

NEUE FEATURES:

macmon TP
macmon guest service
für Mobile Devices und
WLAN Support
macmon 802.1X

macmon[®]
the network security system

Strict Network
Access Control





macmon's job.

macmon schützt Ihre IT vor Angriffen und sorgt dafür, dass sich nur autorisierte, authentifizierte und sicher konfigurierte Systeme im Unternehmensnetz befinden. **macmon** erkennt, meldet und unterbindet den Betrieb von Fremdsystemen im unternehmenseigenen Netzwerk. **macmon** arbeitet herstellerübergreifend mit allen Netzwerkkomponenten. **macmon** überwacht zentral verteilte Infrastrukturen.

Daten ausspähen oder **manipulieren** kann jeder, der eine Zugriffsmöglichkeit zum Netzwerk bekommt und mit seinem Gerät unbemerkt ins lokale Netz eindringt. Wenn der Zugang zum Netzwerk nicht permanent überwacht wird, können Angreifer unentdeckt ihr kriminelles Werk verrichten. Für die Installation und Benutzung nicht freigegebener IT-Komponenten fordert das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** ein Verbot, das regelmäßig zu kontrollieren ist. Zitat: „Die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“ IT-Grundschutzkataloge, Maßnahme 2.216

macmon unterstützt Sie bei der Errichtung von **Verteidigungslinien**, die von Angreifern überwunden werden müssen, um Zugang zum Netzwerk zu erhalten. Abhängig von der Gefährdungslage des Unternehmens bietet **macmon** durch seinen modularen Aufbau Abwehr gegen gezielte und fahrlässige bekannte Angriffsszenarien, die von innen erfolgen können.

Die **erste „Line of Defence“** verhindert den Zugang unbekannter Geräte. Geräte, die am Netzwerkverkehr teilnehmen dürfen, müssen sich über Ihre MAC-Adresse, einen „Fingerprint“ oder ein Zertifikat ausweisen. Die **zweite „Line of Defence“** schützt vor Angriffen auf Netzwerkkomponenten und vor Adressmanipulationen und **verhindert so Lauschangriffe auf den Datenverkehr**. In weiteren Verteidigungslinien dürfen nur sicher konfigurierte Geräte am Netzwerk betrieben werden und es werden mit **macmon** Schutzzonen für definierte Bereiche (z.B. Personal, Vorstand, Produktion, ...) oder bestimmte Gerätetypen (z.B. Drucker, Notebooks, ...) eingerichtet.

Angriffe oder Schädigungen haben nicht immer einen kriminellen Hintergrund. Auch das in guter Absicht mitgebrachte private Notebook eines Mitarbeiters oder der Laptop von Kunden und Dienstleistern können Viren und Trojanern unbeabsichtigt Tür und Tor öffnen. Geräte, die nicht Ihren Standardkonfigurationen und Sicherheitsrichtlinien entsprechen, stellen ein enormes Sicherheitsrisiko für Ihr Netzwerk dar.

macmon's practice.

macmon

Erkennen, Lokalisieren und Abwehr fremder Geräte

macmon schützt Ihr Netzwerk gegen das Einbringen von unerwünschten Geräten. **macmon** verschafft eine umfassende Übersicht über alle Geräte im gesamten Netzwerk und bietet ein Live-Bestandsmanagement. Neue Geräte, die ans Netz angeschlossen werden, erkennt und lokalisiert **macmon** sofort. Bei unbekanntem Geräten, alarmiert **macmon** und leitet – bei entsprechender Konfiguration – automatisch Gegenmaßnahmen ein.

macmon vlan manager

Differenzierte Zugangskontrolle im Netzwerk

Mit dem **macmon** vlan manager können Sicherheitsstrukturen eingeführt und betrieben werden, die eine flexible Zugangskontrolle zu Netzwerkressourcen ermöglichen. **macmon** unterstützt bei der Umsetzung verschiedener Sicherheitskonzepte für die Bereitstellung eines differenzierten Netzwerkzugangs. Besucher- oder Quarantänenetze, statische und dynamische VLANs können so leicht implementiert und betrieben werden.

macmon advanced security

Erkennung, Abwehr und Lokalisierung interner Angriffe

macmon advanced security erkennt, lokalisiert und schützt vor internen Angriffen, die mittels ARP-Spoofing, ARP-Poisoning oder MAC-Spoofing erfolgen. **macmon** erkennt IP-/MAC Adressmanipulationen anhand von Zustandsveränderungen, Vergleichen mit vorgegebenen Werten oder DHCP-Daten und kann auf diese sofort reagieren. MAC-Adressmanipulationen werden über eine dynamische IP-Protokollstack-Analyse (Footprinting) erkannt.

macmon client compliance

Ermittlung und Bewertung des Sicherheitsstatus der Netzwerkarbeitsplätze

Die **macmon** client compliance stellt sicher, dass die von **macmon** zugelassenen Geräte nur dann vollen Zugang zum Netzwerk erhalten, wenn sie der Security-Policy des Unternehmens entsprechen. Geräte ohne ausreichenden Virenschutz oder mit nicht aktuellem Patchlevel werden erkannt und aus dem Netz ferngehalten. In Ergänzung zu dieser sehr flexiblen Lösung unterstützt **macmon** auch das Statement of Health (SOH) Client-Server-Protokoll (TNCCS-SOH) der Trusted Computing Group. Dieser anerkannte Standard zur Überwachung der Client-Sicherheit wird z. B. von Microsoft im Rahmen seiner NAPArchitektur bereitgestellt.



macmon's practice.

macmon guest service mit WLAN-Support

Kontrollierter Netzwerkzugang von Gästen

macmon guest service ist ein Management- und Reporting-System zur Gewährung von kontrollierten temporären Netzwerkzugängen für Gäste, Dienstleister, Lieferanten, Berater und Kunden. Dies ist besonders wichtig für die mit spezifischen Sicherheitsrisiken behafteten Mobile Devices wie Notebook, Netbook, iPad oder Smartphone. **macmon guest service** steuert die Netzwerk-Zugriffsrechte, die dem Besucher eingeräumt werden sollen, über ein Voucher-System. Der Gutschein definiert, auf welche Netze (VLANs) der Gast Zugang erhält, legt einen Gültigkeitszeitraum fest und enthält darüber hinaus Informationen über den Gast, den Anlass des Besuches und den unternehmensinternen Betreuer.

macmon TP

Zuverlässige Geräte-Identifizierung durch Nutzung des Trusted Platform Moduls

Ausgangspunkt der Hochsicherheitskomponente **macmon TP** zur zuverlässigen fälschungssicheren Authentifizierung von Endgeräten ist das „Trusted Platform Modul (TPM). **macmon TP** nutzt den TPM-Chip, der bereits in der Mehrzahl professioneller Computersysteme eingebaut ist, als unabhängige Signierinstanz. Die fest mit dem Motherboard verbundene Hardware-Komponente ist auch gegen Hardware-Angriffe geschützt. Es handelt sich somit um eine äußerst sichere Signierinstanz, die einen eindeutigen kryptografischen Schlüssel enthält. Das System **macmon TP** besteht aus einer Client-Komponente, die einen asymmetrischen **macmon**-Key erzeugt und die Endgeräte-Authentifizierung durch Signierung von Zufallswerten mit dem TPM-Chip auslöst. Die Serverkomponente von **macmon TP** übernimmt sowohl die Verwaltung der öffentlichen Schlüssel als auch die Validierung.

macmon 802.1X

Zertifikate- oder anmeldebasierter Geräte-Zugang auch für Mobile Devices

Die **macmon 802.1X**-Option bietet eine Steuerung des Netzwerkzugangs wahlweise über Zertifikate oder über eine Anmeldung. Die Zertifikate oder auch die Anmeldeinformationen können in **macmon** hinterlegt oder per LDAP von einem anderen System, zum Beispiel dem Active Directory abgefragt werden. Die Ortung und VLAN-Steuerung der Geräte erfolgt über die **macmon**-GUI. Eine 802.1X-Authentisierung ist besonders für den WLAN-Bereich zu empfehlen, da hier MAC-Adressen keinen ausreichenden Schutz bieten.

...macht sicher!

macmon's world.

Strict Network Access Control

IT-Netzwerk

monitoring

- Überwachung des gesamten Netzes, unabhängig von Betriebssystem, Protokoll und Hersteller
- Zentrale Installation, keine Agenten oder Sensoren erforderlich
- Echtzeit-Erfassung und Lokalisierung aller im Netz aktiven Geräte
- Erkennung von Veränderungen und Umzügen
- Ermittlung und Bewertung des Sicherheitsstatus der clients („client compliance“)
- Unterstützung moderner Isolationskonzepte mit Quarantänefunktionen für nicht sichere Computer

processing

- Flexible Reaktion auf Sicherheitsvorfälle wie nicht autorisierte Geräte, Angriffe auf Switches, unberechtigte Umzüge und ARP- und MAC-Spoofing
- Benachrichtigung per E-Mail, Telefon oder SMS oder direkte Erzeugung eines Trouble Tickets im Help-Desk
- Isolation von Geräten durch Portsperrung oder Umschaltung ins Quarantänenetz
- Einfache Umsetzung von differenzierten Netzwerkzugangskonzepten
- Anbindung an andere Managementtools und Sicherheitssysteme über Schnittstellen.

reporting

- Umfassender Überblick über alle Endgeräte im Netzwerk und deren Lokalisierung
- Sicherheitsreports zu Vorfällen nach Bedeutung gewichtet
- Grafische Darstellung aller Ereignisse in frei wählbaren Zeiträumen
- Statistiken zu Endgeräten-Aktivitäten und Device Nutzung
- Auswertung über die Belegung der Switchports
- Exportmöglichkeit aller Reports zur weiteren Analyse

administration

- Webbasierte, browser-unabhängige grafische Benutzeroberfläche
- Vereinfachte Pflege der Referenzdaten durch Autoimport, Lernports oder Schnittstellen zu anderen Datenbanken
- Selbständige Erkennung der Netzwerktopologie
- Funktionsrollen zur Steuerung der Administrationsrechte
- Umfassendes Auditing zur Nachvollziehbarkeit

ZIELE UND NUTZEN

macmon

- ... erkennt, meldet und verhindert nicht zugelassenes Betreiben von Fremdsystemen im Netzwerk.
- ... erkennt Angriffe auf Switches und schützt vor ARP- und MAC-Spoofing.
- ... erfordert geringsten administrativen Aufwand.
- ... ermöglicht leichte Skalierbarkeit.
- ... bietet Schnittstellen zu anderen Sicherheitssystemen.

macmon

- ... ist die strategische und moderne Lösung gegen Datenmanipulation und -spionage im LAN.
- ... arbeitet nicht erkennbar für Angreifer.
- ... erkennt wireless gestartete Angriffe.
- ... bietet eine einfache Umsetzung VLAN-basierter Sicherheitskonzepte.

macmon

- ... arbeitet unabhängig von eingesetzten Betriebssystemen und vom Typ der Netzwerkkomponenten.
- ... besteht aus einer Scan-Engine mit professionellem Eventmanagement.
- ... ist einfach zu implementieren – ein Server, keine Agenten.
- ... bietet ein umfangreiches Reporting.



macmon's environment.

VORAUSSETZUNGEN

für die Software-Lösung

Hardware:

- Server mit 32- / 64-Bit -x86-Architektur, CPU ab 1 GHz, 1 GB RAM, 20 GB HD
- Netzwerkanbindung ab 100 Mbit/s

Software:

- Betriebssystem Microsoft Windows Server 2003/2008 oder Linux, (z.B. openSUSE, CentOS, Red Hat, Debian,...)
- Apache Webserver ab v2
- Net-SNMP ab v5.2
- Datenbanksystem: Microsoft SQL Server 2005/2008 oder MySQL ab v5
- PHP v5.1, v5.2

Switches:

Unterstützung der Standards SNMP v1, v2c, v3 und RFC1493 Bridge MIB.

Unterstützung der Standards SNMP v1, v2c, v3 und RFC1493 Bridge MIB. **macmon** unterstützt Switches, mit dem Standard RFC3580/IEEE 802.1X und ermöglicht so eine einfache, auch partielle Einführung der 802.1X-Technologie in Ihrem Haus.

Alternativ können auch über Telnet / SSH Switches und andere Netzwerk-Devices abgefragt werden.

Der **vlan-manager** unterstützt eine Vielzahl von Switches unterschiedlicher Hersteller.

Die bestehende Netzwerk- und Client-Architektur wird bei der Implementierung unverändert beibehalten.

INSTALLATION

Die Konfiguration und Installation ist einfach, sollte jedoch durch einen qualifizierten **macmon**-Engineer begleitet werden.

- Installation der Softwarekomponenten (entfällt bei der Appliance)

- Festlegung des zu sichernden Netzwerk-Bereichs
- Abbilden der Netzwerktopologie und Erfassen der Switches sowie anderer Netzkomponenten
- Aufbau der Referenzliste
- Konfiguration und Test des Regelwerks entsprechend den Anforderungen
- Einweisung in Funktionen und in die Administration von **macmon**

macmon appliance

Die **macmon** appliance ist die schlüsselfertige Komplettlösung in der **macmon** Familie mit einer optimal abgestimmten Hardware. **macmon** ist vorkonfiguriert, so dass die Integration in eine beliebige IT-Infrastruktur (herkömmliche oder virtualisierte Umgebung) sofort erfolgen kann.

Die Konfigurationsarbeiten zur Einbindung der Appliance in Ihr Netzwerk und zur Einstellung der Datensicherungsoptionen erfolgen über eine grafische Oberfläche. Die Sicherung und die Wiederherstellung der Bewegungsdaten ist auf ein beliebiges Netzwerklaufwerk möglich.

Sollte es Probleme mit der Hardware geben, wird Ihnen per Austausch-Service am Folgetag ein Ersatzgerät bereitgestellt. Sie können dann per USB-Stick den Auslieferungszustand oder den Zustand der letzten Image-Sicherung problemlos wieder herstellen.

Das Gerät wird standardmäßig mit einem 3-jährigen Next Business Day Change-Service ausgeliefert. Die Hardware ist in verschiedenen Ausbaustufen verfügbar, z. B. der Einstiegs-Server für bis zu 25.000 Nodes: 1HE für 19" Rack mit INTEL 3420 Mainboard, Intel Xeon X3430 2,4 GHz Prozessor, 4 GB RAM, 2x 250 GB HDD und vier 10/100/1000 Intel Netzwerkadaptern.

Mit der Cluster-Option steht Ihnen eine ausfallsichere **macmon**-Lösung zur Verfügung.

NUTZUNGSLIZENZ

macmon wird nach Anzahl der **macmon**-Server und Anzahl der zu überwachenden Nodes lizenziert. Die **macmon client compliance** richtet sich nach Anzahl der überwachten Arbeitsplatz-PCs.

profile.

mikado soft ist ein deutscher IT-Hersteller spezialisiert auf Netzwerk-Sicherheit. Das von mikado soft entwickelte, herstellerunabhängige und modulare Network Access Control System **macmon** schützt das LAN vor unautorisierten, nicht sicheren Geräten und internen Angriffen.

Die mit dem Sicherheitssystem bereitgestellten Technologien werden, um ihre Wirksamkeit nicht zu verlieren, den bestehenden und zukünftigen Bedrohungsszenarien laufend angepasst und erweitert.

Hierzu gehört:

- **Die Analyse von heutigen und zukünftigen Angriffsszenarien.**
Die Bewertung und Auswahl geeigneter Technologien zur Abwehr von Angriffen auf Netzwerkdienste.
- **Die Implementierung der Technologien in Produkte.**
Der Schwerpunkt der Entwicklung liegt in der kosten-effizienten und benutzerfreundlichen Bereitstellung der Technologien.

In enger Kooperation mit Forschungseinrichtungen beteiligt sich das Unternehmen an der Weiterentwicklung von Sicherheitstechnologien und -standards.

Die Produkte der mikado soft gewährleisten, dass sich in einem Unternehmensnetz nur autorisierte, authentifizierte und sicher konfigurierte Systeme befinden.

mikado soft gmbh

Bülowstraße 66 · 10783 Berlin

T 030. 217 90 0 · F 030.217 90 200

info@mikado.de · www.mikadosoft.de

Ihr Ansprechpartner:



Volkswagen AG, Wolfsburg
„**macmon** überwacht unsere Produktionsnetze und gibt uns die volle Transparenz.“



Südwestrundfunk, Stuttgart
„Wir schätzen **macmon** als wichtigen Baustein im Sicherheitskonzept unseres Netzwerkbetriebes.“



Harting KGaA, Espelkamp
„Durch den Einsatz von **macmon** ist uns ein wichtiger Schritt in Richtung Zugangssicherheit gelungen.“



Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT), Bonn
„Der Einsatz ist ein bedeutender Schritt in Richtung mehr Sicherheit. Wir sind mit dem Produkt sehr zufrieden.“



Medizinische Hochschule Hannover
„Zusammenfassend kann ich sagen, dass das Programm über hervorragende Produkteigenschaften verfügt und wir sehr zufrieden sind.“



ZF Friedrichshafen AG, Friedrichshafen
„Wir schützen mit **macmon** sensible Zonen unseres IT-Netzes vor Angriffen.“



Hamburger Hochbahn, Hamburg
„Mit **macmon** schützen wir unsere lokalen IT-Netze.“



Berliner Stadtreinigungsbetriebe, Berlin
„**macmon** ist die ideale Sofortlösung auf dem Weg zu IEEE 802.1X.“



Vivantes Netzwerk für Gesundheit GmbH, Berlin
„Mit **macmon** haben wir eine Lösung gefunden, die Sicherheit bietet und mit geringem Aufwand durch die Administration betrieben werden kann.“



Unternehmensgruppe Theo Müller, Aretsried
„Mit **macmon** werden die Standorte autonom gesichert und zugelassene mobile Geräte können konzernweit eingesetzt werden.“



MiRO Mineraloelraffinerie, Oberrhein GmbH & Co. KG, Karlsruhe
„Zum Schutz unserer weitflächigen Infrastruktur ist **macmon** die optimale Lösung.“



Kreditanstalt für Wiederaufbau (KfW), Berlin
„**macmon** verbessert unsere IT-Sicherheit erheblich. Wir sind mit dem Tool sehr zufrieden.“