAL3) ausgewählt. Diese wird im Teil 3 der CC beschrieben und definiert [CCT3, 2007]. Nach Vorgaben der CC für die EAL-Stufe 3 muss ein EVG bei der Evaluation des Sicherheitsverhaltens neben einer Dokumentation für den Gebrauch und einer Spezifikation der Funktionen und Schnittstellen auch eine Beschreibung des architektonischen Aufbaus enthalten. Im Gegensatz zur EAL-Stufe 2 wird bei der EAL-Stufe 3 während der Evaluation ein Augenmerk auf den Aufbau des EVG gelegt. Dies ist insbesondere bei der Untersuchung des EVG auf Backdoors von entscheidender Wichtigkeit. Aus diesem Grund wurde mindestens die EAL-Stufe 3 ausgewählt. Eine höhere Einstufung wird allerdings nicht als angemessen betrachtet, da hierfür eine durchaus aufwändigere Evaluation notwendig wäre. Diese wäre für die Hersteller auch mit höheren Kosten verbunden.
Die EAL-Stufe 3 sieht Kontrollen der Entwicklungsumgebung, ein EVG-Konfigurationsmanagement und Belege der sicheren Auslieferung vor.

SFR	Abhängigkeiten	Auflösung
FAU_GEN.1	FTP_STM.1	Done
FAU_SAR.1	FAU_GEN.1	Done
FAU_SAR.2	FAU_SAR.1	Done
FCS_CKM.1	FCS_CKM.2 o. FCS_COP.1 FCS_CKM.4	FCS_COP.1 keine Löschung von kryptografischen Schlüsseln
FCS_COP.1	FDP_ITC.1 o. FDP_ITC.2 o. FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 keine Löschung von kryptografischen Schlüsseln
FDP_ACC.1	FDP_ACF.1	Done
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Done Standardwerte der Attribute sind nicht sinnvoll
FDP_IFC.1	FDP_IFF.1	Done
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Done Standardwerte der Attribute sind nicht sinnvoll
FDP_IFF.5	FDP_IFC.1	Done
FDP_ITT.1	FDP_ACC.1 o. FDP_IFC.1	FDP_ACC.1 und FDP_IFC.1
FDP_UCT.1	FTP_ITC.1 o. FTP_TRP.1 FDP_ACC.1 o. FDP_IFC.1	FTP_TRP.1 FDP_ACC.1 und FDP_IFC.1
FDP_UIT.1	FDP_ACC.1 o. FDP_IFC.1 FTP_ITC.1 o. FTP_TRP.1	FDP_ACC.1 und FDP_IFC.1 FTP_TRP.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_SOS.1	keine	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	keine	
FMT_MSA.1	FDP_ACC.1 o. FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 und FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.2	FDP_ACC.1 o. FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	FDP_ACC.1 und FDP_IFC.1 FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	keine	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPR_UNL.1	keine	
FPT_STM.1	keine	
FTA_TAH.1	keine	
FTA_TSE.1	keine	
FTP_TRP.1	keine	

Abbildung 6.5: Abhängigkeiten und deren Auflösung.

Literaturverzeichnis

[BMI, 2007] Bundesministerium des Innern (2007): Fragenkatalog des Bundesministeriums der Justiz. Berlin, 22. August 2007.

[BMI2, 2007] Bundesministerium des Innern (2007): Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien. Berlin, 22.08.2007.

[CCT1, 2006] The Common Criteria Recognition Agreement (2006): Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 1, September 2006.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf, Abruf am 11.09.2008.

[CCT2, 2007] The Common Criteria Recognition Agreement (2007): Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Version 3.1, Revision 2, September 2007.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R2.pdf, Abruf am 11.09.2008.

[CCT3, 2007] The Common Criteria Recognition Agreement: Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Version 3.1, Revision 2, September 2007.
http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R2.pdf, Abruf am 11.09.2008.

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik

(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Tobias Kippert, Anastasia Meletiadou, Rüdiger Grimm, Entwurf eines Common Criteria-Schutzprofils für Router zur Abwehr von Online-Überwachung, Arbeitsberichte aus dem Fachbereich Informatik 5/2009

Hannes Schwarz, Jürgen Ebert, Andreas Winter, Graph-based Traceability – A Comprehensive Approach. Arbeitsberichte aus dem Fachbereich Informatik 4/2009

Anastasia Meletiadou, Simone Müller, Rüdiger Grimm, Anforderungsanalyse für Risk-Management-Informationssysteme (RMIS), Arbeitsberichte aus dem Fachbereich Informatik 3/2009

Ansgar Scherp, Thomas Franz, Carsten Saathoff, Steffen Staab, A Model of Events based on a Foundational Ontology, Arbeitsberichte aus dem Fachbereich Informatik 2/2009

Frank Bohdanovicz, Harald Dickel, Christoph Steigner, Avoidance of Routing Loops, Arbeitsberichte aus dem Fachbereich Informatik 1/2009

Stefan Ameling, Stephan Wirth, Dietrich Paulus, Methods for Polyp Detection in Colonoscopy Videos: A Review, Arbeitsberichte aus dem Fachbereich Informatik 14/2008

Tassilo Horn, Jürgen Ebert, Ein Referenzschema für die Sprachen der IEC 61131-3, Arbeitsberichte aus dem Fachbereich Informatik 13/2008

Thomas Franz, Ansgar Scherp, Steffen Staab, Does a Semantic Web Facilitate Your Daily Tasks?, Arbeitsberichte aus dem Fachbereich Informatik 12/2008

Norbert Frick, Künftige Anfordeungen an ERP-Systeme: Deutsche Anbieter im Fokus, Arbeitsberichte aus dem Fachbereicht Informatik 11/2008

Jürgen Ebert, Rüdiger Grimm, Alexander Hug, Lehramtsbezogene Bachelor- und Masterstudiengänge im Fach Informatik an der Universität Koblenz-Landau, Campus Koblenz, Arbeitsberichte aus dem Fachbereich Informatik 10/2008

Mario Schaarschmidt, Harald von Kortzfleisch, Social Networking Platforms as Creativity Fostering Systems: Research Model and Exploratory Study, Arbeitsberichte aus dem Fachbereich Informatik 9/2008

Bernhard Schueler, Sergej Sizov, Steffen Staab, Querying for Meta Knowledge, Arbeitsberichte aus dem Fachbereich Informatik 8/2008

Stefan Stein, Entwicklung einer Architektur für komplexe kontextbezogene Dienste im mobilen Umfeld, Arbeitsberichte aus dem Fachbereich Informatik 7/2008

Matthias Bohnen, Lina Brühl, Sebastian Bzdak, RoboCup 2008 Mixed Reality League Team Description, Arbeitsberichte aus dem Fachbereich Informatik 6/2008

Bernhard Beckert, Reiner Hähnle, Tests and Proofs: Papers Presented at the Second International Conference, TAP 2008, Prato, Italy, April 2008, Arbeitsberichte aus dem Fachbereich Informatik 5/2008

Klaas Dellschaft, Steffen Staab, Unterstützung und Dokumentation kollaborativer Entwurfs- und Entscheidungsprozesse, Arbeitsberichte aus dem Fachbereich Informatik 4/2008

Rüdiger Grimm: IT-Sicherheitsmodelle, Arbeitsberichte aus dem Fachbereich Informatik 3/2008

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik 2/2008

Markus Maron, Kevin Read, Michael Schulze: CAMPUS NEWS – Artificial Intelligence Methods Combined for an Intelligent Information Network, Arbeitsberichte aus dem Fachbereich Informatik 1/2008

Lutz Priese,Frank Schmitt, Patrick Sturm, Haojun Wang: BMBF-Verbundprojekt 3D-RETISEG Abschlussbericht des Labors Bilderkennen der Universität Koblenz-Landau, Arbeitsberichte aus dem Fachbereich Informatik 26/2007

Stephan Philippi, Alexander Pinl: Proceedings 14. Workshop 20.-21. September 2007 Algorithmen und Werkzeuge für Petrinetze, Arbeitsberichte aus dem Fachbereich Informatik 25/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS – an Intelligent Bluetooth-based Mobile Information Network, Arbeitsberichte aus dem Fachbereich Informatik 24/2007

Ulrich Furbach, Markus Maron, Kevin Read: CAMPUS NEWS - an Information Network for Pervasive Universities, Arbeitsberichte aus dem Fachbereich Informatik 23/2007

Lutz Priese: Finite Automata on Unranked and Unordered DAGs Extented Version, Arbeitsberichte aus dem Fachbereich Informatik 22/2007

Mario Schaarschmidt, Harald F.O. von Kortzfleisch: Modularität als alternative Technologie- und Innovationsstrategie, Arbeitsberichte aus dem Fachbereich Informatik 21/2007

Kurt Lautenbach, Alexander Pinl: Probability Propagation Nets, Arbeitsberichte aus dem Fachbereich Informatik 20/2007

Rüdiger Grimm, Farid Mehr, Anastasia Meletiadou, Daniel Pähler, Ilka Uerz: SOA-Security, Arbeitsberichte aus dem Fachbereich Informatik 19/2007

Christoph Wernhard: Tableaux Between Proving, Projection and Compilation, Arbeitsberichte aus dem Fachbereich Informatik 18/2007

Ulrich Furbach, Claudia Obermaier: Knowledge Compilation for Description Logics, Arbeitsberichte aus dem Fachbereich Informatik 17/2007

Fernando Silva Parreiras, Steffen Staab, Andreas Winter: TwoUse: Integrating UML Models and OWL Ontologies, Arbeitsberichte aus dem Fachbereich Informatik 16/2007

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:“E-KRHyper“, Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen“, Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe“
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005