macmon secure GmbH

Sicherheitsvorgaben für *macmon* Version 4.0.9

Autor:

Jürgen Westerkamp

Datum: 28. Oktober 2015

Inhaltsverzeichnis

Versionshistorie

Version	Datum	Autor	Beschreibung
2.0	28.10.2015	JW	Finale Version zur Zertifizierung von *macmon*.

Sicherheitsvorgaben

1 ST-Einleitung

Diese Sicherheitsvorgaben beschreiben die Ziele und Anforderungen für die Sicherheitssoftware *macmon* Version 4.0.9. Hierzu gehören der *macmon*-Server Version 4.0.9 und der Compliance-Agent Version 1.2.9 (siehe auch Kapitel 1.3). Die Form der Sicherheitsvorgaben ist konsistent mit den *Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 4 Final*.

1.1 EVG-Identifikation

ST-Name:	Sicherheitsvorgaben für *macmon* Version 4.0.9
ST-Version:	2.0
Datum:	30. Oktober 2015
Sponsor:	*macmon secure GmbH*
Autor:	Jürgen Westerkamp
EVG-Name:	*macmon*
EVG-Version:	Version 4.0.9
CC-Version:	3.1 Revision 4
EAL-Stufe:	EAL2+ ALC_FLR.1
Suchbegriffe:	NAC, Netzwerkzugriffskontrolle, Network Access Control, Network Admission Control, *macmon*, *macmon*-Appliance

1.2 EVG-Überblick

Das Produkt *macmon* ist ein System zur Kontrolle des Zugriffs von Endgeräten auf ein Netzwerk. Der Einsatz von *macmon* ermöglicht die Verwaltung und Überwachung des Netzwerks und der enthaltenen Komponenten. Damit gehört der EVG zu den Network Access Control (NAC) Systemen. Der Server auf dem *macmon* installiert ist, wird an zentraler Stelle in das bestehende Netzwerk eingebunden (siehe Abbildung 1). Von diesem Server werden unterschiedliche Daten von verschiedenen Geräten im Netzwerk abgefragt. Auf Grundlage der erfassten Daten, wird die Authentifizierung und Autorisierung von Endgeräten vorgenommen. Dadurch wird der Schutz des Netzwerkes und dessen Ressourcen vor unbekannten oder nicht-autorisierten Endgeräten gewährleistet.

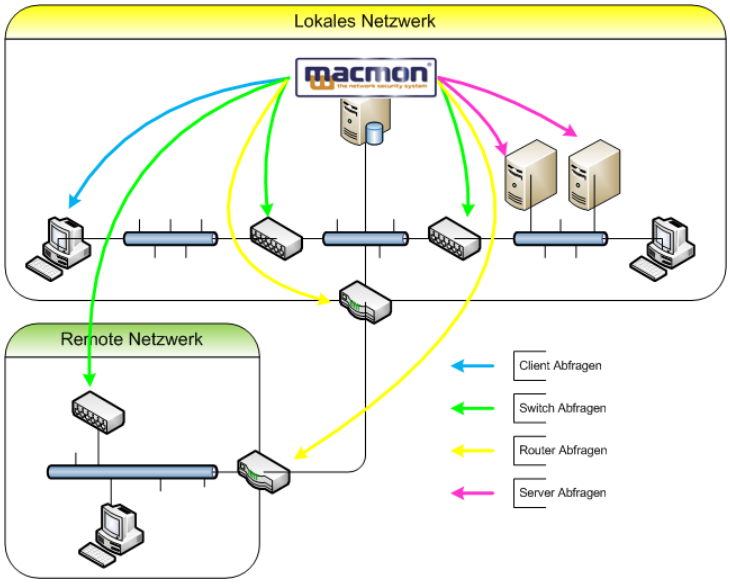

Abbildung 1: Integration von *macmon* in das Netzwerk

1.2.1 Übersicht zur Funktionalität:

Die NAC-Lösung *macmon* bietet die folgenden Möglichkeiten zur Erhöhung der Sicherheit im Netzwerk an:

- Erkennung und Identifizierung aller aktiven Endgeräte im Netzwerk
- Authentifizierung der Endgeräte anhand der MAC-Adresse oder des Fingerprints[1] des Gerätes
- Erfassung weiterer sicherheitsrelevanter Merkmale zu den Endgeräten
- Manuelle oder regelbasierte Kontrolle des Zugriffs auf das Netzwerk
- Überwachung des Netzwerkes und der autorisierten Endgeräte zur Laufzeit
- Erzeugung von Berichten und Statistiken zu Ereignissen im Netzwerk

Die genannten Funktionalitäten werden mithilfe der folgenden Verfahren ermöglicht:

[1] Fingerprint - Eindeutiges Merkmal zum Endgerät bestehend aus internen Daten wie BIOS-ID, CPU-ID, o.ä.

- Erkennung: Zur Erkennung von Endgeräten werden die Statusinformationen von Switchen und Informationen aus ARP-Zwischenspeichern verwendet. Zusätzlich können weiter Identifizierungsmerkmale wie die IP-Adresse, der DNS-Name oder der Hostname von einem DHCP- bzw. DNS-Server abgefragt werden. Diese Informationen können zur leichteren Identifizierung von Geräten vom Administrator genutzt werden.

- Authentifizierung: Um die Identität eines Endgerätes zu prüfen, wird primär die MAC-Adresse verwendet. Des Weiteren können mit Hilfe des Compliance-Agenten interne Eigenschaften eines Endgerätes erfasst werden. Dies können bspw. Seriennummern der CPU oder des BIOS sein. Aus diesen Eigenschaften wird ein eindeutiger Fingerprint für das jeweilige Gerät ermittelt.

- Autorisierung: Zur Autorisierung des Zugriffs auf das Netzwerk schaltet *macmon* virtuelle LANs eines physischen Anschlusses um oder nimmt eine Aktivierung / Deaktivierung des physischen Anschlusses vor. Die Autorisierung kann manuell über die Benutzeroberfläche oder automatisch anhand von benutzerspezifischen Regeln vorgenommen werden.

- Kontrolle: Das Netzwerk wird durch erneute Abfragen der Geräteinformationen periodisch kontrolliert. Bei Erkennung von potenziell sicherheitsrelevanten Events wird anhand des benutzerspezifischen Regelwerks reagiert.

- Monitor: Der aktuelle Status des Netzwerks kann über die Benutzeroberfläche analysiert werden. Statusinformationen der erkannten Geräte, Statistiken und Berichte können hier abgerufen werden.

1.2.2 Benötigte Nicht-EVG Hardware / Software / Firmware:

Der EVG dieser Sicherheitsvorgaben umfasst die Sicherheitssoftware *macmon*. Zum Betrieb des EVGs wird folgende Nicht-EVG Hardware / Software / Firmware vorausgesetzt:

- *macmon*-Appliance: Als Hardware-Plattform für den *macmon*-Server wird die *macmon*-Appliance Version 3.0.3 vorausgesetzt. Die Appliance stellt mit installiertem *macmon*-Server einen einsatzbereiten Management-Server eines NAC-Systems dar. Die Appliance muss folgenden Mindestanforderungen genügen:
  - Hardware:

        * Quad Core CPU mit je 2,4 GHz
        * 4 GB Arbeitsspeicher
        * 250 GB Festplatte
        * 4 mal 1 GBit/s Netzwerkanschlüsse
    - Software:
        * Betriebssystem Linux Kernel 2.6.32
        * Datenbank MySQL 5.1 (DBMS: Datenbank-Management-System)
        * Webserver Apache 2.2.16 (Benötigt für die Authentifizierung von Benutzern des macmon-Servers siehe Kapitel 1.3.2)
        * PHP 5.3.3
        * Mailserver Postfix 2.7.1
        * SNMP Dienst Net-SNMP 5.4.3
        * Statistik-Framework RRDtool 1.4.3

- Web-Browser: Der Zugriff auf den *macmon*-Server geschieht über eine HTTPS-Verbindung zu einer Web-Oberfläche (GUI). Der Web-Browser eines Gerätes, welches für den Zugriff auf die GUI verwendet werden soll, muss das *Transport Layer Security* Protokoll (TLS Version 1.0) und Java Script unterstützen. Folgende Browser werden unterstützt:
    - Internet Explorer ab Version 10
    - Firefox ab Version 24

- Netzwerkverteiler: Switches im verwalteten Netzwerk müssen die Möglichkeit der entfernten Verwaltung unterstützen. Außerdem müssen die Switches die Konfiguration von VLANs anbieten. Für die genannten Funktionalitäten muss das Protokoll SNMP unterstützt werden. Die Switches müssen diesbezüglich die folgenden Standards implementieren:
    - MIB-II[2] (Interface abfragen)
    - IF-MIB[3] (Interface managen)
    - BRIDGE-MIB[4] (MACs abfragen)

[2]MIB-II (RFC 1213) - `http://www.ietf.org/rfc/rfc1213`
[3]IF-MIB (RFC 2863) - `http://www.ietf.org/rfc/rfc2863`
[4]BRIDGE-MIB (RFC 1493) - `http://www.ietf.org/rfc/rfc1493`

  - Q-BRIDGE-MIB[5] (VLANs abfragen und managen)

- Router: Router im verwalteten Netzwerk müssen die Abfrage von ARP-Daten per SNMP unterstützen. Hierzu müssen diese den SNMP Standard MIB-II unterstützen.

- Server: Sollen zur leichteren Identifizierung DNS-Namen und Hostnamen verwendet werden, müssen der DNS- und DHCP-Server konfiguriert werden. Dies ist **nicht** Bestandteil der Zertifizierung und rein als Erleichterung beim Identifizieren von Endgeräten für den Benutzer gedacht. Der DNS-Server muss die Abfrage von DNS-Namen durch den *macmon*-Server entweder via *NSLOOKUP* oder per *Zonentransfer* erlauben. Ein DHCP-Server, der mit dem DHCP-Agenten[6] ausgestattet ist, muss im Netzwerk zur Verfügung stehen. Die Abfrage folgender DHCP-Server wird unterstützt:
  - Novell NDS (entfernte Abfrage über LDAP(S) *möglich*)
  - Windows Server DHCP
  - HaneWIN
  - Linux ISC
  - DHCP QIP
  - Infoblox (entfernte Abfrage HTTPS)

- Endgeräte: Für die Erkennung werden alle Endgeräte unterstützt, die über eine MAC-Adresse verfügen. Um erweiterte interne Informationen zum Endgerät abfragen zu können, muss der Compliance-Agent auf den Endgeräten installiert werden. Welche Endgeräte unterstützt werden, wird in Kapitel 1.3.1 genannt.

- Infrastruktur: Die Unterstützung der genannten Protokolle und die Datenabfrage der genannten Geräte durch den *macmon*-Server muss von der Infrastruktur des Netzwerkes ermöglicht werden. Vorhandene Firewalls im Netzwerk sind gegebenenfalls anzupassen.

[5] Q-BRIDGE-MIB (RFC 4363) - `http://www.ietf.org/rfc/rfc4363`
[6] DHCP-Agent - Script, welcher als Agent auf dem DHCP-Server installiert wird und Daten an den *macmon*-Server sendet.

1.3 EVG-Beschreibung

Der EVG bietet die Überwachung und Verwaltung des Netzwerkes an. Überwacht werden kann dabei jedes im Netzwerk befindliche Gerät mit einer MAC-Adresse. Der EVG besteht aus dem *macmon*-Server, welcher die drei Kernkomponenten der Software enthält, und dem Compliance-Agent (siehe Abbildung 2).

Die drei Kernkomponenten verwenden zur Erfüllung von einigen Sicherheitsfunktionen die zwei Programme OpenSSL und Net-SNMP. Von der Kernkomponente *UI* wird die Bibliothek OpenSSL zur Absicherung der HTTPS-Verbindungen per TLSv1.0 herangezogen. Die Kernkomponenten *Engine* und *EMD* verwenden den Net-SNMP-Client zur Absicherung aller SNMP-Verbindungen per SNMPv3 mit SHA-1 Authentifikation und AES-Verschlüsselung. Diese beiden Programme in der nachfolgenden Version sind dadurch ebenfalls Komponenten des *macmon*-Servers und somit Bestandteile des EVGs:

- OpenSSL Version 0.9.8o
- Net-SNMP-Client 5.4.3

Ein weiterer Bestandteil des EVGs ist eine Datenbank, welche als gemeinsames Speichermedium eingesetzt wird. Die Datenbank wird vom DBMS (siehe MySQL Datenbank, Kapitel 1.2.2) der Betriebsumgebung verwaltet. Das DBMS regelt die Zugriffe auf die TSF-Daten in der Datenbank. Vom DBMS wird ausschließlich **ein lokaler, administrativer** Zugang angeboten, welcher ausschließlich vom *macmon*-Server genutzt wird. Voraussetzung hierfür ist, dass **keine** entfernte Datenbank verwendet wird.

Die folgende Beschreibung gibt genauere Informationen zu den Bestandteilen des EVGs:

- *macmon*-Server (Version 4.0.9): Der *macmon*-Server implementiert die NAC-Funktionalitäten des EVGs. Der Server stellt den zentralen Management-Server des NAC-Systemes dar und bietet alle Managementfunktionen an. Der *macmon*-Server wird im Weiteren synonym als Management-Server bezeichnet. Die folgenden Kernkomponenten sind im Server enthalten:

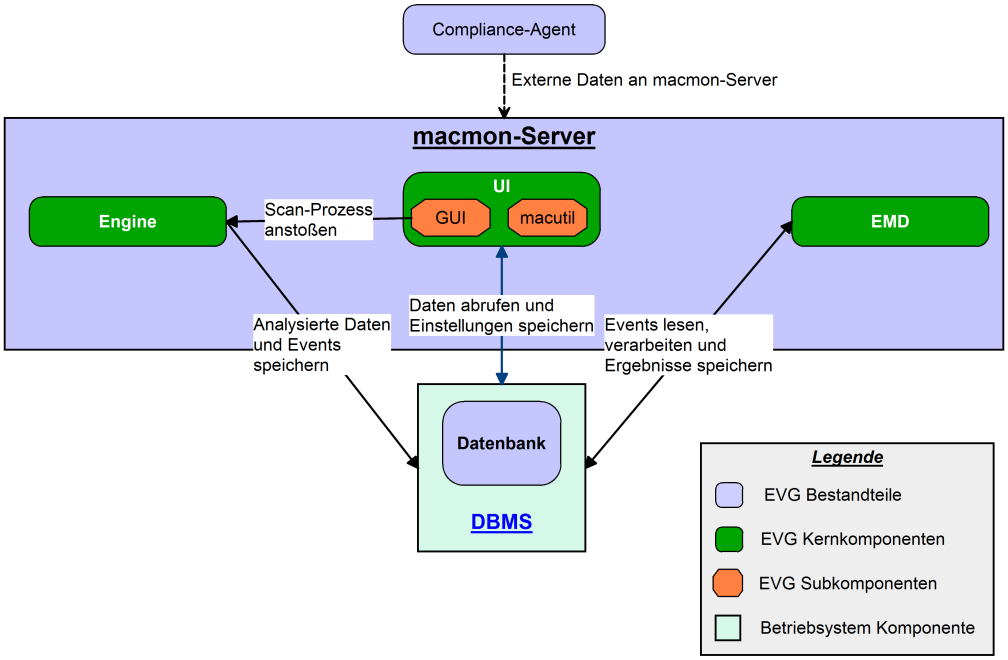

Abbildung 2: Kernkomponenten von *macmon*

- Engine: Die Engine führt die Erfassung von Netzwerkdaten durch. Alle empfangenen Daten werden verarbeitet und in der Datenbank gespeichert. Danach werden die ermittelten Informationen auf spezifische Events hin analysiert. Erkannte Events werden dann mit allen Event-spezifischen Informationen in der Datenbank hinterlegt.
- EMD: Die von der Engine hinterlegten Events werden vom Event Management Daemon verarbeitet und analysiert. Dabei werden die Inhalte der Events anhand eines Regelwerks überprüft. Das Regelwerk besteht aus benutzerspezifischen Regeln, welche vom Administrator verwaltet werden. Jede Regel bezieht sich auf ein bestimmtes Event und kann durch Bedingungen eingegrenzt werden. In den Bedingungen können alle Event-spezifischen Daten und Informationen verwendet werden. Trifft die Bedingung einer oder mehrerer Regeln zu, werden die Aktionen dieser Regeln ausgeführt.
- UI: Die UI Komponente besteht aus zwei Subkomponenten:
  - Die Bedienung des *macmon*-Servers geschieht primär über eine webbasierte Benutzeroberfläche (GUI), auf welche über das HTTPS-

Protokoll zugegriffen werden kann. Alle Konfigurations-, Überwachungs- und Wartungsarbeiten werden von dieser Oberfläche ausgeführt. Des Weiteren bietet die GUI den Zugriff auf die Auditdaten.

  - Alternativ steht die *macutil*-Schnittstelle zur Verfügung. Über *macutil* können rudimentäre Operationen auch lokal mit Befehlen auf der Kommandozeile des Servers aufgerufen werden. Die *macutil*-Schnittstelle ist außerdem auch remote über HTTPS zugreifbar.

- Datenbank: Eine relationale Datenbank stellt den primären Speicher dar. In ihr werden alle Einstellungen, Auditdaten und die vom *macmon*-Server verarbeiteten Netzwerkdaten sowie die erkannten Events gespeichert. Bei der Installation des *macmon*-Servers wird die Datenbank über den Zugang zum DBMS erzeugt. Die Datenbank wird vom DBMS ausschließlich für lokale Zugriffe des *macmon*-Servers verwendet. Die dafür nötige Konfiguration des DBMS wird bei der Installation des *macmon*-Servers durchgeführt.

- Compliance-Agent (Version 1.2.9): Zur Erfassung interner Daten wird eine Agentensoftware auf zu prüfenden Endgeräten im Netzwerk benötigt. Der Agent kann über die GUI herunter geladen werden und muss vom Administrator des Netzwerkes manuell auf den Endgeräten installiert werden. Der Compliance-Agent prüft verschiedene Eigenschaften des Endgerätes und übermittelt die Ergebnisse über eine verschlüsselte Verbindung an den *macmon*-Server. Auf dem Server werden die Daten dann von der Engine analysiert. Welche Eigenschaften ermittelt werden sollen, erfragt der Compliance-Agent beim *macmon*-Server. Die Skripte zum Scannen der Endgeräte werden vom Administrator auf dem *macmon*-Server hinterlegt und vom Compliance-Agenten bei Bedarf heruntergeladen. Die Skripte werden dabei durch eine Signatur vor Manipulationen geschützt.

1.3.1 Physischer Umfang:

Der physische Umfang legt die im EVG enthaltenen Bestandteile fest. Dabei handelt es sich ausschließlich um den *macmon*-Server mit der Datenbank und dem Compliance-Agenten. Der *macmon*-Server wird auf der in 1.2.2 definierten Appliance installiert.

Der Compliance-Agent ist ausschließlich für Systeme auf Basis von Microsoft

Windows 7 einsetzbar. Außerdem wird eine installierte **32bit** Java VM (mindestens JRE Version 1.6) auf dem Endgerät vorausgesetzt.

Zusätzlich dazu umfasst der EVG die folgenden Dokumente:

1. *macmon* appliance Inbetriebnahme: Handbuch mit Beschreibungen zur Inbetriebnahme der *macmon*-Appliance.
2. *macmon* appliance Manual: Handbuch mit Beschreibungen zur Appliance-Hardware und der Konfigurationsoberfläche der *macmon*-Appliance.
3. *macmon* Handbuch: Handbuch zur Erläuterung der Funktionen und Verwaltung des *macmon*-Servers.
4. *macmon* Common Criteria Handbuch: Handbuch mit zusätzlichen Beschreibungen zur Installation, Konfiguration und Inbetriebnahme von *macmon* im Common Criteria konformen Zustand.

1.3.2 Logischer Umfang:

Der logische Umfang legt die vom EVG angebotenen Sicherheitsfunktionen fest. Die im Folgenden beschriebene Funktionalität wird durch den EVG geboten.

Audit: Der EVG generiert Auditdaten für sicherheitsrelevante Ereignisse. Die Ereignisse beziehen sich zum einen auf gesammelte Daten und Events im verwalteten Netzwerk und zum anderen auf Benutzeraktionen am Management-Server. Jeder generierte Auditeintrag wird in der Datenbank abgelegt und ist nur für autorisierte Benutzer des Management-Servers verfügbar.

Identifikation und Authentifizierung: Zur Authentifizierung eines Benutzers vor dem Zugriff auf die Oberfläche wird ein Teil des Authentifizierungsverfahrens vom Web-Server, welcher Bestandteil der Betriebsumgebung (siehe auch Kapitel 1.2.2) ist, vorgenommen. Der verwendete Apache Web-Server führt die Verifizierung des Passwortes eines Benutzers durch und leitet das Ergebnis weiter an den EVG. Der EVG führt die Identifikation jedes Benutzers des Management-Servers durch und kontrolliert die Berechtigungen, bevor dieser Zugriff zum administrativen Zugang erhält. Der Zugang zu Management- oder Auditfunktionen wird bis zur erfolgreichen I&A verweigert.

Management: Der EVG bietet Managementfunktionen, um die Kontrolle und Überwachung des EVGs zu ermöglichen. Zur Differenzierung des Zugangs zu den Funktionen des Management-Servers, werden verschiedene Benutzergruppen (Rollen) unterstützt.

Netzwerkzugriffskontrolle (NAC): Der EVG kontrolliert den Zugriff von Endgeräten auf das verwaltete Netzwerk. Dabei wird der Zugriff für Endgeräte manuell oder anhand von Richtlinien entschieden. Diese Richtlinien werden in Form von benutzerspezifischen Regeln am Management-Server konfiguriert und verwaltet. Der EVG überwacht dazu das verwaltete Netzwerk und erfasst sicherheitsrelevante Daten. Durch Analyse der Daten werden neue Geräte, nicht-autorisierte Geräte oder Geräte, die nicht den Sicherheitsrichtlinien entsprechen, identifiziert.

Bei Einsatz des Compliance-Agenten auf den Endgeräten, können durch den Management-Server komplexe Sicherheitsrichtlinien für alle Endgeräte im Netzwerk durchgesetzt werden. Bspw. kann die Aktivierung eines Virenscanners oder einer Firewall kontrolliert werden. Der Ausfall eines Compliance-Agenten ist hierbei unkritisch, da dann das Endgerät automatisch als nicht konform zu den Sicherheitsrichtlinien gilt.

Bei Erkennung von sicherheitsrelevanten Ereignissen werden Maßnahmen gemäß den Regeln durchgeführt. Als Maßnahmen bietet der EVG das Auslösen eines Alarms und die Ablehnung bzw. den Widerruf einer Autorisierung des Zugriffs auf das Netzwerk an.

1.3.3 Konfiguration des EVGs:

Dieses Kapitel legt fest, wie der EVG und die Betriebsumgebung zur Common Criteria Evaluierung konfiguriert werden müssen. Zur Sicherstellung der definierten Anforderungen aus diesen Sicherheitsvorgaben muss diese Konfiguration eingehalten werden.

Für den Einsatz des EVGs muss die Einsatzumgebung mindestens folgende Komponenten aufweisen:

a) Eine Instanz der *macmon*-Appliance

b) Managebare Switches mit VLAN-Unterstützung

c) Router mit Unterstützung der Abfrage von ARP-Daten

d) Endgeräte mit installiertem Compliance-Agenten

e) Endgeräte ohne Compliance-Agent mit einer festen Zuordnung zu einem bestimmten Netzwerkanschluss

Der EVG wird mit der folgenden Konfiguration eingesetzt:

a) Installation und Konfiguration der Appliance anhand des *macmon* Common Criteria Handbuchs

b) Konfiguration aller Netzwerkverteiler anhand des *macmon* Common Criteria Handbuchs

c) Konfigurierter Router anhand des *macmon* Common Criteria Handbuchs

1.3.4 TSF-Daten:

Die folgende Tabelle 2 beschreibt die Daten der TSF, die vom EVG genutzt werden.

TSF-Daten	Beschreibung
Systemparameter	Einstellungen zur Konfiguration des EVGs, hierzu gehören die folgenden Bereiche: • Engine Einstellungen • GUI Einstellungen • EMD Einstellungen • Compliance Einstellungen • Datenbank Einstellungen • Event Einstellungen

TSF-Daten	Beschreibung
Actions	Regelwerk zur Behandlung von Events im Netzwerk und Reaktionen auf diese. Jede Regel hat folgende Attribute: • Eindeutiger Name • Event • Periode • Bedingung • Kommando (Reaktion)
Benutzer-Accounts	Konten für autorisierte Benutzer des Management-Servers. Jeder Account ist mit den folgenden Attributen assoziiert: • Status (Aktiv / Inaktiv) • User-ID • User-Name • Passwort • Rolle • *Optional: Beschreibung* • *Optional: E-Mail-Adresse*

TSF-Daten	Beschreibung
Netzwerkkomponenten-Parameter	Eigenschaften und Abfrageeinstellungen zu den verwalteten Netzwerkkomponenten. Hierzu gehören: • IP-Adresse • Geräte-Klasse • Geräte-Gruppe • Scan-Methoden • Scan-Einstellungen (Intervalle, Wartezeiten, etc.) • Zugangsdaten

TSF-Daten	Beschreibung
Endgeräte-Parameter	Attribute eines Endgerätes, welche beim Scannen des Netzwerkes vom EVG erfasst werden. Hierzu gehören: • MAC-Adresse • Interface (Switch-ID + Interface-ID) • Endgeräte-Gruppe • IP-Adresse • VLAN-ID • Fingerprint • Sicherheitskonfiguration • Status (Autorisiert, Nicht-Autorisiert, Neu) Zusätzliche Informationen vom Agenten fließen in den Fingerprint und die Sicherheitskonfiguration ein. Welche Informationen dies sind, wird vom Benutzer definiert. Diese Informationen können dann zusätzlich im Regelwerk verwendet werden.

Tabelle 2: Beschreibung der TSF-Daten

2 Antrag auf Konformität

Diese Sicherheitsvorgaben stellen Anspruch auf Konformität zu

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012, CCMB-2012-09-001

2. Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 3.1, Revision 4, September 2012,

CCMB-2012-09-002

3. Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003

wie folgt:

- Part 2 erweitert
- Part 3 konform
- Paket EAL2 erweitert durch ALC_FLR.1

Diese Sicherheitsvorgaben stellen keinen Anspruch auf Konformität zu einem Schutzprofil.

3 Definition der Sicherheitsumgebung

In diesem Kapitel wird die Sicherheitsumgebung für den Evaluierungsgegenstand definiert. Zu Anfang werden hierzu Grundlagen für die Definition beschrieben. Danach werden alle vom EVG abzuwehrenden Bedrohungen aufgeführt. Außerdem werden Annahmen an die Umgebung, in welcher der EVG eingesetzt wird, beschrieben. Diese Annahmen stellen Auflagen an den Betrieb des EVGs dar. Als Letztes werden organisatorische Sicherheitsrichtlinien, welche für den EVG gelten, beschrieben.

3.1 Grundlagen

Im Folgenden werden verschiedene Grundlagen für die Definition der Sicherheitsumgebung beschrieben.

3.1.1 Rollen im EVG:

Die nachfolgenden definierten Rollen werden vom EVG standardmäßig vorgegeben:

- Administrator:
  - Benutzer mit vollem Zugriff auf den EVG. Der Administrator ist der einzige Benutzer mit vollem Zugriff auf die Konfiguration des EVGs, einschließlich der Benutzerverwaltung.
- Operator:
  - Benutzer mit vollem Zugriff auf die Konfiguration des EVGs. Der Operator hat alle Rechte des Administrators ausgenommen dem Zugriff auf die Benutzerverwaltung.
- Helpdesk:
  - Benutzer mit beschränktem Zugriff auf die Konfiguration des EVGs. Der Zugriff beschränkt sich auf die Verwaltung von Endgeräten und Endgeräte-Gruppen. Der Helpdesk hat so das Recht, Endgeräte manuell zu autorisieren. Außerdem erhält der Helpdesk Lese-Zugriff auf alle Auditdaten, die mit den Endgeräten in Verbindung stehen.
- Revisor:
  - Benutzer mit Lese-Zugriff für den EVG. Der Revisor hat ausschließlich Lese-Berechtigung für alle Bereiche des EVGs.

- Nicht-autorisierter Benutzer:
  - Benutzer, der keiner der genannten Rollen angehört. Dieser Benutzer verfügt über keine Zugangsdaten und erhält keinerlei Zugriff auf Funktionen des EVGs.

Benutzer-definierte Rollen mit erweiterten bzw. reduzierten Rechten können vom Administrator zusätzlich zu den genannten Rollen definiert werden.

3.1.2 Definition zu schützender Werte:

In der folgenden Definition werden die zu schützenden Werte, für welche Risiken durch die Bedrohungen aus Kapitel 3.2 bestehen, beschrieben.

- Netzwerk: Hierbei handelt es sich um das vom EVG verwaltete Netzwerk bzw. die Ressourcen und Kommunikation im Netzwerk. Das verwaltete Netzwerk umfasst alle Netzwerksegmente, welche vom EVG durch die Erfassung von Daten kontrolliert werden. Schützenswert ist konkret der Zugriff bzw. die Ermittlung folgende Bestandteile des Netzwerks durch unbefugte Personen:
  - ungesicherte (offene) Netzwerkressourcen
  - Netzwerktopologieinformationen
  - Netzwerkkommunikation (E-Mail, Passwörter, u.ä.)
- Management-Server: Hierbei handelt es sich um den Management-Server und dessen Ressourcen. Als schützenswert sind die folgenden vier Bereiche anzusehen:
  1. Administrativer Zugang: Dieser Zugang bezieht sich auf die Benutzerschnittstellen zu administrativen Funktionen des Management-Servers.
  2. Physischer Zugang: Dieser bezieht sich auf den direkten physikalischen Zugang zur Hardware des Management-Servers oder der Betriebsumgebung.
  3. Ressourcen: Hierbei handelt es sich um die Ressourcen des Management-Servers, wie Programmdateien oder den Datenspeicher.
  4. Kommunikation: Hiebei handelt es sich um die Kommunikation des Management-Servers über das Netzwerk. Zum einen betrifft dies entfernte Verbindungen eines Benutzers zur Benutzerschnittstelle und zum

anderen Verbindungen des Servers zu Netzwerkkomponenten und Endgeräten im verwalteten Netzwerk.

- Autorisierte Endgeräte: Hierbei handelt es sich um alle Endgeräte, welche vom Administrator für den Zugriff auf das verwaltete Netzwerk autorisiert sind. Unterschieden werden privilegierte Endgeräte mit installiertem Compliance-Agenten und unterprivilegierte Endgeräte, welche ausschließlich über ihre MAC-Adresse identifiziert werden können.

- Auditdaten: Hierbei handelt es sich um alle vom Management-Server gesammelten Daten. Die Auditdaten werden im Datenspeicher des EVGs (Datenbank) gespeichert. Diese Daten umfassen Informationen zum verwalteten Netzwerk und Informationen zu vorgenommenen Änderungen an Einstellungen des Management-Servers durch autorisierte Benutzer.

3.1.3 Definition der Angreifer / Rollen:

Die im Folgenden als Angreifer bezeichnete Person gehört der Rolle eines nicht-autorisierten Benutzers an. Dieser Benutzer verfügt über einen geringen Grad an technischer Expertise (EAL2 Attack-Potenzial Basic). Ein Benutzer eines autorisierten Endgerätes, welcher das Endgerät nicht konform zu den Sicherheitsrichtlinien verändert, wird ebenfalls als Angreifer angesehen. Als Ressourcen benötigt der Angreifer, für die in Kapitel 3.2 genannten Bedrohungen, ein netzwerkfähiges Gerät, welches unter seiner Kontrolle steht. Beweggrund für den Angreifer ist folgendes:

- Motivation: Erlangen des Zugriffs auf das Netzwerk bzw. dessen Daten und Ressourcen, wie ein Benutzer mit einem autorisierten Endgerät.

- Möglichkeiten: Zugang zum Netzwerk mit einem Endgerät, welches evtl. nicht den Sicherheitsrichtlinien entspricht. Hierdurch können bspw. Exploitation Tool (bspw. Cain & Abel, Metasploit Framework, o.ä.) zum Einsatz kommen, Viren in das Netzwerk eingeschleust, oder Endgerät mit veralteter Software und darin enthaltenen Sicherheitslücken im Netzwerk verwendet werden. Dies ermöglicht potenziell weitere Angriffe, wie Ausspähen der Netzwerkkommunikation, Zugriff auf im Netzwerk frei verfügbare Ressourcen oder Ermittlung sensibler Daten wie die Netzwerktopologieinformationen.

3.2 Bedrohungen

T.DEV_UNAUTH	Nicht-autorisierte Geräte: Ein Angreifer könnte ein unbekanntes oder nicht-autorisiertes Gerät über eine für ihn zugängliche Netzwerkschnittstelle mit dem Netzwerk verbinden. Die Verbindung ermöglicht dem Angreifer den unbefugten Zugriff auf das Netzwerk über ein von ihm kontrolliertes Gerät.
T.DEV_MASK	Maskierte Geräte: Ein Angreifer könnte ein nicht-autorisiertes Gerät mit der Identität (Manipulation der MAC-Adresse) eines autorisierten Gerätes maskieren. Dieses maskierte Gerät könnte er über eine für ihn zugängliche Netzwerkschnittstelle mit dem Netzwerk verbinden. Die Verbindung ermöglicht dem Angreifer den unbefugten Zugriff auf das Netzwerk über ein von ihm kontrolliertes Gerät. Der Zugriff erfolgt dabei mit der Identität eines autorisierten Gerätes.
T.DEV_MANIP	Manipulierte Geräte: Ein bereits autorisiertes Gerät, welches an das Netzwerk angeschlossen ist, könnte nach Manipulationen oder Änderungen, die nicht den Sicherheitsrichtlinien entsprechen, weiterhin die Verbindung zum Netzwerk aufrechterhalten. Dies ermöglicht einem Angreifer den unbefugten Zugriff auf das Netzwerk mit einem Gerät, welches nicht den Sicherheitsrichtlinien entspricht.

T.SYS_ACCESS	Unberechtigter Zugriff zum System: Ein Angreifer könnte über den administrativen Zugang des Management-Servers unbefugt Zugriff auf dessen Managementfunktionen erlangen. Dies ermöglicht dem Angreifer den Management-Server zu kontrollieren und damit Sicherheitsfunktionen des EVGs zu umgehen oder zu deaktivieren.
T.COM_PRIVACY	Vertraulichkeit der Kommunikation: Ein Angreifer kann Informationen aus einer Verbindung zur Benutzerschnittstelle des Management-Servers oder der Kommunikation zwischen Management-Server und Netzwerkkomponenten ausspähen. Die enthaltenen Informationen kann der Angreifer für weiterführende Angriffe verwenden.
T.COM_INTEG	Integrität der Kommunikation: Ein Angreifer kann übermittelte Informationen aus einer Verbindung zur Benutzerschnittstelle des Management-Servers oder der Kommunikation zwischen Management-Server und Netzwerkkomponenten manipulieren. Dadurch kann der Angreifer Sicherheitsfunktionen des EVGs deaktivieren.

3.3 Annahmen

A.ENV_SERVER	Physikalischer Schutz des Management-Servers: Der Management-Server muss in einer physikalisch abgesicherten Umgebung betrieben werden, darf nicht öffentlich im Internet erreichbar sein und muss vor Ausfällen geschützt sein.

A.ENV_DATA	Zugriff auf Daten des EVGs: Die TSF-, Konfigurations- und Auditdaten des EVGs und die zur Speicherung verwendeten Ressourcen müssen vor direkten Zugriffen über die Betriebsumgebung durch unbefugte Personen geschützt sein.
A.ENV_AVAIL	Verfügbarkeit von Ressourcen: Die vom EVG benötigte Hardwareplattform und die darauf installierte Software müssen dem EVG zur Verfügung stehen.
A.NET_SUPPORT	Hardware- und Protokoll-Unterstützung: Das Netzwerk unterstützt die benötigten Protokolle und enthält alle geforderten Komponenten, welche ordnungsgemäß funktionieren.
A.DEV_CONTROL	Absicherung autorisierter Geräte: Ein privilegiertes Endgerät muss vor **administrativen** Zugriffen und ein unterprivilegiertes Endgerät und dessen physikalischer Netzwerkanschluss vor physikalischen Zugriffen durch unbefugte Personen geschützt werden. Darüber hinaus muss für jedes unterprivilegiertes Endgerät eine feste Zuordnung des Netzwerkanschlusses zur MAC-Adresse im Management-Server hinterlegt sein.
A.INI_SERVER	Installation des Management-Servers: Der Management-Server wird vom verantwortlichen Administrator anhand der Installationsanleitung installiert und konfiguriert.

A.INI_AGENT	Installation der Agenten: Der Compliance-Agent wird auf allen privilegierten Endgeräten, anhand der Installationsanleitung installiert.
A.ADM_QUAL	Qualifizierter Administrator: Der verantwortliche Administrator muss ausreichend qualifiziert und geschult sein, um das System zu bedienen.
A.ADM_NONEVIL	Nicht korrupter Administrator: Der verantwortliche Administrator hat keine böswilligen Absichten.
A.AUD_BACKUP	Backup der Auditdaten: Von den Auditdaten müssen regelmäßig Sicherheitskopien erzeugt werden.

3.4 Organisatorische Sicherheitsrichtlinien

Die folgenden Richtlinien sind als organisatorische Sicherheitsrichtlinien anzusehen, da diese im Allgemeinen von einem Sicherheitsprodukt gefordert wird.

P.SYS_MANAGE	Verfügbarkeit von Managementfunktionen: Der EVG muss autorisierten Benutzern alle nötigen Funktionen zur Verwaltung des EVGs zur Verfügung stellen.
P.SYS_FUNCS	Ausfall von Sicherheitsfunktionen: Der EVG muss autorisierten Benutzern ermöglichen, den Ausfall einer EVG-Komponente zu erkennen, wenn dies die Sicherheitsleistung des EVGs beeinträchtigt.

P.AUD_DETECT	Verfügbarkeit von Auditreviewfunktionen: Der EVG muss autorisierten Benutzern alle nötigen Funktionen zur Erkennung von sicherheitskritischen Änderungen an den Einstellungen des EVGs oder bereits durchgeführter Angriffe in den Auditdaten zur Verfügung stellen. Anderenfalls könnten Fehlkonfigurationen einen Angriff ermöglichen, bereits stattgefundene Angriffe nicht entdeckt oder gleichartige Angriffe nicht verhindert werden.

4 Sicherheitsziele

In diesem Kapitel werden die Sicherheitsziele für den EVG und die Betriebsumgebung dargestellt.

4.1 Sicherheitsziele für den EVG:

O.NAC_DETECT	Erkennung von Events: Der EVG soll alle relevanten Daten im Netzwerk erfassen und sicherheitskritische Events erkennen.
O.NAC_REACT	Reaktion auf Events: Der EVG soll auf erkannte sicherheitskritische Events im Netzwerk mit angemessenen Maßnahmen reagieren.
O.MAN_FUNCS	Erkennung von Ausfällen kritischer EVG-Komponenten: Der EVG soll selbst erkennen, wenn einzelne sicherheitskritische Komponenten des EVGs ausfallen und dies für autorisierte Benutzer ersichtlich machen.
O.MAN_ROLES	Benutzerrollen: Der EVG soll die Rollen Administrator, Operator, Helpdesk und Revisor anbieten. Ein authentifizierter Benutzer erhält, abhängig von seiner Rolle, Zugriff auf die Funktionen und Daten des EVGs.
O.MAN_MANAGE	Managementfunktionen des EVGs: Der EVG soll einem autorisierten Benutzer zur Verwaltung und Konfiguration benötigte Funktionen zur Verfügung stellen.

O.MAN_COMM	Gesicherte Kommunikation: Die Kommunikation zwischen Management-Server, Compliance-Agent und Netzwerkkomponenten, sowie die Kommunikation bei einer entfernte Verbindung zum administrativen Zugang des Management-Servers soll vom EVG verschlüsselt und verifizierbar abgewickelt werden.
O.AUD_GEN	Generierung von Auditdaten: Der EVG soll zu allen erkannten Events im Netzwerk und bei Änderungen der Konfiguration des EVGs Einträge in den Auditdaten erzeugen.
O.AUD_REVIEW	Anzeige von Auditdaten: Der EVG soll die Möglichkeit bieten, Auditdaten in einer für den Benutzer lesbaren Form anzuzeigen.

4.2 Sicherheitsziele für die Betriebsumgebung:

OE.I&A_AUTH	Authentifizierung von Benutzern: Die Betriebsumgebung soll einen Authentifizierungsmechanismus bereit stellen, über den ausschließlich die autorisierten Benutzer Zugriff zur administrativen Schnittstelle des EVGs erhalten.
OE.ENV_PROTECT	Schutz des Management-Servers: Die vom Management-Server benötigte Hardwareplattform und die darauf enthaltenen Softwareressourcen sollen vor physikalischen und logischen Zugriffen durch unberechtigte Personen geschützt sein und der Zugriff soll nur vom internen Netzwerk möglich sein.

OE.ENV_RESOURCE	Verfügbarkeit von Ressourcen: Die Hardwareplattform (macmon-Appliance, siehe Kapitel 1.2.2) und die darauf installierte Software sollen dem EVG zur Verfügung stehen, um dessen Funktionsfähigkeit zu gewährleisten.
OE.ENV_NETWORK	Unterstütztes Netzwerk: Der EVG soll in das bestehende Netzwerk integrierbar sein und benötigte Protokolle sollen von den Netzwerkkomponenten unterstützt werden. Die Netzwerkanschlüsse eines unterprivilegierten Endgerätes müssen vor unbefugten Zugriffen geschützt sein.
OE.ENV_DEV	Schutz der autorisierten Endgeräte: Vom Administrator autorisierte Endgeräte mit Compliance-Agent sollen vor administrativen Zugriffen durch unberechtigte Personen gesichert sein. Autorisierte unterprivilegierte Endgeräte ohne Compliance-Agent sollen zusätzlich vor physikalischen Zugriffen durch unbefugte Personen geschützt und im Management-Server mit einer festen Zuordnung zu einem Netzwerkanschluss gekannt sein.
OE.EVG_INSTALL	Installation des EVGs: Der EVG soll ordnungsgemäß geliefert, installiert und konfiguriert werden. Der Verantwortliche soll dabei nach der Installationsanleitung des Herstellers handeln.
OE.EVG_ADMIN	Adminstator des EVGs: Der Administrator des EVGs soll qualifiziert und geschult sein den EVG zu bedienen. Der Administrator soll keine böswilligen Absichten haben.
OE.EVG_USER	Alle Benutzer: Alle Benutzer des EVGs und der autorisierter Endgeräte sollen sicherstellen, dass ihre Zugangsdaten nicht für Dritte zugänglich sind.

OE.AUD_MIRROR	Sicherung der Auditdaten: Es sollen regelmäßige Sicherheitskopien der Auditdaten erstellt werden.
OE.AUD_TIME	Zeitstempel für Auditdaten: Die Betriebsumgebung soll brauchbare Zeitstempel für die korrekte Erzeugung von Auditeinträgen liefern.

4.3 Argumentation zu den Sicherheitszielen:

Die Tabelle 8 auf Seite 35 zeigt eine Übersicht zur Abdeckung der Bedrohungen, Annahmen und Sicherheitsrichtlinien durch die Sicherheitsziele. Inwieweit die Sicherheitsziele diese abdecken wird im Folgenden beschrieben.

Die Bedrohung **T.DEV_UNAUTH** bezieht sich auf unbekannte oder nicht-autorisierte Geräte im Netzwerk. O.NAC_DETECT stellt sicher, dass alle Daten im Netzwerk erfasst werden, um nicht-autorisierte Geräte zu erkennen. Durch O.NAC_REACT wird sicher gestellt, dass auf solche sicherheitsrelevanten Ereignisse reagiert wird.

Die Bedrohung **T.DEV_MASK** bezieht sich auf maskierte, nicht-autorisierte Geräte im Netzwerk. O.NAC_DETECT stellt sicher, dass alle Daten im Netzwerk erfasst werden, um maskierte Geräte zu erkennen. Durch O.NAC_REACT wird sicher gestellt, dass auf solche sicherheitsrelevanten Ereignisse regiert wird. Zusätzlich stellen OE.ENV_DEV und OE.ENV_NETWORK sicher, dass alle autorisierten Geräte sowie die Netzwerkanschlüsse unterprivilegierter Geräte geschützt werden und im Management-Server feste Zuordnungen von unterprivilegierten Endgeräten zu Netzwerkanschlüssen bekannt sind.

Die Bedrohung **T.DEV_MANIP** bezieht sich auf autorisierte Geräte im Netzwerk, die nicht konform zu den Sicherheitsrichtlinien sind. O.NAC_DETECT stellt sicher, dass alle Daten im Netzwerk erfasst werden, um nicht-konforme Geräte zu erkennen. Durch O.NAC_REACT wird sicher gestellt, dass auf solche sicherheitsrelevanten Ereignisse reagiert wird. Zusätzlich stellt OE.ENV_DEV sicher, dass der Compliance-Agent auf autorisierten privilegierten Geräten vor unbefugten Zugriffen geschützt ist.

Die Bedrohung **T.SYS_ACCESS** bezieht sich auf unberechtigte Zugriffe auf den EVG. OE.I&A_AUTH und O.MAN_ROLES stellen sicher, dass nur autorisierte Benutzer mit den spezifischen Rechten ihrer Rolle auf die administrative Schnittstelle des EVGs zugreifen können. OE.ENV_PROTECT stellt sicher, dass nur autorisierte Benutzer einen physikalischen Zugriff zum EVG erhalten. OE.EVG_USER stellt zusätzlich sicher, dass die Zugangsdaten dieser Benutzer nicht von Dritten in Erfahrung gebracht werden können. Außerdem stellt OE.ENV_RESSOURCE sicher, dass die Betriebsumgebung alle benötigten Ressourcen zur Verschlüsselung der Kommunikation zur Verfügung stellt.

Die Bedrohung **T.COM_PRIVACY** bezieht sich auf die Vertraulichkeit von Informationen, die zwischen dem Management-Server und Netzwerkgeräten ausgetauscht werden. O.MAN_COMM stellt sicher, dass die Kommunikation zwischen den Komponenten vom EVG verschlüsselt und damit vor Offenlegung durch unbefugte Dritte geschützt ist. OE.ENV_RESSOURCE stellt sicher, dass die Betriebsumgebung alle benötigten Ressourcen zur Verschlüsselung der Kommunikation zur Verfügung stellt. Außerdem wird durch O.ENV_NETWORK die Unterstützung der Verschlüsselung durch das Netzwerk und dessen Komponenten sichergestellt.

Die Bedrohung **T.COM_INTEG** bezieht sich auf die Integrität von Informationen die zwischen Management-Server und Netzwerkgeräten ausgetauscht werden. O.MAN_COMM stellt sicher, dass übermittelte Daten verifizierbar sind und Manipulationen erkannt werden. OE.ENV_RESSOURCE stellt sicher, dass die Betriebsumgebung alle benötigten Ressourcen zur Verifizierung der übermittelten Daten zur Verfügung stellt. Außerdem wird durch O.ENV_NETWORK die Unterstützung der Verifizierung durch das Netzwerk und dessen Komponenten sichergestellt.

Die Annahme **A.ENV_SERVER** bezieht sich auf die physikalische und logische Absicherung des Servers. OE.ENV_PROTECT stellt sicher, dass der Server in einer physikalisch abgesicherten Umgebung betrieben wird und der Zugriff auf den Server nur vom internen Netzwerk möglich ist. OE.ENV_RESOURCE stellt sicher, dass alle Ressourcen, welche für den Betrieb des EVGs benötigt werden, von der Betriebsumgebung zur Verfügung gestellt werden.

Die Annahme **A.ENV_DATA** bezieht sich auf unbefugte Zugriffe auf den

Datenspeicher des EVG mit dessen Konfiguration und den Auditdaten. Das Sicherheitsziel OE.ENV_PROTECT stellt sicher, dass die Ressourcen, welche Programmdateien, Konfigurationsdateien oder Auditdaten beinhalten, vor unbefugten Zugriffen geschützt sind.

Die Annahme **A.ENV_AVAIL** bezieht sich auf die Verfügbarkeit der Ressourcen. OE.ENV_RESSOURCE stellt sicher, dass alle zur Funktionsfähigkeit des EVGs benötigten Ressourcen dem EVG zur Verfügung stehen.

Die Annahme **A.NET_SUPPORT** bezieht sich auf die Unterstützung des EVGs durch das bestehende Netzwerk. OE.ENV_NETWORK stellt sicher, dass das Netzwerk alle benötigten Komponenten enthält und diese die vorausgesetzten Protokolle und Funktionen anbieten.

Die Annahme **A.DEV_CONTROL** bezieht sich auf den Schutz des administrativen Zugangs auf autorisierte Geräte und die zusätzliche Absicherung der physikalischen Netzwerkanschlüsse unterprivilegierter autorisierter Geräte vor Zugriffen durch unbefugte Personen. Die Ziele OE.ENV_DEV und OE.EVG_USER stellen sicher, dass alle autorisierten Geräte geschützt sind und die Zugangsdaten eines autorisierten Benutzers nicht von Dritten in Erfahrung gebracht werden können. Zusätzlich stellt OE.ENV_NETWORK sicher, dass der Netzwerkanschluss unterprivilegierter Geräte geschützt ist.

Die Annahme **A.INI_SERVER** bezieht sich auf die Installation des Management-Servers. OE.EVG_INSTALL stellt sicher, dass der Management-Server ordnungsgemäß anhand der Installationsanleitung des Herstellers installiert wird.

Die Annahme **A.INI_AGENT** bezieht sich auf die Installation des Compliance-Agenten. OE.EVG_INSTALL stellt sicher, dass der Compliance-Agent ordnungsgemäß anhand der Installationsanleitung des Herstellers installiert wird.

Die Annahme **A.ADM_QUAL** bezieht sich auf die Qualifikation des verantwortlichen Administrators. OE.EVG_ADMIN stellt sicher, dass dieser ausreichend geschult und qualifiziert ist, um den EVG ordnungsgemäß zu installieren, zu konfigurieren und zu betreiben.

Die Annahme **A.ADM_NONEVIL** bezieht sich auf die Loyalität des Admi-

nistrators. OE.EVG_ADMIN stellt sicher, dass der verantwortliche Administrator keine böswilligen Absichten hat.

Die Annahme **A.AUD_BACKUP** bezieht sich auf die Erstellung von Sicherheitskopien der Auditdaten. OE.AUD_MIRROR stellt sicher, dass die Daten regelmäßig gesichert werden.

Die Sicherheitsrichtlinie **P.SYS_MANAGE** bezieht sich auf die Verfügbarkeit von Funktionen zum Management des EVGs. O.MAN_MANAGE stellt sicher, dass der EVG alle nötigen Funktionen zur Verwaltung und Konfiguration des EVGs für autorisierte Benutzer zur Verfügung stellt.

Die Sicherheitsrichtlinie **P.SYS_FUNCS** bezieht sich auf das Erkennen eines Ausfalls einzelner sicherheitskritischer EVG-Komponenten durch den EVG selbst. Das Sicherheitsziel O.MAN_FUNCS stellt sicher, dass der EVG selbst erkennen kann, wenn einzelne sicherheitskritische Komponenten des EVGs ausfallen, und dies für autorisierte Benutzer erkenntlich macht.

Die Sicherheitsrichtlinie **P.AUD_DETECT** bezieht sich auf Verfügbarkeit von Funktionen zur Erkennung von sicherheitsrelevanten Events in den Auditdaten. O.AUD_GEN stellt sicher, dass die Auditdaten erzeugt werden und alle nötigen Informationen enthalten sind. OE.AUD_TIME stellt sicher, dass zur Erzeugung der Auditdaten zuverlässige Zeitstempel zur Verfügung stehen. O.AUD_REVIEW stellt sicher, dass die Auditdaten in einer Form vom EVG angeboten werden, die zur Prüfung bzw. zur Erkennung von sicherheitsrelevanten Events geeignet ist. Außerdem stellt das Sicherheitsziel OE.ENV_PROTECT sicher, dass der Datenspeicher der Auditdaten vor unbefugten Zugriffen geschützt ist.

	O.NAC_DETECT	O.NAC_REACT	O.MAN_ROLES	O.MAN_FUNCS	O.MAN_MANAGE	O.MAN_COMM	O.AUD_GEN	O.AUD_REVIEW	OE.I&A_AUTH	OE.ENV_PROTECT	OE.ENV_RESOURCE	OE.ENV_NETWORK	OE.ENV_DEV	OE.EVG_INSTALL	OE.EVG_ADMIN	OE.EVG_USER	OE.AUD_MIRROR	OE.AUD_TIME
T.DEV_UNAUTH	✘	✘																

	O.NAC_DETECT	O.NAC_REACT	O.MAN_ROLES	O.MAN_FUNCS	O.MAN_MANAGE	O.MAN_COMM	O.AUD_GEN	O.AUD_REVIEW	OE.I&A_AUTH	OE.ENV_PROTECT	OE.ENV_RESOURCE	OE.ENV_NETWORK	OE.ENV_DEV	OE.EVG_INSTALL	OE.EVG_ADMIN	OE.EVG_USER	OE.AUD_MIRROR	OE.AUD_TIME
T.DEV_MASK	✘	✘										✘	✘					
T.DEV_MANIP	✘	✘											✘					
T.SYS_ACCESS			✘						✘	✘								
T.COM_PRIVACY						✘					✘	✘						
T.COM_INTEG						✘					✘	✘						
A.ENV_SERVER										✘	✘							
A.ENV_DATA										✘								
A.ENV_AVAIL											✘							
A.NET_SUPPORT												✘						
A.DEV_CONTROL												✘	✘			✘		
A.INI_SERVER														✘				
A.INI_AGENT														✘				
A.ADM_QUAL															✘			
A.ADM_NONEVIL															✘			
A.AUD_BACKUP																	✘	
P.SYS_MANAGE					✘													
P.SYS_FUNCS				✘														
P.AUD_DETECT							✘	✘		✘								✘

Tabelle 8: Abdeckung der Bedrohungen, Annahmen und Sicherheitsrichtlinien

5 Definition erweiterter Komponenten

5.1 Erweiterte funktionale Sicherheitskomponenten

Alle Komponenten in diesem Kapitel basieren auf dem Schutzprofil *U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments, PP Version 1.7*[7] vom 25. July 2007. Als Basis wurden Komponenten der Audit-Familie (FAU) aus dem Part 2 der CC verwendet. Zweck dieser Anforderungen ist es, dass Erfassen und Analysieren von Daten im Netzwerk und die Reaktion des NAC-Systems darauf zu beschreiben.

Angepasst wurde die Funktion IDS_SDC.1.2 für diese Sicherheitsvorgaben. Im Original wird im Punkt *b)* zu allen Events aus IDS_SDC.1.1 die Speicherung von Details gefordert. Durch die Selektion der Events in IDS_SDC.1.1 ist dies nicht sinnvoll, da einzelne Events ausgeschlossen werden können. Um dies zu beheben, wurde die Funktion dahingehend angepasst, dass nur zusätzliche Informationen zu den in IDS_SDC.1.1 gewählten Events gespeichert werden müssen.

5.1.1 Netzwerkzugriffskontrolle (NAC):

IDS_SDC.1 - System Data Collection:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):
  a) [selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities]; and
  b) [assignment: *other specifically defined events*].
- IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

[7] `http://www.commoncriteriaportal.org/files/ppfiles/pp_ids_sys_br_v1.7.pdf`

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information [assignment: *additional information*] for collected system events defined by IDS_SDC.1.1.

IDS_ANL.1 - Analyser analysis:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:
  a) [selection: statistical, signature, integrity]; and
  b) [assignment: *other analytical functions*].
- IDS_ANL.1.2 The System shall record within each analytical result at least the following information:
  a) Date and time of the result, type of result, identification of data source; and
  b) [assignment: *other security relevant information about the result*].

IDS_RCT.1 - Analyser react:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_RCT.1.1 The System shall send an alarm to [assignment: *alarm destination*] and take [assignment: *appropriate actions*] when an intrusion is detected.

IDS_RDR.1 - Restricted Data Review:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_RDR.1.1The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.
- IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.
- IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6 Sicherheitsanforderungen

In diesem Kapitel werden die funktionalen Anforderungen für den EVG und die Betriebsumgebung beschrieben. Die Anforderungen bestehen aus funktionellen Komponenten aus dem Part 2 der CC und speziellen Komponenten für NAC-Systeme, welche im Kapitel 5 dieser Sicherheitsvorgaben definiert wurden.

6.1 Definitionen

Im Folgenden werden Definitionen, welche in den SFRs verwendet werden, aufgeführt. Das englische Äquivalent wird zusätzlich, falls nötig, kursiv in Klammern mit angegeben.

6.1.1 Subjekte:

- Autorisierter Benutzer (*Authorised user*): Benutzer der mindestens einer der in Kapitel 3.1.1 definierten Rollen angehört. Ein autorisierter Benutzer wird mit den in den TSF-Daten (Kapitel 1.3.4) unter Benutzer-Accounts angegebenen Sicherheitsattributen assoziiert.

6.1.2 Objekte:

- Benutzer-Account (*User account*): Konto eines autorisierten Benutzers am Management-Server. Ein Benutzer-Account wird mit den in den TSF-Daten (Kapitel 1.3.4) angegebenen Sicherheitsattributen assoziiert. Zusätzlich wird der Status (Aktiv / Inaktiv) des Accounts vom Management-Server verwaltet. Ein *deaktivierter* Account kann temporär (bis zur *Reaktivierung*) nicht vom Benutzer zur Anmeldung am Management-Server verwendet werden.

- Management-Server (*Management server*): Der im EVG enthaltene Management-Server, wie definiert in Kapitel 1.3.

- Endgeräte (*End devices*): Endgeräte (siehe auch 6.1.4) werden vom EVG mit den in den TSF-Daten (Kapitel 1.3.4) angegebenen Sicherheitsattributen assoziiert.

- Netzwerkkomponenten (*Network devices*): Netzwerkgeräte (siehe auch 6.1.4) werden vom EVG mit den in den TSF-Daten (Kapitel 1.3.4) angegebenen Sicherheitsattributen assoziiert.

- Compliance-Agent (*Compliance-Agent*): Im EVG enthaltener Softwareagent, wie definiert in Kapitel 1.3. Sicherheitsattribute des Compliance-Agenten sind der Programmcode der Software selbst und die an den Management-Server übermittelten Daten.
- Administrative Verbindung (*Administrative session*): Verbindung eines autorisierten Benutzers mit der Benutzerschnittstelle des EVGs. Sicherheitsattribute der Verbindung sind die übermittelten Daten selbst.
- Auditdaten (*Audit information*): Die gesammelten und gespeicherten Daten, wie definiert in FAU_GEN.1, IDS_SDC.1 und IDS_ANL.1. Sicherheitsattribute der Auditdaten sind die enthaltenen Informationen selbst.
- Netzwerkpakete (*Network packet*): Paket mit Daten, welches während einer Netzwerkkommunikation übertragen wird. Sicherheitsattribute für ein Netzwerkpaket sind die enthaltenen Daten.

6.1.3 Operationen:

Der CC-Standard definiert bestimmte Operationen für funktionale Anforderungen. Diese werden durch die folgende Konvention bei der Formatierung gekennzeichnet:

- Zuweisung: *Kursiver Text*
- Auswahl: Unterstrichener Text
- Zuweisung innerhalb einer Auswahl: *Unterstrichener und kursiver Text*
- Verfeinerung: **Fetter Text**

Bei der Iteration wird eine Komponente mehrmals mit unterschiedlichen Operationen verwendet. Dies wird durch nachgestellte Nummern in Klammern gekennzeichnet (z.B. FAU_GEN.1(1)).

Jeder Text innerhalb der Komponenten, der nicht auf die beschriebene Weise formatiert ist, entspricht dem englischen Originaltext der jeweiligen Komponente aus Part 2 der *Common Criteria* oder erweiterter Komponenten aus dem Kapitel 5.

6.1.4 Externe Entitäten:

- Endgeräte (*End devices*): Mit dem verwalteten Netzwerk verbundene Endgeräte, wie PCs, Drucker oder Server.
- Netzwerkkomponenten (*Network devices*): Im verwalteten Netzwerk enthaltene Netzwerkgeräte, wie Switche oder Router, welche vom EVG zur Datenerfassung abgefragt werden.

6.2 Funktionale Sicherheitsanforderungen an den EVG

6.2.1 Audit (FAU):

FAU_GEN.1 - Audit data generation:

Hierarchical to: No other components
Dependencies: FPT_STM.1

- FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
  a) Start-up and shutdown of the audit functions;
  b) All auditable events for the not specified level of audit; and
  c) *the events specified in table 9*;
- FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
  a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
  b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional details specified in table 9.*

SFR	Event	Details
FAU_GEN.1	Start of EMD (Engine)	-
	Shutdown of EMD (Engine)	-
FMT_MOF.1	Modification of actions	old value, new value

SFR	Event	Details
FPT_TST.1	System failure	component, reason
FMT_MTD.1	Modification of system properties	property name, old value, new value
	Modification of end device properties	property name, old value, new value
	Modification of network device properties	property name, old value, new value
	Modification of user account properties	property name, old value, new value

Tabelle 9: Details for FAU_GEN.1

FAU_GEN.2 - User identity association:

Hierarchical to: No other components
Dependencies: FAU_GEN.1, FIA_UID.1

- FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 - Audit review:

Hierarchical to: No other components
Dependencies: FAU_GEN.1

- FAU_SAR.1.1 The TSF shall provide *authorised users specified in table 10* with the capability to read *audit information as specified in table 10* from the audit records.
- FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

User Role	Audit information
Administrator	All information
Operator	All information
Helpdesk	Information for end devices only
Revisor	All information

Tabelle 10: Details for FAU_SAR.1

FAU_SAR.2 - Restricted audit review:

Hierarchical to: No other components
Dependencies: FAU_SAR.1

- FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 - Selectable audit review:

Hierarchical to: No other components
Dependencies: FAU_SAR.1

- FAU_SAR.3.1The TSF shall provide the ability to apply *filtering and ordering* of audit data based on *all properties of the audit information.*

6.2.2 Security management (FMT):

FMT_MOF.1 - Management of security functions behaviour:

Hierarchical to: No other components
Dependencies: FMT_SMR.1, FMT_SMF.1

- FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions *specified in the table 11* to *authorised users which are associated with on of the roles as specified in table 11.*

Function	Determine	Dis- / Enable	Modify
Potential security violation definitions in actions	Administrator, Operator, Revisor	Administrator, Operator	Administrator, Operator

Tabelle 11: Details for FMT_MOF.1

FMT_MTD.1 - Management of TSF data:

Hierarchical to: No other components
Dependencies: FMT_SMR.1, FMT_SMF.1

- FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, the *items listed in table 12* to *authorised users which are associated with on of the roles as specified in table 12.*

TSF-Daten	Administrato	Operator	Helpdesk	Revisor
System properties	Full access	Full access	-	Query
Actions	Full access	Full access	-	Query
Network device properties	Full access	Full access	-	Query
End device properties	Full access	Full access	Full access	Query
User accounts	Full access	-	-	Query

Tabelle 12: Details for FMT_MTD.1

FMT_SMF.1 - Specification of Management Functions:

Hierarchical to: No other components
Dependencies: No dependencies

- FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:
  a) Management of user accounts;
  b) Management of actions;

c) Management of system parameters;

d) Management of end device properties and their authorisation status; and

e) Management of network components for data collection.

FMT_SMR.1 - Security roles:

Hierarchical to: No other components
Dependencies: FIA_UID.1

- FMT_SMR.1.1 Die The TSF shall maintain the roles *Administrator, Operator, Helpdesk and Revisor.*
- FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.3 Protection of the TSF (FPT):

FPT_ITC.1 - Inter-TSF confidentiality during transmission:

Hierarchical to: No other components
Dependencies: No dependencies

- FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

FPT_ITI.1 - Inter-TSF detection of modification:

Hierarchical to: No other components
Dependencies: No dependencies

- FPT_ITI.1.1The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: *incorrect Message Authentication Code (MAC)*

- FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform *rejection of network packet and request retransmission for those network packets with incorrect MACs* if modifications are detected.

FPT_ITT.1 - Basic internal TSF data transfer protection:

Hierarchical to: No other components
Dependencies: No dependencies

- FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and modification when it is transmitted between separate parts of the TOE.

FPT_TST.1 - TST testing

Hierarchical to: Not other components
Dependencies: No dependencies

- FPT_TST.1.1 The TSF shall run a suite of self tests periodically during normal operation to demonstrate the correct operation of *Engine, EMD and the Database*.
- FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of *the TSF data in the Database*.
- FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of *the TSF containted by the Engine and EMD*.

Note 1: The purpose of the SFR FPT_TST.1.2 is to assure that the connection to the database which holds the TSF data is properly functioning.

Note 2: The purpose of the SFR FPT_TST.1.3 is to assure that the critical subsystems of the ToE are properly functioning.

6.2.4 Network Access Control (NAC):

IDS_SDC.1 - System Data Collection:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_SDC.1.1 The System shall be able to collect the following information from **end devices**:
  a) Start-up and shutdown, security configuration changes; and
  b) *fingerprint_changed, wrong_tpm_signature, unauthorised, critical_system_failure.*
- IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:
  a) Date and time of the event, type of event, **end device MAC address**, and the outcome (success or failure) of the event; and
  b) The additional information *specified in the Details column of the table 13* for collected system events defined by IDS_SDC.1.1.

Component	Events	Details
IDS_SDC.1	Start-up and Shutdown	none
IDS_SDC.1	security configuration changes	defined security configuration property, differing property
IDS_SDC.1	fingerprint_changed	known fingerprint, requested differing fingerprint
IDS_SDC.1	wrong_tpm_signature	none
IDS_SDC.1	unauthorised	all available end device properties
IDS_SDC.1	critical_system_failure	system component, reason

Tabelle 13: Details for IDS_SDC.1

Note 3: The event *Start-up and shutdown* refers to the *macmon* events *mac_online* and *mac_offline*. The event *security configuration changes* refers to the *macmon* event *now_noncompliant*.

Note 4: The *macmon* event *now_ noncompliant* also covers the *wrong_ tpm_ signature* event. The reason which caused the event can be determined by the security configuration property.

Note 5: The event *fingerprint_ changed* is related to the end device property *fingerprint*. If this property changed the *fingerprint_ changed* event will arise.

Note 6: The event *unauthorised* is related to the end device property *status*. If an end device with status unauthorised or new is detected inside the network the *unauthorised* event will arise.

Note 7: The event *wrong_ tpm_ signature* is related to the TPM public key of the end device. If an end device transmits a value, chosen by the management server, signed by its TPM private key, which can't be decrypt with the saved public key, the *now_ noncompliant* event will arise.

Note 8: The event *critical_ system_ failure* is related to the periodical seft tests of the critical system components. This event will arise if one of critical componente of the ToE does not operate correctly.

IDS_ANL.1 - Analyser analysis:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:
  a) signature; and
  b) *reference list*
- IDS_ANL.1.2 The System shall record within each analytical result at least the following information:
  a) Date and time of the result, type of result, identification of data source; and
  b) *end device properties*.

Note 9: The analysis function *reference list* compare the signature with a reference list of authorised end devices.

IDS_RCT.1 - Analyser react:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_RCT.1.1 The System shall send an alarm to *the alert destination configured for the matching rule* and take *the action configured for the matching rule* when an **event defined by IDS_SDC.1 arises**.

IDS_RDR.1 - Restricted Data Review:

Hierarchical to: No other components
Dependencies: No dependencies

- IDS_RDR.1.1The System shall provide *all authorised users* with the capability to read *all information as defined in IDS_SDC.1* from the System data.
- IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.
- IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

6.3 Anforderungen an die Vertrauenswürdigkeit des EVGs

Der EVG erfüllt die Anforderungen an die Vertrauenswürdigkeit für EAL2+. Die einzelnen Anforderungen sind in Tabelle 14 zusammengefasst.

Klasse	Komponenten-ID	Komponenten-Titel
Sicherheitsvorgaben	ASE_INT.1	ST-Einleitung
	ASE_CCL.1	Antrag auf Konformität
	ASE_SPD.1	Definition der Sicherheitsumgebung
	ASE_OBJ.2	Sicherheitsziele
	ASE_ECD.1	Definition erweiterter Komponenten
	ASE_REQ.2	Sicherheitsanforderungen
	ASE_TSS.1	Zusammenfassung der EVG-Spezifikation
Entwicklung	ADV_ARC.1	Beschreibung der Sicherheitsarchitektur
	ADV_FSP.2	Funktionale Spezifikation (SFR-enforcing)
	ADV_TDS.1	Basis Design-Beschreibung
Handbücher	AGD_OPE.1	Operationales Handbuch
	AGD_PRE.1	Installationshandbuch
Lebenszyklus-unterstützung	ALC_CMC.2	Benutzung eines CM-Systems
	ALC_CMS.2	EVG-Abdeckung im CM-System
	ALC_DEL.1	Lieferverfahren
	ALC_FLR.1	Basis Fehlerbehebung
Tests	ATE_COV.1	Beweis der Abdeckung
	ATE_FUN.1	Funktionales Testen
	ATE_IND.2	Unabhängiges Testen
Schwachstellen Bewertung	AVA_VAN.2	Schwachstellen Analyse

Tabelle 14: Anforderungen der EAL2

Die Anforderungen an die Vertrauenswürdigkeit gemäß der gewählten Vertrauenswürdigkeitsstufe EAL2+ sind angemessen für den EVG, weil somit eine Basissicherheitsleistung zu gewährleisten erreicht wird.

Die EAL2+ soll dem Anwender einen grundlegenden Qualitätsstandard und ei-

ne Basis für die Sicherheit der angebotenen Funktionalitäten bieten. Hierbei ist vor allem zu beachten, dass ein NAC-System im Allgemeinen bestehende Sicherheitslösungen erweitert.Die Schutzleistung des EVGs beschränkt sich hierbei auf den generellen Schutz der im Netzwerk verfügbaren Ressourcen vor fremden oder manipulierten Geräten. Zum Schutz des logischen Zugriffs auf sensible Daten und Ressourcen im Netzwerk werden andere Schutzmaßnahmen benötigt.

Zusätzlich ist eine Basissicherheitsleistung durch EAL2 in der Praxis gebräuchlich für NAC-System.

EAL2 bedeutet nach CC: strukturell getestet. EAL2 schafft Vertrauenswürdigkeit dadurch, dass die Sicherheitsfunktionen unter Verwendung einer funktionalen Spezifikation und einer Schnittstellenspezifikation sowie von Handbüchern und des Entwurfs des EVGs auf hoher Ebene analysiert werden, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängiges Testen der EVG-Sicherheitsfunktionen, durch den Nachweis der Entwicklertests auf Grundlage der funktionalen Spezifikation, durch selektive, unabhängige Bestätigung der Entwicklertestergebnisse und durch einen Nachweis der Suche des Entwicklers nach offensichtlichen Schwachstellen.

EAL2 schafft Vertrauenswürdigkeit auch mittels eines Konfigurationsverzeichnisses für den EVG und durch einen Nachweis der Sicherheit der Auslieferungsprozeduren.

Die Erweiterung durch ALC_FLR.1 wurde gewählt, um die Entdeckung und Beseitigung von offensichtlichen Sicherheitsfehler des EVGs sicherzustellen und überprüfbar zu machen.

6.4 Hierarchie und Abhängigkeiten der Komponenten

Dieses Kapitel demonstriert die Einhaltung der Abhängigkeiten zwischen den funktionalen Sicherheitsanforderungen dieser Sicherheitsvorgaben. Die Tabelle 15 zeigt eine Übersicht der SFRs, deren Abhängigkeiten und wie diese zufrieden gestellt werden.

SFR	Hierarchie	Abhängigkeit	Begründung
FAU_GEN.1	-	FPT_STM.1	erfüllt durch das Bereitstellen eines Zeitstempels durch die Betriebsumgebung
FAU_GEN.2	-	FAU_GEN.1 FIA_UID.1	erfüllt erfüllt durch die Authentifizierung des Benutzers durch die Betriebsumgebung.
FAU_SAR.1	-	FAU_GEN.1	erfüllt
FAU_SAR.2	-	FAU_SAR.1	erfüllt
FAU_SAR.3	-	FAU_SAR.1	erfüllt
FMT_MOF.1	-	FMT_SMR.1 FMT_SMF.1	erfüllt erfüllt
FMT_MTD.1	-	FMT_SMR.1 FMT_SMF.1	erfüllt erfüllt
FMT_SMF.1	-	-	-
FMT_SMR.1	-	FIA_UID.1	erfüllt durch die Authentifizierung des Benutzers durch die Betriebsumgebung.
FPT_ITC.1	-	-	-
FPT_ITI.1	-	-	-
FPT_ITT.1	-	-	-
FPT_TST.1	-	-	-
IDS_SDC.1	-	-	-
IDS_ANL.1	-	-	-
IDS_RCT.1	-	-	-
IDS_RDR.1	-	-	-

Tabelle 15: Einhaltung aller Abhängigkeiten bei SFRs

6.5 Argumentation zu den SFRs

Die Tabelle 16 auf Seite 55 zeigt eine Übersicht zur Abdeckung der Sicherheitsziele durch die funktionalen Sicherheitsanforderungen. Inwieweit die Sicherheitsanforderungen diese abdecken wird im Folgenden beschrieben.

Das Sicherheitsziel **O.NAC_DETECT** verlangt die Erkennung von nicht-autorisierten Geräten im Netzwerk. IDS_SDC.1 sorgt für die Erfassung von Netzwerkdaten wodurch alle Geräte im Netzwerk erkannt werden. IDS_ANL.1 sorgt dafür, dass die Signatur[8] bei allen erkannten Geräten in der Referenzliste enthalten und unverändert ist.

Das Sicherheitsziel **O.NAC_REACT** verlangt, dass sicherheitsrelevante Ereignisse im Netzwerk erfasst werden und darauf Reagiert wird. IDS_ANL.1 stellt sicher, dass erfasste Daten im Netzwerk auf unbefugte Zugriffe durch nicht-autorisierte, maskierte oder nicht-konforme Endgeräte hin analysiert werden. IDS_RCT.1 stellt sicher, dass auf Ergebnisse der Analyse hin der Zugriff für die betreffenden Endgeräte auf das Netzwerk unterbunden wird.

Das Sicherheitsziel **O.MAN_ROLES** verlangt die Unterstützung von verschieden Rollen für Benutzer. Durch FMT_SMR.1 wird sicher gestellt, dass die Rollen Administrator, Operator, Helpdesk und Revisor vom EVG angeboten werden. FMT_MTD.1 definiert hierzu, welche Rollen welche Berechtigungen auf die TSF-Daten besitzen.

Das Sicherheitsziel **O.MAN_MANAGE** verlangt, dass Funktionen zum Management des EVGs einem autorisierten Benutzer zur Verfügung stehen. FMT_SMF.1 stellt sicher, dass Sicherheitsfunktionen für bestimmte Benutzer zur Verfügung stehen. FMT_MOF.1 unterstützt dies dadurch, dass das Verhalten von Sicherheitsfunktionen verwaltet werden kann. FMT_MTD.1 unterstützt dies, durch die Definition von Daten und die Einschränkung des Zugriffs darauf.

Das Sicherheitsziel **O.MAN_COMM** verlangt den Schutz von Verbindungen zwischen unterschiedlichen Bestandteilen des EVGs und zwischen dem EVG und verwalteten Netzwerkkomponenten. FPT_ITT.1 stellt den Schutz der Integrität und der Vertraulichkeit von Übertragungen zwischen den EVG-Bestandteilen sicher. FPT_ITC.1 und FPT_ITI.1 stellen den Schutz der Integrität und der Vertraulichkeit von Übertragungen zwischen dem EVG und anderen Netzwerkkomponenten sicher.

Das Sicherheitsziel **O.AUD_GEN** verlangt das Auditdaten erzeugt werden.

[8] MAC-Adresse (bzw. Fingerprint, abhängig vom Typ des Gerätes)

FAU_GEN.1 und FAU_GEN.2 fordern das Erzeugen von Auditdaten und legen den Informationsumfang der Auditeinträge fest. Zusätzlich wird durch IDS_SDC.1 und IDS_ANL.1 die Erzeugung und der Umfang für Events im Netzwerk gefordert.

Das Sicherheitsziel **O.AUD_REVIEW** verlangt die Möglichkeit des Auditreviews. FAU_SAR.1 sorgt für den Zugriff auf eine lesbare Darstellung der Auditdaten für festgelegte Benutzer. FAU_SAR.2 unterstützt dies dadurch, dass kein anderer Benutzer auf die Auditdaten zugreifen kann. FAU_SAR.3 unterstützt dies, durch die Möglichkeit des Sortierens und Filterns der Auditeinträge. IDS_RDR.1 sorgt zusätzlich für den Zugang zu einer lesbaren Darstellung der Netzwerkdaten.

Das Sicherheitsziel **O.MAN_FUNCS** verlangt die Prüfung sicherheitskritischer Bestandteile des EVGs durch den EVG selbst. FPT_TST.1 sorgt dafür, dass der EVG periodisch die korrekte Funktionsweise der Engine und des EMDs sowie der korrekten Funktionsweise der Verbindung zur Datenbank und den darin enthaltenen TSF-Daten. Außerdem unterstützt FAU_GEN.1 dies dadurch, dass der Ausfall der Engine, des EMDs oder der Datenbankverbindung für den Anwender ersichtlich wird. In Verbindung mit IDS_RCT.1 ist es ebenfalls möglich, eine automatische Reaktion (Alarm-Email) zum Ausfall eines der genannten EVG-Bestandteile auszulösen.

	O.NAC_DETECT	O.NAC_REACT	O.MAN_ROLES	O.MAN_MANAGE	O.MAN_COMM	O.AUD_GEN	O.AUD_REVIEW	O.MAN_FUNCS
FAU_GEN.1						✘		✘
FAU_GEN.2						✘		
FAU_SAR.1							✘	
FAU_SAR.2							✘	
FAU_SAR.3							✘	
FMT_MOF.1				✘				

	O.NAC_DETECT	O.NAC_REACT	O.MAN_ROLES	O.MAN_MANAGE	O.MAN_COMM	O.AUD_GEN	O.AUD_REVIEW	O.MAN_FUNCS
FMT_MTD.1			✘	✘				
FMT_SMF.1				✘				
FMT_SMR.1			✘					
FPT_ITC.1					✘			
FPT_ITI.1					✘			
FPT_ITT.1					✘			
FPT_TST.1								✘
IDS_SDC.1	✘					✘		
IDS_ANL.1	✘	✘				✘		
IDS_RCT.1		✘						✘
IDS_RDR.1							✘	

Tabelle 16: Abdeckung der Sicherheitsziele durch SFRs

7 Zusammenfassung der EVG-Spezifikation

In diesem Kapitel wird demonstriert, dass die Sicherheitsfunktionen des EVGs komplett und sorgfältig von den verwendeten funktionalen Sicherheitsanforderungen abgedeckt werden.

7.1 Sicherheitsfunktionen des EVGs

7.1.1 Mapping SFRs zu den Sicherheitsfunktionen:

Die Tabelle 17 auf der Seite 56 liefert ein Mapping zwischen den Sicherheitsfunktionen des EVGs und den verwendeten SFRs. Das Mapping wird in der nachfolgenden Argumentation zu den Sicherheitsfunktionen beschrieben.

	Audit	Management	NAC
FAU_GEN.1	✘		
FAU_GEN.2	✘		
FAU_SAR.1	✘		
FAU_SAR.2	✘		
FAU_SAR.3	✘		
FMT_MOF.1		✘	
FMT_MTD.1		✘	
FMT_SMF.1		✘	
FMT_SMR.1		✘	
FPT_ITC.1		✘	✘
FPT_ITI.1		✘	✘
FPT_ITT.1			✘
FPT_TST.1		✘	
IDS_SDC.1	✘		✘
IDS_ANL.1	✘		✘
IDS_RCT.1			✘
IDS_RDR.1	✘		✘

Tabelle 17: Abdeckung der Sicherheitsfunktionen des EVGs durch SFRs

7.1.2 Audit:

Der EVG bietet unterschiedliche Möglichkeiten, um autorisierten Benutzern Informationen zum Management-Server, dem verwalteten Netzwerk und Endgeräten im Netzwerk anzubieten.

Die Report-Funktionen liefern alle Informationen zur Überwachung des Netzwerkes und für Entscheidungen, welche die Sicherheit des Netzwerkes betreffen. Im Menu Berichte können Berichte zu unterschiedlichen Themen abgerufen werden. Jeder Bericht kann anhand der enthaltenen Informationen sortiert und durchsucht bzw. gefiltert werden.

Zusätzlich zu den Reports bietet der EVG das Abfragen von Diagrammen mit statistischen Informationen zu erfassten Netzwerkdaten an. Eine Auswahl der wichtigsten Diagramme, kann der Benutzer in die Startseite der Benutzeroberfläche integrieren.

Alle Report-Funktionen sind in die web-basierte Benutzeroberfläche des Management-Servers integriert. Der EVG bietet die folgenden Features für das Auditing:

- Anpassbare Startseite mit den zwei wichtigsten Diagrammen
- Erweiterung von Netzwerkdaten durch das Hinzufügen von zwei benutzerspezifischen Spalten
- Berichte mit Zusammenfassungen zu Geräten im Netzwerk
- Konfigurierbare Mitteilungen für auftretende Events
- Export der Daten in eine CSV-Datei

Die Berichte sind für alle autorisierten Benutzer des EVGs verfügbar. Der Zugriff des Helpdesk ist allerdings auf Berichte zu Endgeräten beschränkt.

Alle Berichte und Auditdaten sind in der Datenbank des EVGs gespeichert. Wenn die Kapazität der Datenbank erschöpft ist, werden neue Informationen ignoriert und eine Fehlermeldung an den Benutzer ausgegeben.

Für die Sicherheitsfunktion **Audit** wurden folgende SFRs eingebunden:

- FAU_GEN.1: Der EVG generiert Auditdaten zu allen angegebenen Events.

- FAU_GEN.2: Soweit möglich, wird der Auditeintrag vom EVG mit einem Benutzer, der das Event ausgelöst hat, assoziiert.
- FAU_SAR.1: Der EVG bietet dem Administrator, dem Operator, dem Helpdesk und dem Revisor die Möglichkeit auf die Auditdaten zuzugreifen.
- FAU_SAR.2: Der EVG sorgt dafür, dass sonst kein Benutzer über den administrativen Zugang des Management-Servers auf die Auditdaten zugreifen kann.
- FAU_SAR.3: Autorisierte Benutzer können über den EVG die Auditdaten anhand aller erfassten Informationen in den Auditeinträgen durchsuchen und sortieren.
- IDS_SDC.1: Der EVG sammelt alle Daten im Netzwerk, die zur Erkennung der definierten Events benötigt werden, und speichert diese sowie erkannte Events in der Datenbank.
- IDS_ANL.1: Der EVG analysiert die durch IDS_SDC.1 generierten Daten anhand der definierten Analysefunktion und speichert die Ergebnisse in der Datenbank.
- IDS_RDR.1: Der EVG sorgt dafür, dass nur autorisierte Benutzer über den administrativen Zugang des Management-Servers auf die Netzwerk- und Eventdaten zugreifen können.

7.1.3 Identifikation und Authentifizierung:

Die I&A wird beim Zugriff auf die Benutzeroberfläche des Management-Servers verlangt. Zur Durchführung des Identifizierungs- und Authentifizierungsprozesses wird der Authentifizierungsmechanismus des Web-Servers verwendet. Der Web-Server ist Bestandteil der Betriebsumgebung. Somit wird der Authentifizierungsmechanismus **nicht** vom EVG implementiert. Vom Web-Server wird die Eingabe des Benutzernamens und des Passwortes verlangt. Hierbei werden die Zeichen des Passwortes durch Sternchen dargestellt. Außerdem gibt es Einschränkungen für Sonderzeichen, die im Passwort verwendet werden dürfen und eine Mindestlänge von acht Zeichen wird verlangt. Werden die Einschränkungen nicht eingehalten, wird das Passwort nicht gespeichert und eine Fehlermeldung wird ausgegeben.

Die Eingabe wird vom Web-Server verifiziert, bevor der Zugriff zur Benutzeroberfläche gestattet wird. Schlägt die Verifizierung fehl, wird der Benutzer erneut zur Eingabe aufgefordert. Ist die Verifizierung erfolgreich, werden die Sicherheitsattribute des Benutzers mit dieser Verbindung assoziiert und die Rollen-spezifischen Inhalte werden angeboten. Der EVG unterstützt multiple, simultane Verbindungen zum Management-Server und assoziiert die Sicherheitsattribute individuell zu den Verbindungen.

Ändern sich die Sicherheitsattribute eines Benutzers zur Laufzeit, werden die Berechtigungen sofort angepasst und der Benutzer verliert möglicherweise den Zugriff auf Bereiche, die er zuvor noch aufrufen konnte. Ebenfalls ist es möglich einen Benutzer zur Laufzeit zu deaktivieren, so dass dieser zur nächsten Benutzeraktion keinen Zugriff mehr auf den EVG bekommt.

7.1.4 Management:

Der EVG bietet Möglichkeiten zum Management, um den EVG kontrollieren und überwachen zu können. Dabei haben die Benutzer unterschiedliche Berechtigungen auf die Funktionen und Daten zum Management des EVGs. Die Berechtigungen werden mit der Rolle des jeweiligen Benutzers assoziiert.

Der Zugang zu Managementfunktionen wird über eine geschützte Verbindung ermöglicht. Die Benutzeroberfläche kann nur über eine HTTPS-Verbindung (TLSv1.0) aufgerufen werden. Der Server kann dabei vom Benutzer durch das SSL-Zertifikat authentifiziert werden.

Zur Verwaltung der Rollen und Benutzer wird dem Administrator eine Benutzerverwaltung angeboten. In der Benutzerverwaltung werden die Passwörter von existierenden Accounts nicht angezeigt. Eine Änderung des Passwortes ist nur für den eigenen Account möglich. Ausgenommen sind hierbei Benutzer der Rolle Administrator, welche alle Passwörter verändern können.

Zum Schutz eines unbemerkten Ausfalls der Sicherheitsleistung des EVGs, führt der EVG periodisch Selbsttests durch. Hierbei kontrollieren die verschiedenen Subsysteme des EVGs sich gegenseitig. Bemerkt ein Subsystem den Ausfall eines anderen, wird dies als Log-Eintrag festgehalten und ein Ereignis ausgelöst. Auf das Ereignis kann mithilfe des Regelwerks automatisch reagiert werden, um bspw. den

Administrator mit einer E-Mail zu warnen. Außerdem werden Ausfälle der einzelnen Subsysteme auch auf der Startseite der GUI dargestellt. Diese Schutzfunktion ist nur funktionsfähig, solange nicht **alle** EVG-Komponenten ausfallen.

Für die Sicherheitsfunktion **Management** wurden die folgenden SFRs eingebunden:

- FMT_MOF.1: Die Privilegien für Managementfunktionen sind für jede Rolle klar definiert und werden vom EVG durchgesetzt.
- FMT_MTD.1: Die Zugriffsberechtigungen für TSF-Daten sind für jede Rolle klar definiert und werden vom EVG durchgesetzt.
- FMT_SMF.1: Alle definierten Managementfunktionen werden vom EVG über die Benutzeroberfläche zur Verfügung gestellt.
- FMT_SMR.1: Alle benötigten Rollen sind klar definiert und werden vom EVG angeboten und verwaltet.
- FPT_ITC.1: Der EVG sorgt dafür, dass die Vertraulichkeit der Daten einer Verbindung zur Benutzeroberfläche des Management-Servers geschützt ist.
- FPT_ITI.1: Der EVG sorgt dafür, dass die Integrität der Daten einer Verbindung zur Benutzeroberfläche des Management-Servers anhand der definierten Metriken überprüft wird und damit wie spezifiziert verfahren wird.
- FPT_TST.1: Der EVG sorgt dafür, dass Ausfälle einzelner sicherheitskritischer EVG-Bestandteile für den Anwender ersichtlich sind. Hierzu prüft der EVG periodisch die korrekte Funktionsweise der jeweiligen Komponente.

7.1.5 Netzwerkzugriffskontrolle:

Der EVG überwacht durch periodische Abfragen von Daten das verwaltete Netzwerk. Dadurch kann jedes Endgerät, welches sich im verwalteten Netzwerk befindet erkannt werden.

Zur Erkennung werden primär die Port-Informationen von den Switchen abgerufen. Anhand der Informationen lassen sich der Standort (bzw. der physikalische Port) und die MAC-Adresse des Endgerätes bestimmen. Manuell oder anhand

von Regeln können die Endgeräte in eine Referenzliste für autorisierte Geräte eingetragen werden. Dies ermöglicht den Schutz vor neuen und nicht-autorisierten Endgeräten im Netzwerk.

Zusätzlich zu den primären Informationen werden interne Informationen (Sicherheitskonfiguration und Fingerprint) zum Endgerät vom Agenten abgefragt. Welche Daten dabei vom Agenten erfasst werden, wird vom Administrator definiert. Dazu kann der Administrator selbst erstellte Skripte in einem festgelegten Format auf dem Server speichern, welche dann an den Agenten übertragen werden. Zusätzlich kann der Administrator aus diesen Daten Merkmale für einen Fingerprint bestimmen, welcher für jedes Endgerät eindeutig sein sollte. Diese zusätzlichen Daten und der Fingerprint werden für autorisierte Endgeräte ebenfalls erfasst und gespeichert. Durch Analyse dieser Daten zur Laufzeit, kann ein verdächtiges Verhalten von Endgeräten erkannt werden. Bspw. können durch die Erfassung der IP-Adresse mit der MAC-Adresse potenzielle ARP-Spoofing-Angriffe erkannt werden. Ein weiteres Beispiel ist ein Endgerät, dessen Virenscanner nicht mehr aktuell ist. Dieses Endgerät wird ebenfalls erkannt und entsprechend den Regeln behandelt. Durch den Fingerprint ist es außerdem möglich, die Endgeräte Identifikation per MAC-Adresse zu erweitern.

Welche Informationen für die Auslösung einer Reaktion notwendig sind, wird vom Administrator oder Operator anhand von Regeln definiert. Ebenfalls kann individuell für die Scan-Methode und das Gerät, das Intervall für die Erfassung der Daten festgelegt werden. Je geringer dieses Intervall, desto schneller werden Events erkannt, aber desto mehr Datenvolumen wird durch den Management-Server erzeugt.

Als Reaktion bietet der EVG das Senden eines Alarms per E-Mail an. Dazu kommen restriktive Maßnahmen zum Aussperren eines Endgerätes aus dem Netzwerk. Dies wird durch Deaktivierung des physikalischen Anschlusses oder Umschaltung des VLANs erreicht. Beim Umschalten des VLANs ist es allerdings auch möglich, ein Endgerät nicht auszuschließen, sondern in ein Netzwerk mit geringerer Priorität zu verschieben. Zusätzlich zu den hier genannten Reaktionen, kann der Benutzer eigene Befehle angeben, welche an das Betriebssystem weiter geleitet werden.

Alle im NAC-Bereich erkannten Events und ausgelösten Aktionen als Reaktion

werden ebenfalls erfasst. Diese Daten werden zusammen mit den Auditdaten in der Datenbank gespeichert. Für diese Daten gelten die gleichen Berechtigungen und Regeln wie für die anderen Auditdaten.

Für die Sicherheitsfunktion **Netzwerkzugriffskontrolle** wurden die folgenden SFRs eingebunden:

- IDS_SDC.1: Der EVG erfasst für alle Endgeräte im verwalteten Netzwerk die MAC-Adresse und interne Informationen vom Compliance-Agenten. Alle erfassten Daten und Details zu den spezifizierten Events werden vom EVG in der Datenbank gespeichert.
- IDS_ANL.1: Der EVG sorgt dafür, dass durch die Analysefunktionen alle Abweichungen einer Signatur (Gesamtheit der erfassten Daten) zu einem Endgerät, mit allen benötigten Informationen in den Auditdaten abgespeichert werden.
- IDS_RCT.1: Der EVG stellt sicher, dass auf erkannte Events angemessen reagiert wird.
- IDS_RDR.1: Alle Daten des verwalteten Netzwerks und der enthaltenen Geräten werden vom EVG für den Administrator, Operator, Helpdesk und Revisor zur Verfügung gestellt. Sonstige Benutzer erhalten vom EVG keinen Zugriff auf diese Daten.
- FPT_ITC.1: Der EVG sorgt dafür, dass die Vertraulichkeit einer Datenabfrage bei der Verbindung zwischen dem Management-Server und Geräten im verwalteten Netzwerk durch SNMPv3 geschützt ist.
- FPT_ITI.1: Der EVG sorgt dafür, dass die Integrität einer Datenabfrage bei der Verbindung zwischen dem Management-Server und Geräten im verwalteten Netzwerk durch SNMPv3 geschützt ist.
- FPT_ITT.1: Bei der Verbindung zwischen dem Management-Server und Compliance-Agent wird für einen Schutz vor Offenlegung und Modifikation der TSF-Daten mit Hilfe einer TLS-Verschlüsselung (TLSv1.0) gesorgt.

Abkürzungsverzeichnis

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CC	Common Criteria
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAL	Evaluation Assurance Level
EVG	Evaluierungsgegenstand (Deutsche Übersetzung zu TOE)
IDS	Intrusion Detection System
IP	Internet Protocol
JRE	Java Runtime Edition
MAC	Media Access Control
NAC	Network Access Control
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
ST	Security Target
TLS	Transport Layer Security
TLSv1.0	TLS Protokoll Version 1.0
TOE	Target of Evaluation
TPM	Trusted Platform Modul
TSF	TOE Security Functions
VLAN	Virtual Local Area Network
VM	Virtuelle Maschine