Security Target (ST)

macmon NAC

Inhaltsverzeichnis

1 ST-Einleitung (ASE_INT) 8
1.1 ST-Referenz 8
1.2 TOE-Referenz 8
1.3 TOE-Überblick 8
1.3.1 Übersicht zur Funktionalität 9
1.3.2 Benötigte Nicht-TOE Hardware/Software/Firmware 10
1.4 TOE-Beschreibung 12
1.4.1 Physischer Umfang des TOEs 14
1.4.2 Logischer Umfang des TOE 15
1.4.3 Konfiguration des TOEs 16
1.4.4 TSF-Daten 16
2 Antrag auf Konformität (ASE_CCL) 18
3 Definition der Sicherheitsumgebung (ASE_SPD) 19
3.1 Grundlagen 19
3.1.1 Rollen im TOE 19
3.1.2 Definition zu schützender Werte 19
3.1.3 Definition der Angreifer/Rollen 20
3.2 Bedrohungen 21
3.3 Annahmen 22
3.4 Organisatorische Sicherheitsrichtlinien 23
4 Sicherheitsziele (ASE_OBJ) 24
4.1 Sicherheitsziele für den TOE 24
4.2 Sicherheitsziele für die Betriebsumgebung 25
4.3 Argumentation zu den Sicherheitszielen 26
5 Definition erweiterter Komponenten (ASE_ECD) 29
5.1 Erweiterte funktionale Sicherheitskomponenten 29
5.1.1 Netzwerkzugriffskontrolle (NAC) 29
6 Sicherheitsanforderungen (ASE_REQ) 31
6.1 Definitionen 31
6.1.1 Subjekte 31

6.1.2 Objekte ... 31
6.1.3 Operationen ... 32
6.1.4 Externe Entitäten ... 32
6.2 Funktionale Sicherheitsanforderungen an den TOE ... 32
6.2.1 Security Audit (FAU) ... 32
6.2.2 Identification and authentication (FIA) ... 34
6.2.3 Security management (FMT) ... 35
6.2.4 Protection of the TSF (FPT) ... 37
6.2.5 Intrusion Detection System (IDS) ... 37
6.3 Anforderungen an die Vertrauenswürdigkeit des TOEs ... 40
6.4 Argumentation zu den SFRs ... 41
7 Zusammenfassung der TOE-Spezifikation (ASE_TSF) ... 44
7.1 Sicherheitsfunktionen des TOEs ... 44
7.1.1 Mapping SFRs zu den Sicherheitsfunktionen ... 44
7.1.2 SF Audit ... 44
7.1.3 SF Identifikation und Authentifizierung (I&A) ... 45
7.1.4 SF Management ... 46
7.1.5 SF Netzwerkzugriffskontrolle (NAC) ... 46

Abbildungsverzeichnis

Abbildung 1: Integration von macmon NAC in das Netzwerk 9
Abbildung 2: Subsysteme und Komponenten des TOE 12

Tabellenverzeichnis

Tabelle 1: Lieferbestandteile des TOE 15
Tabelle 2: Beschreibung der TSF-Daten 17
Tabelle 3: Bedrohungen 22
Tabelle 4: Annahmen 23
Tabelle 5: Organisatorische Sicherheitsrichtlinien 23
Tabelle 6: Sicherheitsziele für den TOE 24
Tabelle 7: Sicherheitsziele für die Betriebsumgebung 25
Tabelle 8: Abdeckung der Bedrohungen, Annahmen und Sicherheitsrichtlinien 28
Tabelle 9: Details for FAU_GEN.1 33
Tabelle 10: Details for FAU_SAR.1 34
Tabelle 11: Details for FMT_MOF.1 35
Tabelle 12: Details for FMT_MTD.1 36
Tabelle 13: Details for IDS_SDC.1 38
Tabelle 14: Anforderungen der EAL2+ 40
Tabelle 15: Abdeckung der Sicherheitsziele durch SFRs 43
Tabelle 16: Abdeckung der Sicherheitsziele des TOEs durch SFRs 44

Abkürzungsverzeichnis

802.1X ..... IEEE 802.1X Standard zur Authentifizierung

ARP ..... Address Resolution Protocol

CC ..... Common Criteria

CM ..... Configuration Management

DBMS ..... Datenbank-Management-System

EAL ..... Evaluation Assurance Level

EAP ..... Extensible Authentication Protocol

GUI ..... Graphical User Interface

IDS ..... Intrusion Detection System

LAN ..... Local Area Network

MAC ..... Media Access Control

NAC ..... Network Access Control

SFR ..... Security Functional Requirement

SNMP ..... Simple Network Management Protocol

TLS ..... Transport Layer Security

TOE ..... Target of Evaluation

TSF ..... TOE Security Functionality

VLAN ..... Virtual Local Area Network

Versionshistorie

Version	Datum	Beschreibung
3.8	12.03.2025	Formulierung der Objectives angepasst.
3.7	06.11.2024	Subsysteme Beschreibung überarbeitet.
3.6	24.05.2024	Alternativen zu VMWare entfernt und Referenzen aktualisiert.
3.5	07.09.2023	Update auf neue TOE-Version.
3.4	10.08.2023	Versionen von Nicht-TOE-Software aktualisiert.
3.3	07.03.2023	Finale Version.
3.2	10.11.2022	Fehlendes Mapping zu OE.AUD_TIME hinzugefügt.
3.1	05.10.2021	Annahmen leicht erweitert und fehlerhafte Referenzen korrigiert.
3.0	16.08.2021	Kleiner Inkonsistenzen, Rechtschreibfehler etc. behoben.
2.9	09.08.2021	Vereinfachung der SPD und OBJ. Verlagerung der kryptografischen Funktionen in die Betriebsumgebung. Überarbeitung der TSF-Beschreibung
2.8	02.07.2021	Platzhalter bei TOE-Version ersetzt und FCS_RNG.1 Klassen angepasst.
2.7	30.06.2021	Argumentation zu SFR FPT_STM.1 entfernt
2.6	28.06.2021	Fehlendes Mapping zu FCS_RNG und fehlende Argumentation zu SFR FPT_STM.1 aufgenommen
2.5	25.06.2021	Neue SFR für Zufallszahlengenerator FCS_RNG.1 aufgenommen
2.4	01.06.2021	Überarbeitung der zu schützenden Wert und Bedrohungen
2.3	21.05.2021	Überarbeitung der Sicherheitsziele und der SFRs
2.2	29.04.2021	Überarbeitung der TOE-Beschreibung und der enthaltenen Abbildung
2.1	16.12.2020	Überarbeitete Version
2.0	28.10.2015	Finale Version zur ersten Zertifizierung

Referenzierte Dokumente

Dokument	Beschreibung
[1] macmon-Appliance Inbetriebnahme	macmon-Appliance Inbetriebnahme, Ausgabe 2023/06
[2] macmon-Appliance Manual	macmon-Appliance Handbuch, Ausgabe 2023/05
[3] macmon Handbuch	macmon Handbuch, Ausgabe 5.36, 2023-07-31
[4] macmon CC-Handbücher	macmon CC-Handbücher (AGD), 2.10
[5] IDS Protection Profile	U.S. Government Protection Profile for Intrusion Detection System System

1 ST-Einleitung (ASE_INT)

Diese Sicherheitsvorgaben beschreiben die Ziele und Anforderungen für die Sicherheits-Software macmon NAC.

1.1 ST-Referenz

Titel:	Security Target (ST) macmon NAC
Version	3.8
Datum	12.03.2025

1.2 TOE-Referenz

TOE-Titel:	macmon NAC
TOE-Version	5.36.2
TOE-Datum	04.09.2023
TOE-Typ	Network Access Control (NAC)

1.3 TOE-Überblick

Das Produkt macmon NAC ist ein System zur Kontrolle des Zugriffs von Endgeräten auf ein Netzwerk. Der Einsatz von macmon NAC ermöglicht die Verwaltung und Überwachung des Netzwerks und der enthaltenen Netzwerkgeräte und Endgeräte. Damit gehört das TOE zu den Network Access Control (NAC)-Systemen. Der Server, auf dem macmon NAC installiert ist, wird im Folgenden synonym als macmon-Server bezeichnet. Der macmon-Server 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 werden der Schutz des Netzwerkes und dessen Ressourcen vor unbekannten oder nicht-autorisierten Endgeräten gewährleistet.

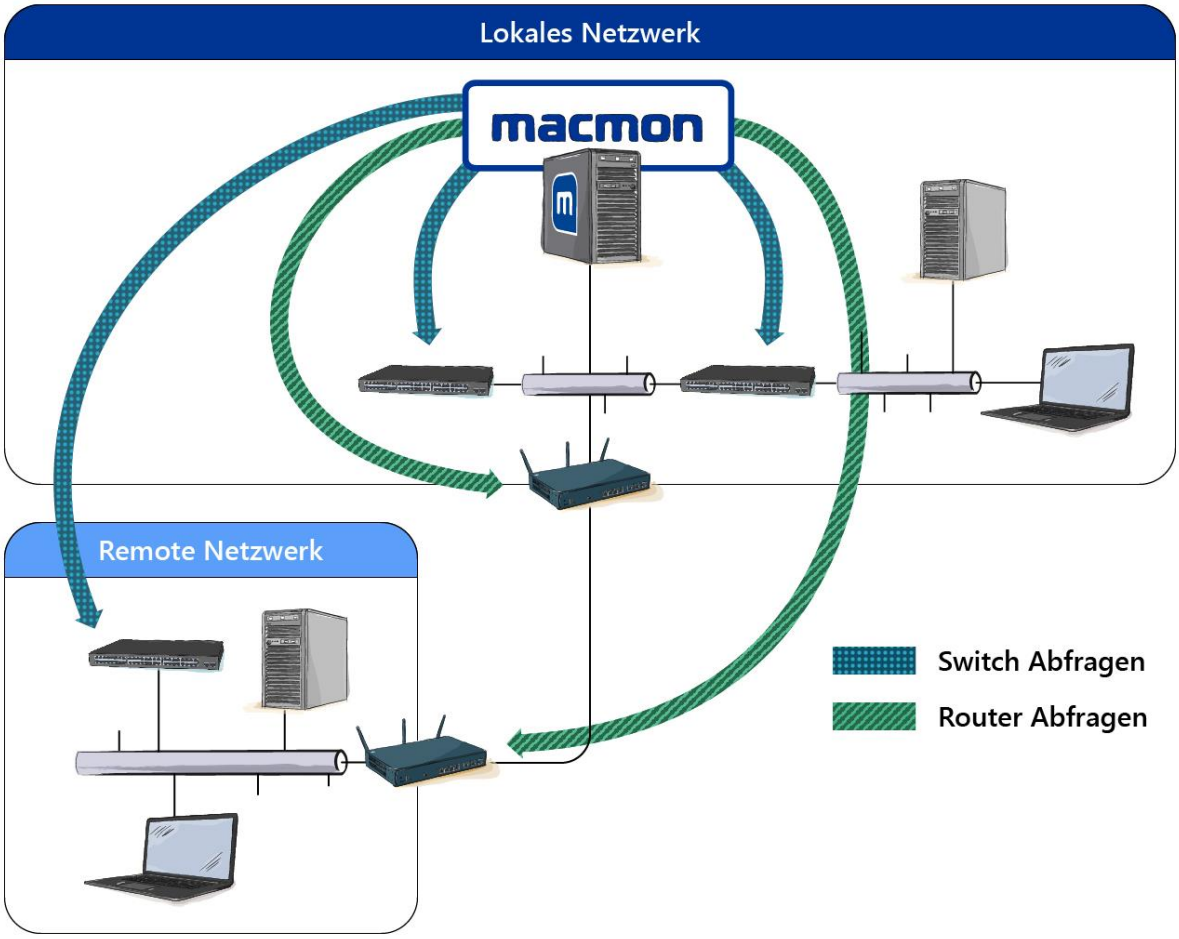

Abbildung 1: Integration von macmon NAC in das Netzwerk

1.3.1 Übersicht zur Funktionalität

Die NAC-Lösung macmon NAC 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 und der 802.1X-Zugangsdaten.
- Manuelle oder automatische/regelbasierte Kontrolle des Zugriffs auf das Netzwerk
- Überwachung des Netzwerkes und der autorisierten Endgeräte zur Laufzeit
- Erzeugung von Berichten zu Ereignissen im Netzwerk

Die genannten Funktionalitäten werden mithilfe der folgenden Verfahren ermöglicht:

- **Erkennung**: Zur Erkennung von Endgeräten werden die Statusinformationen von Switches und Informationen aus ARP-Zwischenspeichern von Routern verwendet.
- **Authentifizierung**: Um die Identität eines Endgerätes zu prüfen, werden die MAC-Adresse und die 802.1X-Zugangsdaten aus RADIUS-Anfragen der Switches verwendet. Als Zugangsdaten können Benutzername und Passwort, oder ein Zertifikat verwendet werden.

- **Autorisierung**: Zur Autorisierung des Zugriffs auf das Netzwerk verwendet macmon NAC das Umschalten von virtuelle LANs eines physischen Anschlusses oder die Aktivierung/Deaktivierung des physischen Anschlusses. Die Autorisierung wird automatisch anhand von Standard-Regeln oder benutzerspezifischen Regeln vorgenommen und per RADIUS an den Netzwerkverteiler gemeldet.
- **Kontrolle**: Das Netzwerk wird durch erneute Abfragen der Statusinformationen periodisch kontrolliert. Bei Erkennung von potenziell sicherheitsrelevanten Ereignissen wird anhand des Regelwerks reagiert.
- **Monitoring**: Der aktuelle Status des Netzwerks kann über die Benutzeroberfläche analysiert werden. Statusinformationen der erkannten Geräte und Berichte können hier abgerufen werden.

1.3.2 Benötigte Nicht-TOE Hardware/Software/Firmware

Das TOE umfasst die Sicherheits-Software macmon NAC. Zum Betrieb des TOEs wird folgende Nicht-TOE Software/Firmware vorausgesetzt:

- **macmon-Appliance**: Als Plattform für den macmon-Server wird die virtuelle macmon-Appliance in der gleichen Version wie der TOE (siehe Kapitel 1.1) vorausgesetzt. Die macmon-Appliance stellt mit installiertem macmon NAC einen einsatzbereiten Management-Server eines NAC-Systems dar. Die Virtualisierungsumgebung muss folgenden Mindestanforderungen genügen:
  - Virtualisierungssoftware:
    - VMware vSphere ab Version 7
    - VMware ESXi ab Version 7.0
  - Anforderung an die virtuelle Maschine:
    - 8 GB Arbeitsspeicher
    - 1 CPU mit 4 Kernen
    - 250 GB Festplatte
    - 1 GBit/s Netzwerkanschlüsse
  - Installierte Software:
    - Betriebssystem Debian Linux Kernel 4.19
    - Datenbank MariaDB 1:10.3.39-0+deb10u1 (DBMS: Datenbank-Management-System)
    - Webserver Apache 2.4.38-3+deb10u8
    - PHP 7.3.31-1~deb10u3
    - OpenJDK 11.0.18+10-1~deb10u1
    - OpenSSL 1.1.1n-0+deb10u4
    - FreeRADIUS 3.0.17+dfsg-1.1+deb10u2
    - Mailserver Postfix 3.4.23-0+deb10u1

- **Web-Browser**: Der Zugriff auf den macmon-Server geschieht über eine HTTPS-Verbindung zu der macmon-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 mindestens Version 1.2) und Java Script (mindestens Version ES6[1]) unterstützen. macmon NAC unterstützt folgende Browser ab der jeweils genannten Version:
  - Microsoft Edge (90.0.818.62)
  - Mozilla Firefox (88.0.1)
  - Google Chrome (90.0.4430.212)

- **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 oder 802.1X unterstützt werden. Die Switches müssen diesbezüglich die folgenden Standards implementieren:
  - MIB-II[2] (Interfaces abfragen)
  - BRIDGE-MIB[3] (MAC-Adressen abfragen)
  - Q-BRIDGE-MIB[4] (VLANs abfragen)
  - RADIUS[5] mit folgenden Standards:
    - IEEE 802.1X[6] Port-Based NAC
    - RADIUS Remote Authentication[7]
    - RADIUS VLANs[8]

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

- **Endgeräte**: Für die Erkennung werden alle Endgeräte unterstützt, die 802.1X unterstützen und über eine MAC-Adresse verfügen.

---

[1] Java Script ES6 (ECMAScript 2015) - https://262.ecma-international.org/6.0/

[2] MIB-II (RFC 1213) - http://www.ietf.org/rfc/rfc1213

[3] BRIDGE-MIB (RFC 1493) - http://www.ietf.org/rfc/rfc1493

[4] Q-BRIDGE-MIB (RFC 4363) - http://www.ietf.org/rfc/rfc4363

[5] RADIUS (RFC 2865) - https://tools.ietf.org/html/rfc2865

[6] IEEE 802.1X - https://1.ieee802.org/security/802-1x

[7] RADIUS Remote Authentication (RFC 3579) - https://tools.ietf.org/html/rfc3579

[8] RADIUS for VLAN Support (RFC 4675) - https://tools.ietf.org/html/rfc4675

- **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.

1.4 TOE-Beschreibung

Das TOE bietet die Überwachung und Verwaltung des Netzwerkes an. Überwacht werden kann dabei jedes im Netzwerk befindliche Endgerät, welches an einen Netzwerkverteiler angeschlossen ist. Das TOE besteht aus dem macmon-Server, welcher technisch in zwei Bereiche, Engine und Webserver, unterteilt werden kann (siehe Abbildung 2).

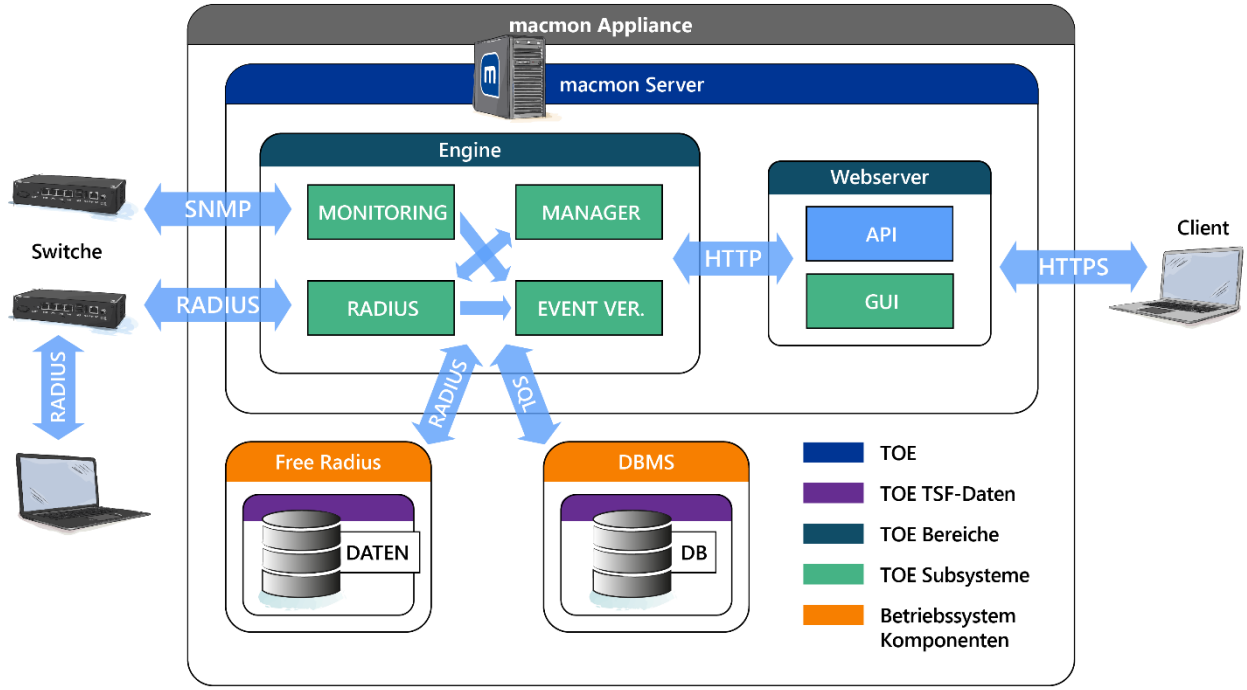

Abbildung 2: Subsysteme und Komponenten des TOE

Der macmon-Server implementiert die NAC-Funktionalitäten des TOEs. Der Server stellt den zentralen Management-Server des NAC-Systems dar und bietet alle Managementfunktionen an. Der macmon-Server wird im Weiteren synonym als Management-Server bezeichnet. Die folgenden Subsysteme (SFR-enforcing) sind im TOE enthalten:

- Engine: Im Bereich der Engine liegen die Subsysteme zur Erfassung und Analyse von Daten, sowie der Reaktion auf sicherheitsrelevante Ereignisse. Die Engine besteht grob aus vier Subsystemen:
  - Netzwerk-Monitoring: Diese Komponente führt die Erfassung von Netzwerkdaten durch. Alle empfangenen Daten werden verarbeitet und analysiert und in der

Datenbank gespeichert. Bei der Analyse erkannte sicherheitsrelevante Ereignisse werden anhand der Standard-Regeln überprüft und gegebenenfalls darauf reagiert. Verschiedene Ereignisse im Netzwerk werden zudem im System für andere Komponenten publiziert.

  - Event-Verarbeitung: Die während der Analyse publizierten Ereignisse werden parallel von dieser Komponente verarbeitet. Dabei werden die Inhalte der Ereignisse anhand eines Regelwerks überprüft. Das Regelwerk besteht aus benutzerspezifischen Regeln, welche vom Administrator verwaltet werden. Jede Regel bezieht sich auf ein bestimmtes Ereignis und kann durch Bedingungen eingegrenzt werden. In den Bedingungen können alle ereignisbezogenen Daten und Informationen verwendet werden. Trifft die Bedingung einer Regel zu, werden die Aktionen dieser Regeln ausgeführt. Erkannte Ereignisse werden zusätzlich mit allen ereignisbezogenen Informationen in der Datenbank hinterlegt.
  - RADIUS-Handler: Bei dieser Komponente handelt es sich um einen Empfänger für RADIUS-Anfragen. Alle RADIUS-Anfragen von autorisierten Netzwerkverteilern werden entgegengenommen und anhand der Standard-Regeln analysiert. Das Ergebnis wird als Antwort an den Netzwerkverteiler gesendet und bestimmt ob und inwieweit der Zugriff eines Endgeräts vom Netzwerkverteiler gewährt wird.
  - Manager: Diese Komponente bietet den Zugriff auf TSF-Daten und die Authentifizierung und Autorisierung von Benutzern als Service an. Der Manager steht ausschließlich für interne Anfragen zu Verfügung und wird von der UI zur Verwaltung von TSF-Daten und zur Verifizierung von Anmeldungen mit Benutzername und Passwort genutzt. Außerdem wird dieser Service vom RADIUS-Handler verwendet, um die Autorisierung für eine gültige RADIUS-Anfrage anhand des Regelwerks zu berechnen.

- Webserver: Der Bereich Webserver beinhaltet die Subsysteme zur Verwaltung des TOE per HTTPS:
  - GUI: Die Bedienung des macmon-Servers geschieht primär über eine web-basierte Benutzeroberfläche, 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.
  - API: Zusätzlich kann ein Großteil der Konfigurationen per REST-API über HTTPS durchgeführt werden. Die API ist kein eigenes Subsystem, sondern ein Proxy für das Subsystem Manager um diesen abgesichert durch HTTPS von extern erreichbar zu machen. Der Zugriff auf diese Schnittstelle des Managers ist von extern ausschließlich auf Benutzer der Rolle Administrator (siehe auch Kapitel 3.1.1) beschränkt.

Zwei weitere Subsysteme (SFR-supporting) des TOEs sind eine Datenbank, welche als Speichermedium eingesetzt wird und der FreeRADIUS-Server der Betriebsumgebung, welcher zur Prüfung von RADIUS Anfragen genutzt wird. Die Datenbank wird vom DBMS (siehe MariaDB Datenbank in Kapitel 1.3.2) der Betriebsumgebung verwaltet. Das DBMS regelt die Zugriffe auf die TSF-Daten in der Datenbank. Das

DBMS und der FreeRADIUS-Server sind ausschließlich für **lokale** Zugriffe konfiguriert und werden exklusiv vom macmon-Server genutzt.

- 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 Ereignisse 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.

- FreeRADIUS-Server: Hierbei handelt es sich um den FreeRADIUS-Server[9] der Betriebsumgebung. Dieser wird von der Komponente Engine zur Prüfung von EAP[10] RADIUS-Anfragen herangezogen. Der FreeRADIUS-Server wird hierfür bei der Installation des macmon-Servers konfiguriert und ist ebenfalls ausschließlich lokal erreichbar. Zu den Daten des FreeRADIUS gehören auch die Zertifikate der Endgeräte.

1.4.1 Physischer Umfang des TOEs

Der physische Umfang legt die im TOE enthaltenen Bestandteile fest. Dabei handelt es sich ausschließlich um den macmon-Server mit der Datenbank und dem FreeRADIUS-Server. Der macmon-Server ist auf der in Kapitel 1.3.2 definierten macmon-Appliance vorinstalliert. Zusätzlich dazu umfasst das TOE die folgenden Dokumente:

1. macmon-Appliance Inbetriebnahme (siehe [1] macmon-Appliance Inbetriebnahme): Handbuch mit Hinweisen zur Inbetriebnahme der macmon-Appliance in der Virtualisierungsumgebung.
2. macmon-Appliance Handbuch (siehe [2] macmon-Appliance Manual): Handbuch mit Beschreibungen zur Konfigurationsoberfläche der macmon-Appliance.
3. macmon Handbuch (siehe [3] macmon Handbuch): Handbuch zur Erläuterung der Funktionen und Verwaltung des macmon-Servers.
4. macmon Common Criteria Handbücher (siehe [4] macmon CC-Handbücher): Common Criteria AGD Dokument mit zusätzlichen Beschreibungen zur Installation, Konfiguration und Inbetriebnahme von macmon NAC im Common Criteria-konformen Zustand.

[9] FreeRADIUS-Server - https://freeradius.org

[10] EAP (RFC-3748) - https://tools.ietf.org/html/rfc3748

Die folgenden Bestandteile werden für das TOE als Download vom Service Portal[11] geliefert:

ID	Name	Format
1	macmon Server auf macmon-Appliance	OVF
2	macmon-Appliance Inbetriebnahme	PDF
3	macmon-Appliance Handbuch	PDF
4	macmon Handbuch	PDF
5	macmon Common Criteria Handbücher	PDF

Tabelle 1: Lieferbestandteile des TOE

1.4.2 Logischer Umfang des TOE

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

Audit: Das TOE generiert Auditdaten für sicherheitsrelevante Ereignisse. Die Ereignisse beziehen sich zum einen auf gesammelte Daten und Ereignisse 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 oder die REST-API werden dessen Zugangsdaten vom TOE verifiziert. Das TOE 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 Identifizierung und Autorisierung verweigert.

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

Netzwerkmonitioring und Zugriffskontrolle (NAC): Das TOE kontrolliert den Zugriff von Endgeräten auf das verwaltete Netzwerk. Dabei wird der Zugriff für Endgeräte manuell oder anhand von Richtlinien entschieden. Diese Richtlinien beinhalten Standard-Regeln und benutzerspezifischen Regeln, welche am Management-Server konfiguriert und verwaltet werden können. Das TOE überwacht dazu das verwaltete Netzwerk und erfasst sicherheitsrelevante Daten. Durch Analyse der Daten werden neue Endgeräte und nicht-autorisierte Geräte identifiziert. Bei Erkennung von sicherheitsrelevanten Ereignissen werden Maßnahmen gemäß den Regeln durchgeführt. Als Maßnahmen bietet das TOE das Auslösen eines Alarms und die Ablehnung bzw. den Widerruf einer Autorisierung des Zugriffs auf das Netzwerk an.

[11] Service Portal: Webseite mit Downloadbereich für Kunden https://portal.macmon.eu

1.4.3 Konfiguration des TOEs

Dieses Kapitel legt fest, wie das TOE 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 TOEs muss die Einsatzumgebung mindestens folgende Komponenten aufweisen:

1. Eine Instanz der macmon-Appliance
2. Managebare Switches mit VLAN- und RADIUS-Unterstützung
3. Router mit Unterstützung der Abfrage von ARP-Daten

Das TOE wird mit der folgenden Konfiguration eingesetzt:

1. Installation und Konfiguration der macmon-Appliance anhand des macmon Common Criteria Handbuchs
2. Konfiguration aller Netzwerkverteiler anhand des macmon Common Criteria Handbuchs
3. Konfigurierter Router anhand des macmon Common Criteria Handbuchs

1.4.4 TSF-Daten

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

TSF-Daten	Beschreibung
Systemparameter	Einstellungen zur Konfiguration des TOEs, hierzu gehören die folgenden Bereiche: • Engine-Einstellungen • Datenbank-Einstellungen • FreeRADIUS-Einstellungen • GUI-Einstellungen
Aktionen	Regelwerk zur Behandlung von Ereignissen im Netzwerk und Reaktionen auf diese. Jede Regel hat folgende Attribute: • Eindeutiger Name • Ereignis • Bedingungen • Reaktionen

TSF-Daten	Beschreibung
Benutzer-Accounts	Konten für autorisierte Benutzer des Management-Servers. Jeder Account ist mit den folgenden Attributen assoziiert: • Status (Aktiv/Inaktiv) • Benutzer-ID • Benutzer-Name • Passwort • Rolle • *Optional: Beschreibung* • *Optional: E-Mail-Adresse*
Netzwerkkomponenten	Eigenschaften und Abfrageeinstellungen zu den verwalteten Netzwerkkomponenten. Hierzu gehören: • IP-Adresse • Geräteklasse (Scan-Methoden) • Gerätegruppe (Scan-Aktionen) • Scan-Einstellungen (Intervalle, Wartezeiten etc.) • Zugangsdaten
Endgeräteparameter	Attribute eines Endgerätes, welche beim Scannen des Netzwerkes erfasst werden. Hierzu gehören: • MAC-Adresse • Interface (Switch-ID und Interface-ID) • Endgerätegruppe • IP-Adresse • VLAN-ID • RADIUS-Zugangsdaten • Status (Autorisiert, Nicht-Autorisiert, Neu)

Tabelle 2: Beschreibung der TSF-Daten

2 Antrag auf Konformität (ASE_CCL)

Das Security Target (ST) und der Evaluierungsgegenstand (TOE) stellen Anspruch auf Konformität zu:

- Common Criteria for Information Technology Security Evaluation – Part 1 (CC Part 1): Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation – Part 2 (CC Part 2): Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation – Part 3 (CC Part 3): Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

Der Antrag auf Konformität besteht aus den folgenden Konformitäts-Erklärungen:

- Das ST ist **konform zu CC Part 2 erweitert** durch die zusätzlichen Komponenten (siehe Kapitel 5 und [5] IDS Protection Profile)
  - IDS_SDC.1 “System Data Collection”
  - IDS_ANL.1 “Analyser analysis”
  - IDS_RTC.1 “Analyser react”
  - IDS_RDR.1 “Restricted Data Reviewer”
- Das ST ist **konform zu CC Part 3**.

Das ST ist **konform zu EAL 2 erweitert** durch die zusätzliche Komponente ALC_FLR.1 “Basic flaw remediation” (siehe Kapitel 6.2).

Diese Sicherheitsvorgaben stellen keinen Anspruch auf Konformität zu einem Schutzprofil.

3 Definition der Sicherheitsumgebung (ASE_SPD)

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

3.1 Grundlagen

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

3.1.1 Rollen im TOE

Die nachfolgenden definierten Rollen werden vom TOE standardmäßig vorgegeben:

- **Administrator**: Benutzer mit vollem Zugriff auf den TOE. Der Administrator ist der einzige Benutzer mit vollem Zugriff auf die Konfiguration des TOEs, einschließlich der Benutzerverwaltung und der REST-API.
- **Operator**: Benutzer mit vollem Zugriff auf die Konfiguration des TOEs. Der Operator hat alle Rechte des Administrators ausgenommen dem Zugriff auf die Benutzerverwaltung.
- **Helpdesk**: Benutzer mit beschränktem Zugriff auf die Konfiguration des TOEs. Der Zugriff beschränkt sich auf die Verwaltung von Endgeräten und Endgerätegruppen. 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 TOE. Der Revisor hat ausschließlich Lese-Berechtigung für alle Bereiche des TOEs.
- **Nicht-autorisierter Benutzer**: Benutzer, der keiner der genannten Rollen angehört. Dieser Benutzer verfügt über keine Berechtigungen und erhält keinerlei Zugriff auf Funktionen des TOEs.

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

Bei den Rollen Administrator, Operator, Helpdesk und Revisor handelt es sich um „autorisierte Benutzer".

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.

- AS.NETZWERK: Hierbei handelt es sich um alle lokalen/remote Netzwerk (siehe auch Abbildung 1), welche vom TOE verwaltet werden, bzw. um die Ressourcen und Kommunikation im Netzwerk. Das verwaltete Netzwerk umfasst alle Netzwerksegmente, welche vom TOE durch die Erfassung von

Daten kontrolliert werden. Schützenswert ist konkret der Zugriff bzw. die Ermittlung folgender Bestandteile des Netzwerks durch unbefugte Personen:

- ungesicherte (offene) Netzwerkressourcen,
- Informationen über die Netzwerktopologie und
- Netzwerkkommunikation (E-Mail, Passwörter, u. ä.)

- AS.MGMT_SERVER: Hierbei handelt es sich um den Management-Server und dessen Ressourcen. Als schützenswert sind die folgenden vier Bereiche anzusehen:
  - Administrativer Zugang: Dieser Zugang bezieht sich auf die Benutzerschnittstellen zu administrativen Funktionen des Management-Servers.
  - Physischer Zugang: Dieser bezieht sich auf den direkten physikalischen Zugang zur Hardware der Virtualisierungsumgebung des Management-Servers oder der Betriebsumgebung.
  - Ressourcen: Hierbei handelt es sich um die Ressourcen des Management-Servers, wie Programmdateien oder den Datenspeicher (z. B. Datenbank, Dateisystem, etc.), welcher bspw. alle Audit-Daten enthält.
  - Kommunikation: Hierbei 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 im verwalteten Netzwerk.

- AS.ENDGERÄT: Hierbei handelt es sich um alle Endgeräte, welche vom Administrator für den Zugriff auf das verwaltete Netzwerk autorisiert sind. Als schützenswert gelten hier der administrative Zugang zu den RADIUS-Zugangsdaten und die RADIUS-Kommunikation zum Netzwerkverteiler.

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 Potential 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 kann Folgendes sein:

- 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 Informationen über die Netzwerktopologie.

3.2 Bedrohungen

Bedrohung	Beschreibung	Bedrohter Wert
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.	AS.NETZWERK
T.DEV_MASK	Maskierte Geräte: Ein Angreifer könnte ein nicht autorisiertes Gerät mit der Identität eines autorisierten Gerätes maskieren (Manipulation der MAC-Adresse). 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.	AS.NETZWERK
T.DEV_ACCESS	Unberechtigter Zugriff zum Geräte: Die Zugangsdaten eines bereits autorisiertes Gerät könnten einem Angreifer den unbefugten Zugriff auf das Netzwerk mit einem nicht autorisierten Gerät ermöglichen.	AS.ENDGERÄT AS.NETZWERK
T.SYS_ACCESS	Unberechtigter Zugriff zum System: Ein Angreifer könnte über den administrativen Zugang des Management-Servers unbefugt Zugriff auf dessen Managementfunktionen und Daten erlangen. Dies ermöglicht dem Angreifer den Management-Server zu kontrollieren und damit Sicherheitsfunktionen des TOEs zu umgehen oder zu deaktivieren.	AS.MGMT_SERVER
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/Endgerät ausspähen. Die	AS.MGMT_SERVER AS.ENDGERÄT

Bedrohung	Beschreibung	Bedrohter Wert
	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/Endgerät manipulieren. Dadurch kann der Angreifer Sicherheitsfunktionen des TOEs deaktivieren.	AS.MGMT_SERVER AS.ENDGERÄT

Tabelle 3: Bedrohungen

3.3 Annahmen

Annahmen	Beschreibung
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_CLIENT	Absicherung autorisierter Geräte: Ein autorisiertes Endgerät und dessen Zugangsdaten, sowie der Web-Browser für den Zugriff auf den TOE, müssen vor administrativen Zugriffen durch unbefugte Personen oder der Installation von Schadsoftware geschützt werden.
A.ENV_OS	Betriebssystem und Virtualisierungsumgebung: Das Betriebssystem stellt die vom TOE benötigten Zeitstempel, Zugriff auf das Dateisystem und kryptografische Funktionen zur Verfügung. Des Weiteren wird sichergestellt, dass die TSF-, Konfigurations- und Auditdaten des TOEs vor direkten Zugriffen über die Betriebsumgebung durch unbefugte Personen geschützt sind. Alle vom TOE benötigten Ressourcen werden von der Virtualisierungsumgebung zur Verfügung gestellt.
A.NET_SUPPORT	Hardware- und Protokoll-Unterstützung: Das Netzwerk muss die in Kapitel 1.3.2 genannten Protokolle für Netzwerkverteiler unterstützen und alle geforderten Komponenten enthalten, welche ordnungsgemäß funktionieren müssen.

Annahmen	Beschreibung
A.ADM_NONEVIL	Qualifizierter und nicht korrupter Verantwortliche: Der verantwortliche Administrator (Rolle Administrator oder Operator wie in Kapitel 3.1.1 definiert) muss ausreichend qualifiziert und geschult sein, um das System zu bedienen und folgt bei der Installation und dem Betrieb des TOE den beiliegenden Anleitungen (siehe Kapitel 1.4.1). Außerdem hat der verantwortliche Administrator keine böswilligen Absichten.

Tabelle 4: Annahmen

3.4 Organisatorische Sicherheitsrichtlinien

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

Sicherheitsrichtlinien	Beschreibung
P.SYS_MANAGE	Verwendung von Managementfunktionen: Der Anwender soll den TOE so konfigurieren, dass alle autorisierten Endgeräte Zugriff auf das Netzwerk erhalten und alle zu überwachten Netzwerkkomponenten abgefragt werden.
P.SYS_FUNCS	Ausfall von Sicherheitsfunktionen: Der Anwender muss den Ausfall einer TOE-Komponente erkennen können, wenn dies die Sicherheitsleistung des TOE beeinträchtigt.
P.AUD_DETECT	Verfügbarkeit von Auditreview-Funktionen: Der Anwender muss Änderungen an sicherheitskritischen Einstellungen des TOEs erkennen können. Anderenfalls könnten Fehlkonfigurationen einen Angriff ermöglichen, bereits stattgefundene Angriffe nicht entdeckt oder gleichartige Angriffe nicht verhindert werden.

Tabelle 5: Organisatorische Sicherheitsrichtlinien

4 Sicherheitsziele (ASE_OBJ)

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

4.1 Sicherheitsziele für den TOE

Sicherheitsziele	Beschreibung
O.NAC_DETECT	Erkennung von Ereignissen: Das TOE soll alle relevanten Daten im Netzwerk erfassen und sicherheitskritische Ereignisse erkennen.
O.NAC_REACT	Reaktion auf Ereignisse: Das TOE soll auf erkannte sicherheitskritische Ereignisse im Netzwerk mit angemessenen Maßnahmen reagieren.
O.I&A	Authentifizierung von Benutzern: Das TOE soll einen Benutzer identifizieren und authentisieren, so dass ausschließlich die autorisierten Benutzer Zugriff zur administrativen Schnittstelle des TOEs erhalten.
O.MAN_FUNCS	Erkennung von Ausfällen kritischer TOE-Komponenten: Das TOE soll selbst erkennen, wenn einzelne sicherheitskritische Komponenten des TOEs ausfallen und dies für autorisierte Benutzer ersichtlich machen.
O.MAN_ROLES	Benutzerrollen: Das TOE soll die Rollen Administrator, Operator, Helpdesk und Revisor anbieten. Ein authentifizierter Benutzer erhält, abhängig von seiner Rolle, Zugriff auf die Funktionen und Daten des TOEs.
O.MAN_MANAGE	Managementfunktionen des TOEs: Das TOE soll einem autorisierten Benutzer zur Verwaltung und Konfiguration benötigte Funktionen zur Verfügung stellen.
O.AUD_GEN	Generierung von Auditdaten: Das TOE soll zu allen erkannten Ereignissen im Netzwerk und bei Änderungen der Konfiguration des TOEs Einträge in den Auditdaten erzeugen.
O.AUD_REVIEW	Anzeige von Auditdaten: Das TOE soll die Möglichkeit bieten, Auditdaten in einer für den Benutzer lesbaren Form anzuzeigen.

Tabelle 6: Sicherheitsziele für den TOE

4.2 Sicherheitsziele für die Betriebsumgebung

Sicherheitsziel	Beschreibung
OE.ENV_PROTECT	Schutz des Management-Servers: Die vom Management-Server benötigte Virtualisierungsplattform muss vor physikalischen und logischen Zugriffen durch unberechtigte Personen geschützt sein und der Zugriff darf nur vom internen Netzwerk möglich sein.
OE.ENV_RESOURCE	Verfügbarkeit von Ressourcen: Die Virtualisierungsumgebung (macmon-Appliance, siehe Kapitel 1.3.2) und die darauf installierte Software müssen dem TOE zur Verfügung stehen, um dessen Funktionsfähigkeit zu gewährleisten.
OE.ENV_NETWORK	Unterstütztes Netzwerk: Das TOE muss in das bestehende Netzwerk integrierbar sein und benötigte Protokolle müssen von den Netzwerkkomponenten unterstützt werden.
OE.ENV_DEV	Schutz der autorisierten Endgeräte: Vom Administrator autorisierte Endgeräte mit RADIUS-Zugangsdaten und der Installierte Web-Browser für den Zugriff auf den TOE, müssen vor administrativen Zugriffen durch unberechtigte Personen gesichert sein.
OE.TOE_INSTALL	Installation des TOEs: Das TOE muss ordnungsgemäß geliefert, installiert und konfiguriert werden. Der Verantwortliche muss dabei nach der Installationsanleitung des Herstellers handeln.
OE.TOE_ADMIN	Administrator des TOEs: Der Administrator (Rolle Administrator oder Operator wie in Kapitel 3.1.1 definiert) des TOEs muss qualifiziert und geschult sein, den TOE zu bedienen. Der Administrator darf keine böswilligen Absichten haben.
OE.TOE_USER	Alle Benutzer: Alle Benutzer des TOEs und die autorisierten Endgeräte müssen sicherstellen, dass ihre Zugangsdaten nicht für Dritte zugänglich sind.
OE.AUD_TIME	Zeitstempel für Auditdaten: Die Betriebsumgebung muss Zeitstempel für die korrekte Erzeugung von Auditeinträgen liefern.

Tabelle 7: Sicherheitsziele für die Betriebsumgebung

4.3 Argumentation zu den Sicherheitszielen

Die Tabelle 8 auf Seite 28 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 Endgeräte 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 sichergestellt, dass auf solche sicherheitsrelevanten Ereignisse reagiert wird.

Die Bedrohung **T.DEV_MASK** bezieht sich auf maskierte, nicht-autorisierte Endgeräte im Netzwerk. O.NAC_DETECT stellt sicher, dass alle Daten im Netzwerk erfasst werden, um maskierte Geräte zu erkennen. Durch O.NAC_REACT wird sichergestellt, dass auf solche sicherheitsrelevanten Ereignisse regiert wird. Zusätzlich stellen OE.ENV_DEV sicher, dass alle autorisierten Geräte geschützt werden.

Die Bedrohung **T.DEV_ACCESS** bezieht sich auf den unberechtigten Zugriff auf die Zugangsdaten eines autorisierten Endgerätes im Netzwerk. OE.ENV_DEV stellt sicher, dass die 802.1X-Zugangsdaten auf autorisierten Geräten vor unbefugten Zugriffen geschützt ist.

Die Bedrohung **T.SYS_ACCESS** bezieht sich auf unberechtigte Zugriffe auf den TOE. O.I&A und O.MAN_ROLES stellen sicher, dass nur autorisierte Benutzer mit den spezifischen Rechten ihrer Rolle auf die administrative Schnittstelle des TOEs zugreifen können. OE.ENV_PROTECT stellt sicher, dass nur autorisierte Benutzer einen physikalischen Zugriff zum TOE erhalten. OE.TOE_USER stellt zusätzlich sicher, dass die Zugangsdaten dieser Benutzer nicht von Dritten in Erfahrung gebracht werden können. Außerdem stellt OE.ENV_RESOURCE 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/Endgeräten ausgetauscht werden. OE.ENV_RESSOURCE stellt sicher, dass die Betriebsumgebung alle benötigten kryptografischen Funktionen und 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/Endgeräten ausgetauscht werden. OE.ENV_RESSOURCE stellt sicher, dass die Betriebsumgebung alle benötigten Ressourcen und kryptografischen Funktionen 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 Management-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 TOEs benötigt werden, von der Betriebsumgebung zur Verfügung gestellt werden.

Die Annahme **A.ENV_CLIENT** bezieht sich auf den Schutz des administrativen Zugangs auf autorisierte Endgeräte vor Zugriffen durch unbefugte Personen. Die Ziele OE.ENV_DEV und OE.TOE_USER stellen sicher, dass alle autorisierten Geräte und deren Anwendungen geschützt sind und die Zugangsdaten eines autorisierten Benutzers nicht von Dritten in Erfahrung gebracht werden können.

Die Annahme **A.ENV_OS** bezieht sich auf benötigte Funktionen des Betriebssystems und der Verfügbarkeit sowie dem Schutz der Ressourcen des TOE. Das Sicherheitsziel OE.ENV_PROTECT stellt sicher, dass die Ressourcen, welche Programmdateien, Konfigurationsdateien oder Auditdaten beinhalten, vor unbefugten Zugriffen geschützt sind. OE.ENV_RESSOURCE stellt sicher, dass alle zur Funktionsfähigkeit des TOEs benötigten Ressourcen dem TOE zur Verfügung stehen. Hierzu gehören auch die durch OE.AUD_TIME geforderten Zeitstempel für die Generierung von Auditeinträgen.

Die Annahme **A.NET_SUPPORT** bezieht sich auf die Unterstützung des TOEs 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.ADM_NONEVIL** bezieht sich auf die Qualifikation und Loyalität des verantwortlichen Administrators/Operators. OE.TOE_ADMIN stellt sicher, dass dieser ausreichend geschult und qualifiziert ist, um den TOE ordnungsgemäß zu installieren, zu konfigurieren und zu betreiben und keine böswilligen Absichten hat. OE.TOE_INSTALL stellt sicher, dass der Management-Server ordnungsgemäß anhand der Installationsanleitung des Herstellers installiert wird.

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

Die Sicherheitsrichtlinie **P.SYS_FUNCS** bezieht sich auf die Erkennung von Ausfällen einzelner sicherheitskritischer TOE-Komponenten. Das Sicherheitsziel O.MAN_FUNCS stellt sicher, dass das TOE selbst erkennen kann, wenn einzelne sicherheitskritische Komponenten des TOEs ausfallen, und dies für autorisierte Benutzer erkenntlich macht.

Die Sicherheitsrichtlinie **P.AUD_DETECT** bezieht sich auf Verfügbarkeit von 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 TOE angeboten werden, die zur Prüfung bzw. zur Erkennung von sicherheitsrelevanten Ereignissen 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.I&A	O.MAN_FUNCS	O.MAN_ROLES	O.MAN_MANAGE	O.AUD_GEN	O.AUD_REVIEW	OE.ENV_PROTECT	OE.ENV_RESOURCE	OE.ENV_NETWORK	OE.ENV_DEV	OE.TOE_INSTALL	OE.TOE_ADMIN	OE.TOE_USER	OE.AUD_TIME
T.DEV_UNAUTH	X	X														
T.DEV_MASK	X	X										X				
T.DEV_ACCESS												X				
T.SYS_ACCESS			X		X				X	X					X	
T.COM_PRIVACY										X	X					
T.COM_INTEG										X	X					
A.ENV_SERVER									X	X						
A.ENV_CLIENT												X			X	
A.ENV_OS									X	X						X
A.NET_SUPPORT											X					
A.ADM_NONEVIL													X	X		
P.SYS_MANAGE						X										
P.SYS_FUNCS				X												
P.AUD_DETECT							X	X	X							X

Tabelle 8: Abdeckung der Bedrohungen, Annahmen und Sicherheitsrichtlinien

5 Definition erweiterter Komponenten (ASE_ECD)

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*[12] vom 25. Juli 2007 für IDS-Systeme. Als Basis wurden Komponenten der Audit-Familie (FAU) aus dem Part 2 der CC verwendet. Zweck dieser Anforderungen ist es, das 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 Ereignissen aus IDS_SDC.1.1 die Speicherung von Details gefordert. Durch die Selektion der Ereignisse in IDS_SDC.1.1 ist dies nicht sinnvoll, da einzelne Ereignisse ausgeschlossen werden können. Um dies zu beheben, wurde die Funktion dahingehend angepasst, dass nur zusätzliche Informationen zu den in IDS_SDC.1.1 gewählten Ereignissen 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 con- figuration, 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:
  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.

[12] Protection Profile IDS http://www.commoncriteriaportal.org/files/ppfiles/pp_ids_sys_br_v1.7.pdf

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.1.1 The 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 (ASE_REQ)

In diesem Kapitel werden die funktionalen Anforderungen für den TOE 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 außer dem nicht-autorisierten Benutzer. Ein autorisierter Benutzer wird mit den in den TSF-Daten (Kapitel 1.4.4) 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 1.4.4) 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 TOE enthaltene Management-Server, wie in Kapitel 1.4 definiert.
- Endgeräte (*End devices*): Endgeräte (siehe auch Kapitel 6.1.4) werden vom TOE mit den in den TSF-Daten (Kapitel 1.4.4) angegebenen Sicherheitsattributen assoziiert.
- Netzwerkkomponenten (*Network devices*): Netzwerkgeräte (siehe auch Kapitel 6.1.4) werden vom TOE mit den in den TSF-Daten (Kapitel 1.4.4) angegebenen Sicherheitsattributen assoziiert.
- Administrative Verbindung (*Administrative session*): Verbindung eines autorisierten Benutzers mit der Benutzerschnittstelle des TOEs. 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 packets*): Pakete mit Daten, welche während einer Netzwerkkommunikation übertragen werden. 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 TOE zur Datenerfassung abgefragt werden.

6.2 Funktionale Sicherheitsanforderungen an den TOE

6.2.1 Security 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 Tabelle 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 Tabelle 9*.

SFR	Event	Details
FAU_GEN.1	Start of the Engine	-
	Shutdown of the Engine	-
FMT_MOF.1	Modification of actions	old value, new value
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
FPT_TST.1	System failure	component, reason

Tabelle 9: Details for FAU_GEN.1

Note 1: The dependency to FPT_STM.1 (FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.) is met due to the timestamps provided by the system environment and therefore not defined as separate SFR.

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 Tabelle 10 with* the capability to read *audit information as specified in Tabelle 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 Identification and authentication (FIA)

FIA_UID.2 – User identification before any action:

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

- FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 – User authentication before any action:

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

- The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3 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 Tabelle 11* to *authorised users which are associated with one of the roles as specified in Tabelle 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 Tabelle 12* to *authorised users which are associated with one of the roles as specified in table Tabelle 12.*

TSF data	Administrator	Operator	Helpdesk	Revisor	Nicht-autorisierter Benutzer
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	-
Own user account	Full access	Full access	Full access	Full access	-

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

6.2.4 Protection of the TSF (FPT)

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 and the Database*.
- FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *the TSF data in the Database*.
- FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *the TSF contained by the Engine*.

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.

6.2.5 Intrusion Detection System (IDS)

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) *networksession_denied, 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* Tabelle 8 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	previous security configuration, new security configuration
IDS_SDC.1	networksession_denied	denied reason
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 networksession_started and networksession_endet. The event security configuration changes refers to the macmon event authorization_changed.

Note 6: The event networksession_denied is related to a denied connection attempt. If an end device fails to connect to the network, the unauthorised event will arise.

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) *list of authorised end devices*
- 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 6: The analysis function *list of authorised end devices* compares 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 TOEs

Das TOE erfüllt die Anforderungen an die Vertrauenswürdigkeit für EAL2 erweitert um ALC_FLR.1. Die einzelnen Anforderungen sind in Tabelle 14 zusammengefasst.

Klasse	Komponente	Komponententitel
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 das TOE-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
Lebenszyklusunterstützung	ALC_CMC.2	Benutzung eines CM-Systems
	ALC_CMS.2	TOE-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 TOE, weil somit eine Basissicherheitsleistung zu gewährleisten erreicht wird.

Die EAL2 soll dem Anwender einen grundlegenden Qualitätsstandard und eine 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 TOEs 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 TOEs auf hoher Ebene analysiert werden, um das Sicherheitsverhalten zu verstehen.

Die Analyse wird unterstützt durch unabhängiges Testen das TOE-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 TOE und durch einen Nachweis der Sicherheit der Auslieferungsprozeduren.

Die Erweiterung von EAL2 auf EAL2+ durch ALC_FLR.1 wurde gewählt, um die Entdeckung und Beseitigung von offensichtlichen Sicherheitsfehler des TOEs sicherzustellen und überprüfbar zu machen.

6.4 Argumentation zu den SFRs

Die Tabelle 15 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[13] bei allen erkannten Geräten in der Liste von autorisierten Endgeräten 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.I&A** verlangt, dass jeder Benutzer vorm Zugriff auf den TOE erfolgreich identifiziert und authentifiziert sein muss und nur mit den Rechten seiner Benutzerrolle auf den TOE zugreifen kann. FIA_UID.2 und FIA_UAU.2 stellen sicher, dass das TOE einem Benutzer keine TSF zur Verfügung stellt, bevor dieser nicht identifiziert und erfolgreich authentifiziert ist.

[13] 802.1X-Zugangsdaten bzw. MAC-Adresse, abhängig vom Typ des Endgerätes

Das Sicherheitsziel **O.MAN_FUNCS** verlangt die Prüfung sicherheitskritischer Bestandteile des TOEs durch den TOE selbst. FPT_TST.1 sorgt dafür, dass das TOE periodisch die korrekte Funktionsweise der Engine 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 oder der Datenbankverbindung für den Anwender ersichtlich wird. In Verbindung mit IDS_RCT.1 ist es ebenfalls möglich, eine automatische Reaktion (Alarm-E-Mail) zum Ausfall eines der genannten TOE-Bestandteile auszulösen.

Das Sicherheitsziel **O.MAN_ROLES** verlangt die Unterstützung von verschieden Rollen für Benutzer. Durch FMT_SMR.1 wird sichergestellt, dass die Rollen Administrator, Operator, Helpdesk und Revisor vom TOE 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 TOEs 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.AUD_GEN** verlangt das Auditdaten erzeugt werden. FAU_GEN.1 und FAU_GEN.2 fordern das Erzeugen von Auditdaten und legen den Informationsumfang der Auditeinträge fest. Zusätzlich werden durch IDS_SDC.1 und IDS_ANL.1 die Erzeugung und der Umfang für Ereignisse im Netzwerk gefordert.

Das Sicherheitsziel **O.AUD_REVIEW** verlangt die Möglichkeit des Audit Review. 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.

	O.NAC_DETECT	O.NAC_REACT	O.I&A	O.MAN_ROLES	O.MAN_MANAGE	O.AUD_GEN	O.AUD_REVIEW	O.MAN_FUNCS
FAU_GEN.1						X		X
FAU_GEN.2						X		
FAU_SAR.1							X	
FAU_SAR.2							X	
FAU_SAR.3							X	
FIA_UID.2			X					
FIA_UAU.2			X					
FMT_MOF.1					X			
FMT_MTD.1				X	X			
FMT_SMF.1					X			
FMT_SMR.1				X				
FPT_TST.1								X
IDS_SDC.1	X					X		
IDS_ANL.1	X	X				X		
IDS_RCT.1		X						X
IDS_RDR.1							X	

Tabelle 15: Abdeckung der Sicherheitsziele durch SFRs

7 Zusammenfassung der TOE-Spezifikation (ASE_TSF)

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

7.1 Sicherheitsfunktionen des TOEs

7.1.1 Mapping SFRs zu den Sicherheitsfunktionen

Die Tabelle 16 liefert ein Mapping zwischen den Sicherheitsfunktionen des TOEs und den verwendeten SFRs. Das Mapping wird in der nachfolgenden Argumentation zu den Sicherheitsfunktionen beschrieben.

	SF Audit	SF I&A	SF Management	SF NAC
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAR.1	X			
FAU_SAR.2	X			
FAU_SAR.3	X			
FIA_UID.2		X		
FIA_UAU.2		X		
FMT_MOF.1			X	
FMT_MTD.1			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_TST.1			X	
IDS_SDC.1	X			X
IDS_ANL.1	X			X
IDS_RCT.1				X
IDS_RDR.1	X			X

Tabelle 16: Abdeckung der Sicherheitsziele des TOEs durch SFRs

7.1.2 SF Audit

Der TOE generiert zu sicherheitskritischen Ereignissen und allen Änderungen an den TSF-Daten immer Auditdaten (FAU_GEN.1) in Form von Datenbankeinträgen oder Logdateien. Die Auditdaten zu

Änderungen an den TSF werden hierbei immer dem verantwortlichen Benutzer zugewiesen (FAU_GEN.2).

Alle vom TOE generierten Auditdaten können vom Administrator, dem Operator, dem Helpdesk und dem Revisor (FAU_SAR.1) über die webbasierte Benutzeroberfläche des Management-Servers abgefragt werden. Der Zugriff des Helpdesk ist allerdings auf Berichte zu Endgeräten beschränkt. Der Zugriff auf die Auditdaten ist ausschließlich für autorisierte Benutzer möglich, welche sich zuvor erfolgreich am TOE angemeldet haben (FAU_SAR.2). Die Auditdaten werden über die Benutzeroberfläche für den Benutzer in Form von Logdateien oder Berichten aufbereitet (FAU_SAR.1). Die so aufbereiteten Daten können beliebig gefiltert und im Falle der Berichte beliebig sortiert werden (FAU_SAR.3). Die Auditdaten aus verschiedenen Themenbereichen sind in einzelne Logdateien bzw. Berichte eingruppiert.

In den Berichten werden auch die abgefragten Informationen vom verwalteten Netzwerk dargestellt. Hierzu gehören insbesondere die endgerätespezifischen Ereignisse zur Nachverfolgung wann ein Endgerät mit dem Netzwerk verbunden war (IDS_SDC.1). Ebenfalls werden das Ergebnis der Authentifizierung eines Endgerätes im Netzwerk (IDS_ANL.1) und potenzielle Reaktionen auf dessen Autorisierung (IDS_RDR.1) gespeichert.

Zusätzlich bietet das TOE die Darstellung von Diagrammen mit statistischen Informationen zu erfassten Netzwerkdaten an. Alle Auditdaten sind in der Datenbank bzw. dem Dateisystem des TOEs gespeichert. Wenn die Kapazität der Datenbank erschöpft ist, werden neue Informationen ignoriert und eine Fehlermeldung an den Benutzer ausgegeben.

7.1.3 SF Identifikation und Authentifizierung (I&A)

Vor jeglichem Zugriff auf die Benutzeroberfläche des Management-Servers verlangt der TOE, dass der Benutzer sich identifiziert (FIA_UID.2). Alle ausgeführten Aktionen werden so vom TOE diesem Benutzer zugeordnet. Um die Identität des Benutzers festzustellen, muss sich dieser erfolgreich am TOE authentifizieren (FIA_UAU.2).

Ohne erfolgreiche Authentifizierung hat ein Benutzer ausschließlich Zugriff auf die Anmeldeseite des TOE. Die Anmeldung am TOE erfolgt über die Benutzeroberfläche mit der Eingabe des Benutzernamens und des Passwortes. Die Zugangsdaten werden dabei geschützt vom Browser zum TOE übertragen, wo diese dann mit den gespeicherten Daten abgeglichen werden. Das Passwort wird dabei vom TOE ausschließlich als Hashwert vorgehalten. Ist die Authentifizierung erfolgreich, wird die Autorisierung des Benutzers berechnet und der Zugriff zur Benutzeroberfläche gestattet. Die Sicherheitsattribute des Benutzers werden mit dessen Verbindung assoziiert und nur die rollenspezifischen Inhalte werden angeboten. Schlägt die Authentifizierung fehl, wird der Benutzer erneut zur Eingabe der Zugangsdaten aufgefordert.

Das TOE unterstützt mehrfache, 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 TOE bekommt.

7.1.4 SF Management

Das TOE bietet Managementmöglichkeiten über die Benutzeroberfläche, um den TOE kontrollieren und überwachen zu können. Dabei haben die Benutzer unterschiedliche Berechtigungen auf die Funktionen und Daten zum Management des TOEs. Die Berechtigungen werden mit der Rolle des jeweiligen Benutzers assoziiert.

Sicherheitskritische Funktionen können nur von Benutzern mit den Rollen Administrator und Operator deaktiviert oder angepasst werden, während der Benutzer mit der Rolle Revisor nur den aktuellen Status der Funktionen ermitteln kann (FMT_MOF.1). Das gleiche gilt für den Zugang zu allen TSF-Daten (FMT_MTD.1), wobei hier zusätzlich die Benutzer mit der Rolle Helpdesk Zugriff auf die Eigenschaften von autorisierten Endgeräten haben.

Insgesamt bietet der TOE die folgenden Managementfunktionen zur Verwaltung der folgenden Objekte an (FMT_SMF.1):

- Benutzern
- NAC-Regeln
- Systemeinstellungen
- Autorisierte Endgeräte
- Netzwerkkomponenten

Über die Managementfunktionen zur Verwaltung von Benutzern hat der Administrator die Möglichkeit, einem Benutzer die vordefinierten Rollen Administrator, Operator, Helpdesk und Revisor zuzuweisen (FMT_SMR.1). Eine Änderung des Passwortes ist nur für den eigenen Account möglich. Ausgenommen sind hierbei Benutzer mit der Rolle Administrator, welche alle Passwörter über die Benutzerverwaltung verändern können.

Zum Schutz eines unbemerkten Ausfalls der Sicherheitsleistung des TOEs führt das TOE periodisch Selbsttests durch (FPT_TST.1). Hierbei werden die verschiedenen Subsysteme des TOEs vom Management-Server kontrolliert. Bemerkt der Management-Server den Ausfall eines Subsystems, wird dies neugestartet. Außerdem werden Ausfälle der einzelnen Subsysteme auch auf der Startseite der GUI dargestellt. Diese Schutzfunktion ist nur funktionsfähig, solange der Management-Server nicht komplett ausfällt.

7.1.5 SF Netzwerkzugriffskontrolle (NAC)

Zur Überwachung des verwalteten Netzwerks sammelt der TOE periodisch Daten von Netzwerkkomponenten ein oder erhält Endgeräte-802.1X-Zugangsdaten von Netzwerkverteilern zur Verifizierung (IDS_SDC.1). Alle gesammelten Daten enthalten dabei insbesondere die Information, wann (Start- und Endzeitpunkt), von welchem Standort (physikalischer Port) und in welchem Umfang (VLAN-Autorisierung) der Endgeräte-Zugriff auf das Netzwerk bestand. Außerdem enthalten die Daten Informationen darüber, ob dessen Zugriff abgelehnt wurde oder sich dessen Autorisierung

verändert hat. Das Endgerät selbst wird dabei anhand seiner MAC-Adresse und den 802.1X-Zugangsdaten identifiziert.

Die Autorisierung eines Endgerätes wird auf Grundlage der Analyse der gesammelten Daten vorgenommen (IDS_ANL.1). Die Authentifizierung wird mit Hilfe der 802.1X-Zugangsdaten (Benutzername/Passwort oder Zertifikat) und der Liste autorisierter Endgeräte bestimmt. Anhand der Konfiguration am Endgerät und/oder weiterer Regeln wird dann die Autorisierung berechnet.

Das Ergebnis der Autorisierung wird vom TOE an den Netzwerkverteiler zurückgeschickt, welcher auf Basis der Daten reagiert (IDS_RCT.1). Als Reaktion kann der Netzwerkverteiler den Zugriff auf das Netzwerk für das Endgerät durch Aktivierung des physikalischen Ports freigegen und ggf. ein konkretes VLAN schalten, oder den physikalischen Port inaktiv lassen und dem Endgerät den Zugriff verwehren. Darüber hinaus werden vom TOE direkt als Reaktion E-Mails versendet, falls bei der Abfrage der Netzwerkgeräte nicht autorisierte Endgeräte erkannt werden.

Alle gesammelten Daten, Analyseergebnisse und ausgeführte Reaktionen werden vom TOE über die grafische Oberfläche für den Administrator, Operator, Helpdesk und Revisor zur Verfügung gestellt (IDS_RDR.1). Sonstige Benutzer erhalten vom TOE keinen Zugriff auf diese Daten.

macmon secure GmbH

Alte Jakobstraße 79-80

10179 Berlin

Tel.: +49 30 2325 777 - 0

www.macmon.eu