macmon NAC Handbuch

Version 5.31

2022-04-26

macmon secure GmbH
Alte Jakobstraße 79-80
10179 Berlin
Germany

Phone: +49 (0)30 / 23 25 777 - 444
Fax: +49 (0)30 / 23 25 777 - 200
Mail: supe="vertical-align:top;text-align:center;">2c

1. Einleitung

1.1. Motivation

Wenn man damit beschäftigt ist, alles zu machen, wie soll man je etwas verbessern?

Das Thema Netzwerkzugangskontrolle oder **Network Access Control (NAC)** ist ein sehr aktuelles Thema, welches in vielen Unternehmen plötzlich diskutiert wird. Doch weshalb? Und weshalb erst jetzt, wo es doch bereits seit vielen Jahren offene Netzwerk-Ports und auch entsprechende Produkte gibt?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert wegen dieser Gefährdungen schon lange im Grundschutzhandbuch (BSI) die Verhinderung ungesicherter Netzzugänge (Maßnahme 2.204) und vor allem ein Verbot sowie eine regelmäßige Kontrolle bezüglich der Installation und der Nutzung nicht freigegebener IT-Komponenten (Maßnahme 2.216). Für Router und Switches (Baustein 7.11) wird direkt eine port-basierte Zugriffskontrolle (Maßnahme 4.206) verlangt.

Der Hauptgrund für die Zunahme des Bedarfs an funktionierenden NAC-Lösungen dürfte jedoch der rasante Anstieg der Anzahl der vielen verschiedenen Endgeräte sein. Jeder Benutzer bzw. Mitarbeiter hat heute ein Smartphone oder einen eigenen Laptop, Ultrabook bzw. Tablet. Die Möglichkeiten und den Komfort dieser Geräte erwarten die Mitarbeiter heute und zukünftig auch an ihrem Arbeitsplatz. Viele Unternehmen halten dem Druck, mitarbeitereigene Geräte zuzulassen zwar noch stand, es kann nur eine Frage der Zeit sein, bis diese Standhaftigkeit zumindest in Teilen aufweicht. Zudem sind viele Netzwerkgeräte, wie auch einfache Access Points heute so leicht zu bedienen, dass Mitarbeiter ohne weiteres entsprechende „Verteiler“ mitbringen, anschließen und betreiben können, ohne dass die IT-Abteilung es mitbekommen würde. Die Mitarbeiter selbst haben jedoch oftmals kein Gefühl und auch nicht das Knowhow für „gefährliche“ Geräte.

Die genutzten Netzwerkgeräte sind aber in der Regel gar nicht für den Unternehmenseinsatz gedacht und damit auch nicht einfach zentral managebar. Das Zulassen einzelner Geräte öffnet jedoch den Zugang für alle anderen, wenn nicht zeitgleich oder vorher eine entsprechende Kontrollinstanz eingeführt wurde. Diese Instanz heißt Network Access Control.

Ein weiterer Grund, warum aktuell die Netzwerkzugangskontrolle auf dem Vormarsch ist, ist die Tatsache, dass es inzwischen funktionierende NAC-Lösungen gibt. Bis vor einiger Zeit basierte die Mehrheit der angebotenen Produkte auf Technologien und Lösungsansätzen, die nicht oder nicht zufriedenstellend arbeiteten. So sollten flächendeckend Appliances im Netzwerk verteilt werden, die den Traffic von unerwünschten Systemen blockieren, Software auf allen Clients installiert werden, die die Kommunikation nur zu eigenen Geräten erlauben oder die Infrastruktur aufwendig auf Komponenten eines Herstellers umgerüstet werden. Die Aufwände und auch die Kosten für solche Implementierungen führten zwangsläufig zum Scheitern der Projekte und auch zu einer negativen Empfindung des gesamten Themas.

Heute geht es auch besser!

Neue und alte, aber dafür gereifte Technologien, bieten heute die Möglichkeit, eine Kontrolle und damit eine zentrale Sicherheitsinstanz einzuführen, ohne das bestehende Netzwerk anpassen zu müssen, hohe Investitionen tätigen zu müssen oder einem extremen Aufwand gegenüber zu stehen. Die Möglichkeiten folgen dabei vor allem dem Dreisatz „Sicherheit, Komfort und Übersicht“:

Sicherheit
Durch die Kontrolle aller Netzwerkzugänge und den Einsatz zukunftssicherer Technologien stellt eine NAC-Lösung die zentrale Machtinstanz im Netzwerk dar. Das heißt, eine zentrale Instanz kann über die Zugangsberechtigungen von neuen, fremden, eigenen und sicheren, eigenen und unsicheren Geräten sowie von Gastgeräten entscheiden. Die eingesetzten Techniken decken das gesamte Netzwerk

– lückenlos und unabhängig von der bestehenden Netzwerkinfrastruktur - ab und agieren unabhängig von den vielen eingesetzten Betriebssystemen der Endgeräte. Viele weitere Vorteile ergeben sich zudem daraus, dass macmon integrierbar mit anderen bestehenden oder geplanten Sicherheitsprodukten ist.

Komfort

Selbstverständlich soll der Pflegeaufwand so gering und auch so einfach wie möglich sein, um die gewonnene Sicherheit nicht zu einer Belastung werden zu lassen. Das bedeutet, dass wir bei jeder Funktionalität Wert darauf legen, die Komplexität im Hintergrund abzubilden und parallel möglichst viele Vorteile zum täglichen Arbeitsablauf beizutragen. So sind z. B. dynamische VLAN-Konfigurationen für die eigenen Endgeräte, einfache und zugleich sichere Zugänge für Gäste und sonstige Besucher (wie Dienstleister) elementare Vorzüge von NAC. Der Betrieb eines Netzwerkes, gleich welcher Größe, kann mit erheblichem täglichen Aufwand einhergehen – macmon als zentrale Komponenten kann und sollte daher zur Reduzierung dieses Aufwandes beitragen.

Übersicht

Die Kontrolle aller Netzwerkzugänge von zentraler Stelle und dynamische Netzwerkkonfigurationen bedeutet, dass viele Informationen vorhanden und nutzbar sein müssen, die anderweitig genutzt werden sollten. Eine grafische Darstellung der Topologie, eine Übersicht der aktuell und zuletzt betriebenen Endgeräte mit Details wie z. B. Ort der letzten Sichtung, usw. sowie freie oder mehrfach genutzte Ports, sind Ergebnisse, die macmon Ihnen liefern kann. Die Netzwerktransparenz steigt enorm und jedes Gerät lässt sich per Knopfdruck finden bzw. identifizieren.

1.2. Systembeschreibung

Überblick

Das Produkt macmon ist eine Software-Lösung zur Kontrolle des Zugriffs von Endgeräten auf ein lokales Netzwerk. Der Einsatz von macmon ermöglicht die Verwaltung und Überwachung des Netzwerks und der enthaltenen Komponenten. macmon kann unabhängig von den im zu überwachenden Netzwerk eingesetzten Protokollen und Betriebssystemen der Server, PCs und sonstigen Komponenten genutzt werden.

Der Server auf dem macmon installiert ist, wird zentral in das bestehende Netzwerk eingebunden und benötigt keine Agenten in den zu überwachenden Netzwerkbereichen (sehen Sie bitte folgende *Abbildung 1: Systemübersicht*). Der zu überwachende Bereich kann sich über mehrere Standorte, Domänen oder Organisationen erstrecken. Vom Server werden unterschiedliche Daten von verschiedenen Quellen im Netzwerk abgefragt. Zur Überwachung managebarer Netzwerkgeräte im Netzwerk muss der Zugriff per SNMP (v1, v2C, v3/MIB II/RFC 1493) und evtl. per Telnet oder SSH bestehen. Auf Grundlage der im Netzwerk 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. Zur Durchsetzung der Autorisierung bzw. zum Aussperren von Endgeräten aus dem Netzwerk ist zusätzlich ein schreibender SNMP-Zugriff auf die betroffenen Netzwerkgeräte erforderlich.

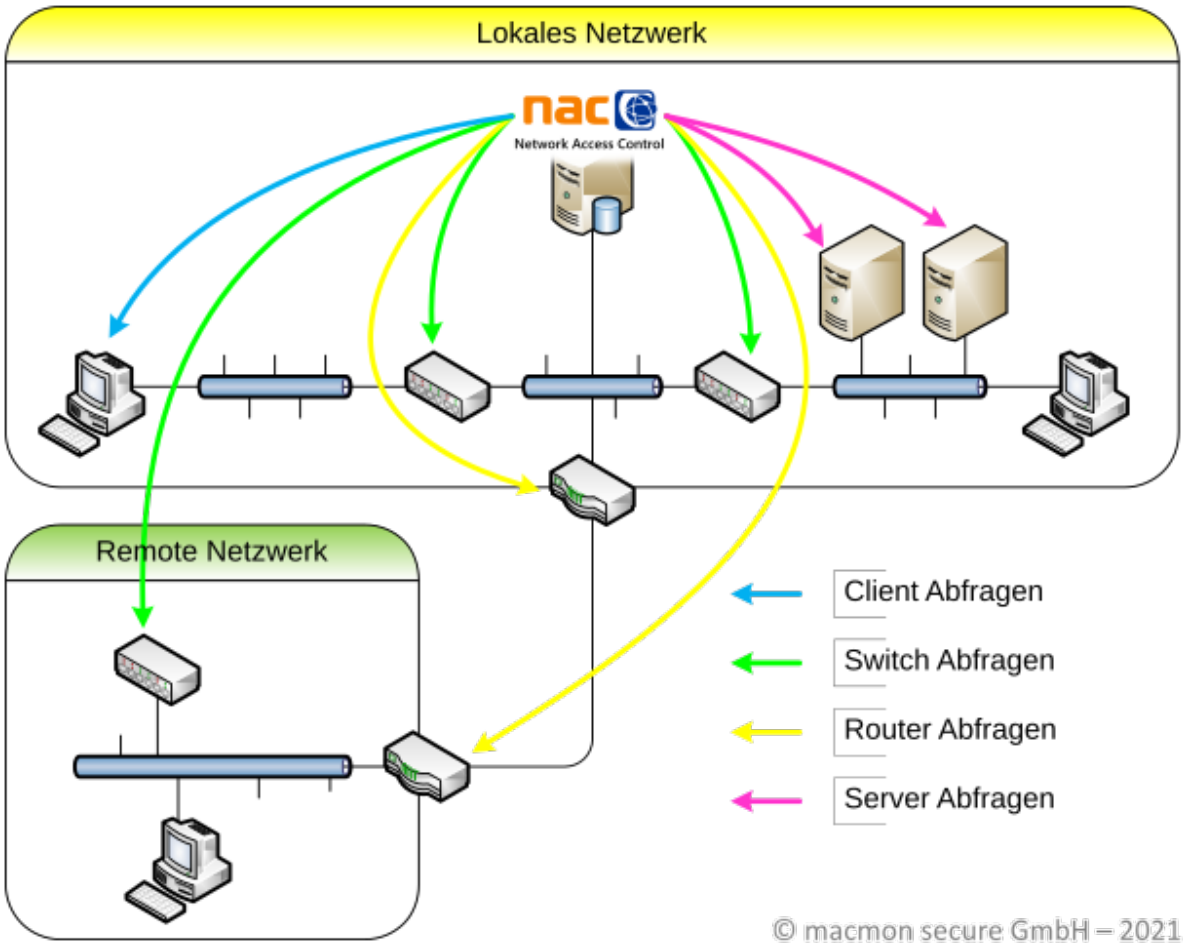

Abbildung 1: Systemübersicht

Funktionalität

macmon bietet folgenden Möglichkeiten zur Erhöhung der Sicherheit im Netzwerk an:

- Erkennung und Identifizierung aller aktiven Komponente (Switches, Router) im Netzwerk
- Authentifizierung der Endgeräte (PC, Notebooks usw.) anhand der MAC-Adresse oder des Fingerprints bzw. der -Signatur vom macmon-Agent. Zusätzlich kann das Footprinting eingesetzt werden, um Geräte ohne macmon-Agent zuverlässiger zu identifizieren.
- 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 Berichte und Statistiken zu Ereignissen im Netzwerk
- Gewährung von temporären Netzwerkzugängen für Gäste, Besucher, Lieferanten, Berater und Kunden durch das Gästeportal.

System-Architektur

macmon besteht aus einem Server, welcher die drei Kernkomponenten des Systems (Scan-Engine, Ereignis-Regelwerk und GUI) enthält, und dem macmon-Agenten. Ein weiterer Bestandteil von macmon ist eine Datenbank, welche als gemeinsames Speichermedium eingesetzt wird (sehen Sie *Abbildung 2: Systemarchitektur)*.

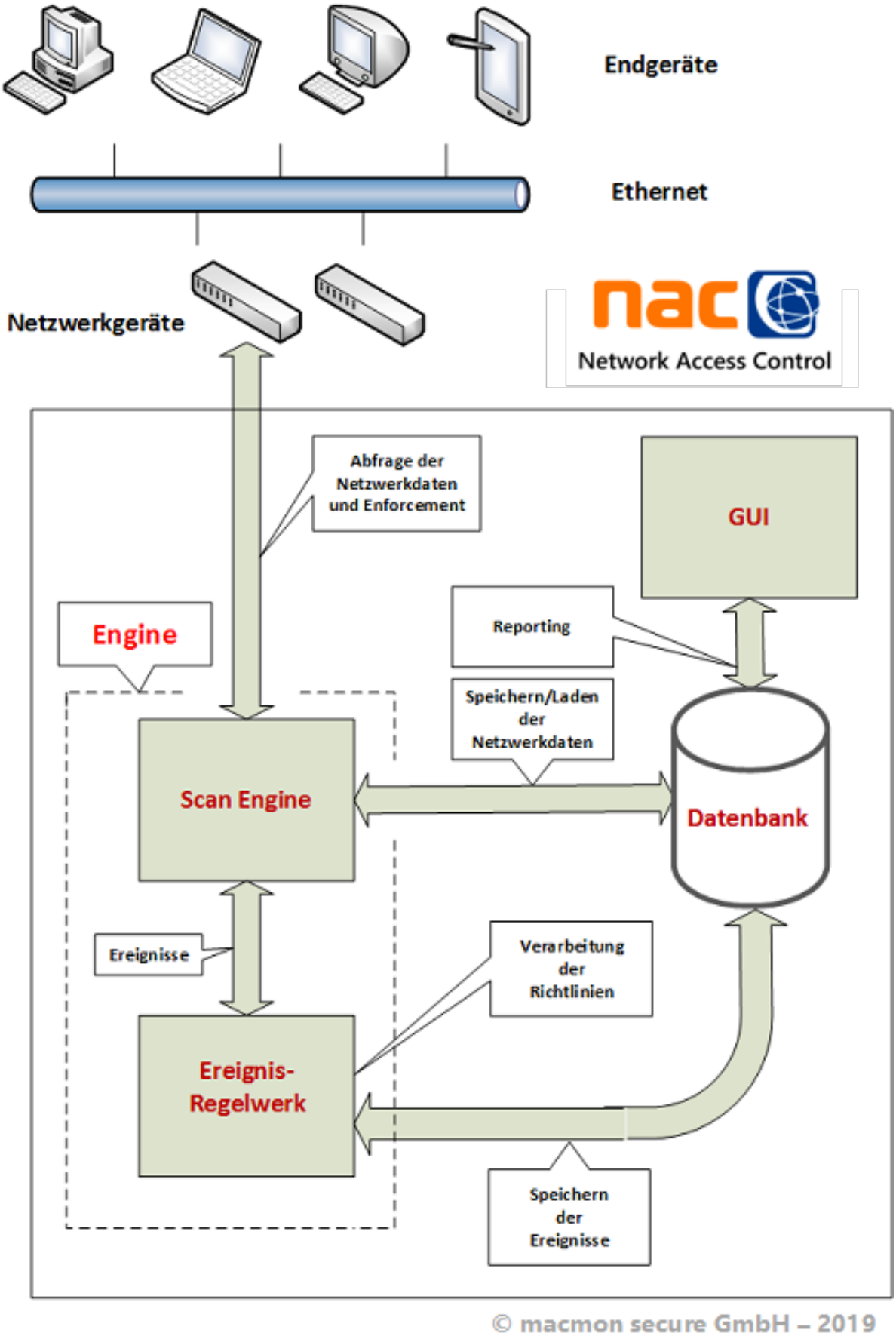
Endgeräte
Ethernet
Netzwerkgeräte
nac
Network Access Control
Abfrage der Netzwerkdaten und Enforcement
GUI
Engine
Reporting
Speichern/Laden der Netzwerkdaten
Scan Engine
Datenbank
Ereignisse
Verarbeitung der Richtlinien
Ereignis-Regelwerk
Speichern der Ereignisse
© macmon secure GmbH – 2019

Abbildung 2: Systemarchitektur

- ***macmon-Server***: Der Server stellt den zentralen Management-Server des Systemes dar und bietet alle Management-Funktionen an. Die folgenden Kernkomponenten sind im Server enthalten:
    - **Scan-Engine**: Die Engine führt die Erfassung von Netzwerkdaten durch. Alle empfangenen Daten werden verarbeitet und in der Datenbank gespeichert. Danach werden die ermittelten Informationen analysiert und erkannte Ereignisse (Events) werden in der Datenbank hinterlegt.
    - **Ereignis-Regelwerk**: Die von der Engine gespeicherten Ereignisse werden verarbeitet und analysiert. Dabei werden die Inhalte der Ereignisse anhand eines Regelwerks überprüft. Das Regelwerk besteht aus benutzerspezifischen Richtlinien, welche vom Administrator verwaltet werden.
    - **Web-Oberfläche (GUI)**: Die Bedienung des Servers geschieht primär über eine web-basierte Benutzeroberfläche, auf die per Browser zugegriffen werden kann. Alternativ steht die macutil als Kommandozeilen-Schnittstelle **macutil** zur Verfügung. Über **macutil** können rudimentäre Operationen auch lokal mit Befehlen auf der Kommandozeile des Servers aufgerufen werden. Die Schnittstelle ist außerdem auch ferngesteuert als macutil unter Verwendung von HTTPS verfügbar.
    - **Datenbank**: Eine relationale Datenbank stellt den primären Speicher dar. In der Datenbank werden alle Einstellungen, Audit-Daten und die verarbeiteten Netzwerkdaten sowie erkannten Ereignisse gespeichert.
- ***macmon-Agent***: Zur Erfassung und Prüfung sicherheitsrelevanter Daten auf unternehmenseigenen Endgeräten, wird auf diesen eine Agenten-Software benötigt. Der macmon-Agent prüft verschiedene Eigenschaften des Endgerätes und übermittelt die Ergebnisse über eine verschlüsselte Verbindung an den Server. Zur Ermittlung der Eigenschaften werden verschiedenen Agent Scan-Job Scripte Agent-Scan-Job-Skripte verwendet.

macmon-Appliance

Die macmon-Appliance gibt es auf Hardware- oder Software-Basis (als virtuelle Maschine). macmon und das entsprechende Betriebssystem sind auf der jeweiligen Appliance in der aktuellsten Version vorinstalliert. **Die macmon-Appliance verfügt über eine eigenständige Web-Oberfläche (GUI)**. Über diese GUI können wichtige Appliance-Funktionalitäten wie

- Backup
- Dienste
- E-Mail
- Hilfe
- Hochverfügbarkeit
- Netzwerkkonfiguration
- Sicherheit
- SNMP
- Sprache
- Status
- Systemzeit
- Update
- Zertifikat
- Zugangsdaten

verwaltet werden. Mehr dazu finden Sie in der mitgelieferten Datei **ApplianceManual-de_DE.pdf** bzw. in der Appliance-Hilfe: macmon-GUI -> Status -> Appliance –> Appliance-Konfiguration –> Hilfe.
Hinweis: Die Datensicherung des macmon-Servers wird über die Funktionalität **Backup** der macmon-Appliance durchgeführt.

1.3. Begriffe und Definitionen

Begriff	Bedeutung in macmon
Authentifizierung	Unter der Authentifizierung verstehen wir die aufgaben- und benutzerabhängige Zugangs- und/oder Zugriffsberechtigung. Die Authentifizierung hat den Zweck, Systemfunktionen vor Missbrauch zu schützen. In der Kommunikation stellt die Authentifizierung sicher, dass der Kommunikationspartner auch derjenige ist, für den er sich ausgibt. Die Authentifizierung und Autorisierung von Endgeräten wird auf Grundlage der im Netzwerk erfassten Daten vorgenommen: MAC-Adresse, Fingerprint, Footprint, Kerberos (GUI), 802.1X (RADIUS), MAB, MS Active Directory, Benutzername/Passwort. Es gibt folgende Authentifizierungslevel: • niedrig (MAC), • mittel (802.1X), • hoch (802.1X + Zertifikat). Anderes formuliert, als Authentifizierung bezeichnen wir den Nachweis und damit die Echtheit einer Identität. Es wird also nur überprüft, ob jemand der ist, für den er sich ausgibt.

Autorisation

Autorisation (Ermächtigung, Vollmacht) bedeutet gewähren von Rechten (z. B. Zugriffsrechten). Wenn Sie eine Datei den anderen Benutzern per Dateifreigabe zur Verfügung stellen, autorisieren Sie diese, auf die Datei zuzugreifen. Möglicherweise haben Sie das Recht der anderen beschränkt, sodass diese die Datei z. B. nicht löschen können. **Anderes formuliert ist die Autorisation das *Ergebnis* einer Autorisierung**.

Die Regeln von macmon dienen dazu, nach der Authentifizierung an der Benutzeroberfläche eine Autorisation stattfinden zu lassen, wodurch Sie z. B. die Möglichkeit haben einem Benutzer trotz erfolgreicher Authentifizierung den Zugang zu verweigern. Im Falle der Benutzeroberfläche können den Benutzern anhand von Regeln Rollen zugeteilt werden, die dann bei der Autorisation zugewiesen werden.

Autorisierung (Befugnis, Berechtigung)

Autorisieren/Autorisierung steht für den *Vorgang* „Autorisation erteilen“. Die Autorisierung ist eine Berechtigung, eine explizite Zulassung, die sich auf einen Benutzer bezieht. Sie definiert wer in einem Netzwerk welchen Dienst und welche System-Ressourcen nutzen darf. Bei der Autorisierung werden dem Nutzer Rechte zugewiesen. Sie berechtigen den Benutzer eine bestimmte Aktion auszuüben. Um einen wirksamen Schutz zu erreichen, sollten bei der Rechtevergabe der Nutzer nur für die Ressourcen autorisiert werden, die er unbedingt benötigt.

Auf Grundlage der im Netzwerk erfassten Daten wird die Authentifizierung und Autorisierung von Endgeräten vorgenommen. MAC-Autorisierung mit

statischem DHCP bietet die Möglichkeit, statische DHCP-Einträge automatisch in die Unternehmensgeräte von macmon zu übernehmen.

Damit auch Mitarbeiter (Sponsoren/BYOD), das Gästeportal nutzen können, müssen Richtlinien für die Autorisierung und Authentifizierung über das Regelwerk konfiguriert werden.

Eine 802.1X-Autorisierung (auch MAB) durchläuft dabei folgende Schritte:

1. Zuerst erfolgt die Authentifizierung (Verifizierung einer Identität) gegen eine Identitätsquelle.
2. Anschließend wird mit Hilfe von Regeln die Autorisation (Berechtigung) ermittelt.
3. Als letztes wird die Berechtigung an den Authentifikator (Switch/AP) gesendet.

Anderes formuliert, die Autorisierung sagt aus, was ein Benutzer alles darf und was nicht. Die Autorisierung geht häufig mit der Authentifizierung einher, da eine reine Autorisierung praktisch nutzlos ist, wenn Sie nicht die Echtheit einer Identität verifizieren.

Compliance	IT-Compliance beschreibt in der Unternehmensführung die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft. Die macmon-Komponente Client Compliance kann Compliance-Status-Werte von Endgeräten entgegennehmen und daran anknüpfend Aktionen ausführen. Es können Messergebnisse von beliebigen externen Quellen an macmon übergeben werden. Solange ein Endgerät von keiner Quelle als non-compliant eingestuft wird, bewertet macmon das Endgerät insgesamt als compliant. Meldet eine Quelle einen non-compliant-Status, gilt das Endgerät insgesamt als non-compliant.
Endgerät	Als Endgerät bezeichnen wir Computer-Hardware in einem TCP/IP-Netzwerk. Der Begriff kann sich auf Desktop-Computer, Laptops, Smartphones, Tablets, Thin Clients, Drucker oder andere spezielle Hardware wie zum Beispiel POS-Terminals beziehen. macmon regelt mit Hilfe von Network Access Control (NAC) den Zugang der Engeräte zum lokalen Netzwerk des Anwenders.
Enforcement	Durchsetzung, Anwendung (von Richtlinien)

Fingerprint	In sicherheitsrelevanten Techniken dient der Fingerprint zum Erkennen von eindeutigen Merkmalen von Daten. Der Fingerprint enthält ausgewählte Scandaten, die auf Veränderung überwacht werden. Der Parameter FINGERPRINT ist eine Aufzählung von Scanvariablen. Liefert eine Quelle nach einem Scanvorgang sein Ergebnis dem macmon-Server, so werden die Werte der hier angegebenen Scanvariablen mit den schon bekannten Werten auf Veränderung überprüft.
Footprint	Footprinting ist ein Begriff aus der IT-Sicherheit. Er bezeichnet die Informationsbeschaffung über ein Zielsystem. Footprints nennen wir Informationen über das Betriebssystem eines Gerätes, die hierbei - im Gegensatz zu Fingerprints - keine eindeutige Identifikation darstellen. Zwei gleich konfigurierte Drucker desselben Models z. B. haben den gleichen Footprint bzw. ein Client könnte Microsoft Windows Vista SP0 oder SP1, Server 2008 SP1 oder Windows 7 als Betriebssystem aufweisen.

Identität	Eine Identität ist der eindeutige Identifikator für eine Person, Organisation, Ressource oder einen Service zusammen mit optionaler zusätzlicher Information (z. B. Berechtigungen, Attributen). Die Identität umfasst eindeutig kennzeichnende Merkmale. Identitäten im Sinne von macmon können Computernamen, Benutzernamen oder MAC-Adressen sein. Es gibt aktiven und inaktiven Identitätsquellen, die in der Reihenfolge angegeben werden, in der sie bei einer Authentifizierung z. B. am Gästeportal abgearbeitet werden. Bei einer Authentifizierung wird lediglich versucht gegen die erste Identitätsquelle zu authentifizieren, in der die mitgegebene Identität gefunden wurde. Identitätsquellen sind Quellen wie Datenbanken, Microsoft Active Directory, SAML Identity Provider und LDAP-Verzeichnisdienste, aus denen Geräte- und Benutzeridentitäten bezogen werden können. In macmon werden diese Quellen für die Authentifizierung und Autorisierung bei der Benutzeroberfläche, beim RADIUS-Server und im Gästeportal verwendet.

MAC-Adresse

Eine MAC-Adresse ist die Hardware-Adresse eines Netzwerkadapters, die weltweit eindeutig vergeben wird und zur Identifikation des Netzwerkadapters im Netzwerk dient. Die Vergabe dieser MAC-Adressen wird über die IEEE (Institute of Electrical and Electronics Engineers, Inc. (IEEE)) koordiniert und letztlich durch Hersteller von Netzwerkprodukten umgesetzt. Bei der IEEE können über eine Datenbank bzw. Online-Abfrage die Hersteller von Netzwerkkomponenten an Hand der festgestellten MAC-Adressen identifiziert werden.

Eine MAC-Adresse hat eine Länge von 6 Byte, besteht somit aus 12 Hexadezimalziffern und wird üblicherweise in nachfolgender hexadezimaler Schreibweise notiert (zum Beispiel 00-10-DC-B0-98-75). Die ersten 3 Bytes, die sogenannte OUI (Organizationally Unique Identifier), verweist auf den Hersteller (in diesem Beispiel die MICRO-STAR INTERNATIONAL CO., LTD.). Die verbleibenden 3 Byte werden vom Hersteller zur eindeutigen Kennzeichnung seiner Produkte genutzt. Sie können die oui.txt-Datei über den Link OUI herunterladen.

Monitoring

Im Netzwerkmanagement ist das Monitoring eine vom Administrator regelmäßig ausgeführte Überwachungsfunktion für das Netzwerk, für dessen Funktionen und für die Hardware. Mit dem Monitoring werden leistungsrelevante Netzwerk-Kennwerte wie die Verzögerungszeiten, das Antwortzeitverhalten, der Datendurchsatz, die Paketverluste, die Last-verteilung und andere Kennwerte hin überprüft.

Netzwerkgerät	Als Netzwerkgeräte gelten alle aktive Bestandteile eines Rechnernetzes. Aktive Netzwerkkomponenten sind alle Geräte, die aktiv Signale verarbeiten bzw. verstärken können. Sie benötigen dazu eine Stromversorgung. Zu dieser Gruppe gehören Hubs und Switches, Router, Bridges, Firewalls, Server usw.. macmon fragt die Daten der im Netzwerk vorhandenen Netzwerkgeräte ab mit dem Ziel, die angeschlossenen Endgeräte zu erfassen und mit Hilfe der NAC-Richtlinien ihren Zugang zum Netzwerk zu steuern.
Skalierbarkeit	Eine Skalierbarkeit ist eine Zusammenfassung mehrerer macmon-Server (Instanzen) zu einem Verbund. Das ermöglicht den beteiligten macmon-Instanzen untereinander zu kommunizieren und somit benötigte Informationen auszutauschen. Diese Funktionalität dient dazu, die Arbeitslast einer einzelnen macmon-Instanz auf andere Instanzen zu verteilen. Die Skalierbarkeit ist nicht mit dem Hochverfügbarkeitscluster zu verwechseln!
SNMP	Das Simple Network Management Protocol (SNMP; deutsch: Einfaches Netzwerkverwaltungsprotokoll) ist ein Netzwerkprotokoll, das von der IETF (Internet Engineering Task Force) entwickelt wurde, um Netzwerkgeräte (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station - z. B. macmon - aus überwachen und steuern zu können. (Sehen Sie auch z. B. Elektronik-Kompendium).
Widget	Ein Widgwet ist eine Komponente einer grafischen Benutzeroberfläche. Steuerelement, ein Bedienelement einer grafischen Benutzeroberfläche.

2. Monitoring

Monitoring ist ein Überbegriff für alle Arten der unmittelbaren systematischen Erfassung (Protokollierung), Messung, Beobachtung oder Überwachung eines Vorgangs oder Prozesses mittels technischer Hilfsmittel, z. B. mittels macmon.

Für das Monitoring benötigen Sie die so genannte Observer-Lizenz.

2.1. Allgemein

Die Netzwerkverwaltung grenzt den Umfang des von macmon zu überwachenden Netzwerks ein. Hier werden alle Netzwerkgeräte verwaltet, die von macmon überwacht werden sollen.

Die einfachste Form der Überwachung des Netzwerkes ist zu wissen, welche Endgeräte überhaupt und wo genau im Unternehmensnetzwerk betrieben werden.

Hierzu ist es notwendig die Netzwerkgeräte, über welche der Netzzugang realisiert wird, zu überwachen. Das können Switches sein, mit deren Ports Endgeräte per Kabel verbunden sind. Es können aber auch Access Points oder WLAN-Controller sein, mit denen Endgeräte via Funknetz verbunden sind.

macmon kann von diesen Netzwerkgeräten nicht nur erfahren, wo sich ein Endgerät befindet, sondern auch weitere Details wie gerade verwendete IP-Adresse(n) oder konfigurierten DHCP-Adresszuweisungen, DNS-Namen usw. ermitteln.

Switches pflegen im Rahmen ihrer Funktionalität eine Liste der MAC-Adressen der Endgeräte und die Zuordnung zu dem Port, über diesen zuletzt ein Datenpaket von diesem Endgerät vermittelt wurde. Diese Liste wird meist **Forwarding Database (FDB)** oder auch **Source Address Table (SAT)** bzw. **Content Addressable Memory (CAM)**

genannt.

IP-Router besitzen in der Regel ein umfangreiches Wissen über IP-Adressen der angeschlossenen Netzwerke und welche IP-Adressen die MAC-Adressen verwenden (**Address Resolution Protocol – ARP**). Es muss natürlich möglich sein, die gewünschten Informationen von diesen Netzwerkgeräten abfragen zu können, entweder über das **Simple Network Management Protocol (SNMP)** oder mittels der Protokolle **SSH (Secure Shell)** bzw. **Telnet (Teletype Network)**. Es handelt sich dann um managebare Netzwerkgeräte.

2.1.1. Netzwerkgeräte, -gruppen und -klassen

Die zu überwachenden Netzwerkgeräte werden in Gerätegruppen eingeteilt. Jeder Gerätegruppe werden vordefinierte Scanaktionen zugewiesen. Einer Gerätegruppe *Switch* werden typischerweise Aktionen wie Interfaces auslesen oder MAC-Adressen auslesen zugewiesen. Die erforderlichen Zugangsdaten und Scanintervalle werden ebenfalls je Gerätegruppe erfasst. Gerätegruppen können z. B. nach Gesichtspunkten wie Netzwerkstruktur, Gerätetyp des Netzwerkgerätes oder Lokalität angelegt werden.

Jedes in macmon erfasste Netzwerkgerät erbt die Einstellungen seiner ihm zugewiesenen Gerätegruppe. Die Zugangsdaten lassen sich allerdings bei Bedarf direkt am Netzwerkgerät überschreiben.

macmon verfügt über eine interne, globale **Root-Gruppe**, die in der GUI nicht angezeigt wird und nicht editiert oder gelöscht werden kann. Alle bereits vorhandenen Gruppen werden Kinder der neuen Root-Gruppe. Jede neu zu erstellende Netzwerkgerätegruppe kann Mitglied einer bestimmten Elterngruppe werden. Hiermit wird eine **Hierarchie** der Netzwerkgerätegruppen eingeführt. In der Gruppen-Liste wird beim Gruppennamen der absolute Pfad in dieser Hierarchie angezeigt, z. B. Europa/Berlin/Server (der Hierarchie nach sind Europa und Berlin die Elterngruppen).

Wichtig: Es wird empfohlen, die benötigten Gerätegruppen **vor** dem Erfassen der Netzwerkgeräte zu konfigurieren.

Die Gerätegruppen definieren ausschließlich welche Aktionen auf ein Netzwerkgerät angewandt werden sollen. Wie diese Aktion ausgeführt wird, gibt die Geräteklasse des Netzwerkgerätes vor. *Die Geräteklasse definiert hierzu die konkreten Methoden, mit denen das Netzwerkgerät abgefragt wird*.

Geräteklassen sollten im Normalfall nicht manuell angelegt werden. Wird ein neues Netzwerkgerät angelegt, wird beim ersten Scan des Netzwerkgerätes von der Engine anhand der SNMP-System-ID (**SysObjectID**) eine passende Klasse zugewiesen. Existiert für die betreffende ID noch keine Klasse, so wird automatisch eine Klasse angelegt. Die angelegte Klasse erhält automatisch die Methoden einer bereits existierenden Klasse, welche eine übergeordnete SysObjectId besitzt. Existiert z. B. eine Klasse Cisco mit der SysObjectId `1.3.6.1.4.1.9` und es wird ein neues Netzwerkgerät mit der SysObjectId `1.3.6.1.4.1.9.12345` erkannt, so bekommt die neue Klasse alle Methoden aus der bereits bestehenden Cisco-Klasse. Es gibt immer eine "globale default Template-Klasse" mit dem Namen *_Default Template Class*. Diese hat eine leere SysObjectId und passt, falls keine andere passende Template-Klasse bestimmt werden konnte. Die neu angelegten Klasse wird aus dem Namen des Herstellers und aus den letzten Ziffern des SysObjectIDs gebildet, z. B. **Colubris Networks Inc..1.52**. Diese Klasse kann dann mit den jeweiligen passenden Methoden konfiguriert werden. Allen Netzwerkgeräten mit der gleichen SNMP-System-ID wird dann automatisch diese Klasse zugewiesen.

macmon liefert eine Menge von vorkonfigurierten Geräteklassen. Diese Klassen können individuell angepasst werden. Bei einem Produkt-Update werden neue Geräteklassen (falls vorhanden) in macmon integriert.

Die automatische Zuweisung von Geräteklassen ist nur bei Netzwerkgeräten möglich, welche die Abfrage mit Hilfe von SNMP unterstützen. Wichtig ist hierbei, dass am Netzwerkgerät, dessen Gruppe oder global in macmon Zugangsdaten vom Typ SNMP konfiguriert sind.

Die abzufragenden Netzwerkkomponenten werden von macmon tabellarisch aufgelistet. Sinnvolle Einträge sind Netzwerkgeräte, die SNMP, Telnet oder SSH unterstützen und für die in macmon

Scanmethoden existieren. Es stehen Scanmethoden für Switches, Router und Server zur Verfügung. Jedes durch macmon abzufragende Netzwerkgerät wird in der Netzwerkgeräteliste durch eine Zeile repräsentiert. Die jeweils eingestellte Gerätegruppe bestimmt, welche Daten vom Netzwerkgerät abgefragt werden. Die angegebene Geräteklasse legt die konkreten Scanmethoden fest, welche bei dem Netzwerkgerät zur Anwendung kommen.

macmon kann die neu eingerichteten Netzwerkgeräte anhand der vorhandenen Geräteklassen automatisch klassifizieren. Der Administrator **muss** die Netzwerkgeräte zu den vorhandenen Gerätegruppen (Switch, Router, Server usw.) zuordnen. Damit wird die Verknüpfung Netzwerkgerät - Aktion hergestellt.

Hinweise zur Konfiguration der Netzwerkgeräte finden Sie im Kapitel Netzwerk.

Wichtiger Hinweis:
Eine zweckmäßige Auswahl der zu überwachenden Switches kann die Performance und das Gesamtverhalten von macmon wesentlich positiv beeinflussen. Die Überwachung von Switches einschließlich ihrer verwendeten Interfaces in ausreichend geschützten Bereichen, wie zum Beispiel Serverräumen, Infrastrukturräumen, Rechenzentren usw. liefert in den meisten Fällen lediglich redundante Daten. Es ist wesentlich zweckmäßiger und ausreichend solche Switches zu überwachen, deren Anschlüsse nicht anderweitig geschützt werden können. In der Regel trifft das die so genannten Access Switches für den Etagenbereich (Tertiär-, evtl. Sekundär-Bereich) einer LAN-Verkabelung zu. Die Überwachung eines Backbone Switches, der lediglich Verbindungen mit anderen Switches oder Server-Links mit hohen Verfügbarkeitsanforderungen bereitstellt, ist nicht zweckmäßig.

2.1.2. Links

Für das Erkennen von Switches und deren Verbindungen untereinander stehen u. a. zwei Protokolle, das **Cisco Discovery Protocol** (**CDP**) und das **Link Layer Discovery Protocol** (**LLDP**) zur Verfügung. CDP wurde

von der Firma Cisco entwickelt und wird z. T. auch von anderen Herstellern unterstützt. Das LLDP ist eine Weiterentwicklung des CDP, ist im Standard 802.1AB beschrieben und damit herstellerunabhängig.

Bidirektionale Links

Zur Definition eines Links werden die zwei miteinander verbundenen Interfaces ausgewählt und als Link gespeichert. Da ein Link eine gerichtete Verbindung von einem Interface zu einem anderen Interface ist, legt das System automatisch zwei Einträge für die zwei Richtungen an. Auch beim Auflösen eines Links wird der Link der Gegenrichtung automatisch mit entfernt. Dass die Links gerichtet gespeichert werden ist vor allem der Tatsache geschuldet, dass auch die Protokolle LLDP und CDP unidirektional konzipiert sind und somit jeweils einen Eintrag pro Richtung vorsehen.

Hinweise zur verwaltung der Links finden Sie im Kapitel Netzwerk.

2.1.3. Netzwerk-Sessions

Eine Netzwerk-Session beschreibt, dass ein Endgerät an einem Switch-Interface oder über WLAN Zugang zum Netzwerk hat. Eine Netzwerk-Session wird gestartet, wenn macmon an einem Netzwerkgerät ein neu angeschlossenes Endgerät erkennt oder eine RADIUS-Authentifizierung zu einem Endgerät verarbeitet wird.

Eine Netzwerk-Session wird beendet, wenn das Endgerät vom Netzwerk getrennt wurde bzw. eine bestimmte Zeit nicht mehr kommuniziert hat.

Es werden dann jeweils die Ereignisse *networksession_started*, *networksession_ended* bzw. *networksession_denied* erzeugt.

2.2. Topologieerkennung

macmon stellt die Scanmethoden CDP-Abfrage und LLDP bzw. LLDP ohne Port-Abfrage bereit. Mit ihnen können für einen Switch dessen nächste Nachbarn ermittelt werden. Die Scanmethoden *CDP* und/oder *LLDP* bzw. *LLDP ohne Port-Mapping* sind der Netzwerkgeräteklasse des Switches hinzuzufügen. Die CDP/LLDP Informationen können zum automatischen Setzen der Verbindungen zwischen den Netzwerkgeräten genutzt werden. Die **uplink_auto**-Eistellung muss unter Einstellungen --> Scan-Engine --> Uplink gewählt werden.

macmon generiert beim Auffinden von benachbarten Netzwerkgeräte das Ereignis *device_new*. Die neuen Netzwerkgeräte werden in Netzwerk --> Geräte-Vorschläge aufgelistet und können von hier in die Liste der Netzwerkgeräte übernommen werden. Das Ereignis *device_new* wird nur dann generiert, wenn macmon die IP-Adresse des anderen Netzwerkgerätes aus den CDP/LLDP-Daten direkt oder durch ARP-Informationen an Hand der durch CDP/LLDP übermittelten MAC-Informationen ermitteln kann.

Die Verbindungen zwischen den Netzwerkgeräten werden nur dann gesetzt, wenn von beiden verbundenen Netzwerkgeräte konsistente CDP- bzw. LLDP-Informationen vorliegen, d. h. jeweils das Interface am Nachbar-Netzwerkgerät eindeutig ermittelt werden konnte. Interfaces vom Typ 'wlan' (z. B. Access Points eines WLAN-Controllers) werden bei der Suche nach Nachbar-Interfaces ignoriert. Die Interfaces erhalten dann das Flag *CDP* bzw. *LLDP* in der Spalte *Verbindungen* auf der Seite der Netzwerkgeräte-Interfaces und es wird das Ereignis *link_set* generiert.

Automatisch gesetzte Verbindungen zwischen den Netzwerkgeräten werden automatisch wieder gelöscht, wenn beide Netzwerkgeräte den Link in ihren CDP-/LLDP-Daten nicht mehr verzeichnen oder eines der Geräte gelöscht wird. Es wird das Ereignis *link_removed* generiert.

2.3. Zugangsdaten

Zugangsdaten sind strukturierte, geheime Informationen, die den Zutritt zu etwas (Gerät, Dienst usw.) ermöglichen.

Um sich bei den Netzwerkgeräten authentifizieren zu können, müssen Zugangsdaten in macmon hinterlegt werden. Diese können dann einem Netzwerkgerät direkt oder über die Netzwerkgerätegruppen zugeordnet werden. Es kann notwendig sein, mehrere Zugangsdaten für unterschiedliche Protokolle zuordnen zu müssen.

Für reines Monitoring genügen Zugangsdaten, welche einen ausschließlich lesenden Zugriff auf die gewünschten Informationen erlauben.

In macmon werden unterschiedliche Typen von Zugangsdaten unterstützt. Der Typ legt dabei das Netzwerk-Protokoll fest, über welches mit dem Netzwewrkgerät kommuniziert wird. Zurzeit werden von macmon folgende Protokolle, Verfahren und Architekturen unterstützt:

- SNMPv1/SNMPv2c
- SNMPv3
- Telnet
- SSH
- HTTP(S)
- LDAP(S)
- RADIUS-Secret
- WMI
- Meraki verwaltetes Netzwerkgerät
- API-Schlüssel

Warnung: Zur Gewährleistung der Vertraulichkeit und Integrität bei der Datenabfrage der Netzwerkgeräte muss **ein Protokoll mit Verschlüsselung** verwendet werden. Hierzu gehören ausschließlich SNMPv3, SSH und RADIUS-Secret (802.1X). Die weiteren Protokolle stellen ein Sicherheitsrisiko dar und sollten nicht mehr verwendet werden.

Hinweise zur Verwaltung der Zugangsdaten finden Sie im Kapitel Zugangsdaten.

2.4. Datenerfassung im Netzwerk

Zur Datenerfassung im Netzwerk nutzt macmon die Protokolle **SNMP**, **DHCP** und den Dienst **DNS**.

2.4.1. SNMP-Datenverwendung in macmon

macmon

macmon secure GmbH
Alte Jakobstraße 79-80
10179 Berlin
Germany

Phone: +49 (0)30 / 23 25 777 - 444
Fax: +49 (0)30 / 23 25 777 - 200
Mail: supe="vertical-align:top;text-align:center;">2c macmon