



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** verhindert den Einsatz von nicht autorisierten Geräten und den Betrieb von Software auf diesen Geräten, die zum Ausspähen, Manipulieren und Entwenden von Unternehmensinformationen genutzt werden können. **macmon** arbeitet herstellerübergreifend mit allen Netzwerkkomponenten. **macmon** überwacht zentral verteilte Infrastrukturen.

**Angriffe** auf Informationen und Daten von Unternehmen, welche in Netzwerken des Unternehmens verarbeitet werden, erfolgen zum großen Teil durch Zugang zum Unternehmensnetz **von innen**. Wenn keine Sicherheitssysteme vorhanden sind, erhalten nicht autorisierte Geräte – ausgestattet mit Software zur Beobachtung des Netzwerkverkehrs, zur Manipulation und zum Kopieren von Datenströmen – gezielt oder fahrlässig Zugang zum Netzwerk. **macmon** unterbindet den Zugang solcher Geräte und schützt die Unternehmensinformationen. Die Administratoren des Netzwerks sind jederzeit über die Teilnehmer am Netzwerkverkehr informiert und werden über Verletzungen der IT – Sicherheitsregeln bezüglich des Zugangsschutzes sofort benachrichtigt.

**Schützen Sie Ihr Netzwerk vor fremden Geräten**, wie z. B. vor Notebooks, unbekanntem Laptops und PDAs, die auch über autorisierte und unautorisierte WLAN-Access-Points in Ihr System eindringen können. **macmon** stellt sicher, dass nur registrierte und zugelassene Geräte am Netzwerkverkehr teilnehmen.

**macmon** errichtet **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.

Mit der **ersten „Line of Defence“** wird der **Zugang unbekannter Geräte verhindert**. 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 Schutzzone für definierte Bereiche (z.B. Personal, Vorstand, Produktion, ...) oder Gerätetypen (z.B. Drucker, Notebooks, ...) etabliert werden.

**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, welche nicht Ihren Standardkonfigurationen und Sicherheitsrichtlinien entsprechen, stellen ein enormes Sicherheitsrisiko für Ihr Netzwerk dar.

**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*

# ...macht sicher!

## macmon's world.

### Strict Network Access Control

# IT-Netzwerk

#### monitoring

- Überwachung des gesamten Netzes, unabhängig vom 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 der VLAN-Konfiguration und Portbelegung der Switches
- 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-Spoofing
- Benachrichtigung per E-Mail, Telefon oder SMS oder direkte Erzeugung eines Trouble Tickets im Help-Desk
- Isolation von Geräten durch Portsperren oder Umschaltung ins Quarantänenetz
- Reaktion auf Ereignisse abhängig von Uhrzeit und Tag
- Flexible Regelausführung abhängig von Endgerätetyp, Netzsegment, Switchhersteller etc.
- Einfache Umsetzung VLAN-basierter Sicherheitskonzepte mit dem VLAN-Manager
- Anbindung an andere Managementtools und Sicherheitssysteme möglich

#### 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
- Endgerätereport mit Switchport, Herstellerangabe, IP-Adresse und Gerätenamen
- Auswertung über die Belegung der Switchports
- Exportmöglichkeit aller Reports zur weiteren Analyse

#### ZIELE UND NUTZEN

##### macmon

- ... erkennt, meldet und verhindert nicht zugelassenes Betreiben von Fremdsystemen im Netzwerk.
- ... erkennt Angriffe auf Switches und schützt vor ARP-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's practice.

### administration

- Webbasierte, browser-unabhängige grafische Benutzeroberfläche, kein Java/Javaskript
- Clientunabhängig, ein Server, keine Agenten
- Ein Überwachungsserver für mehrere Standorte
- Vereinfachte Pflege der Referenzdaten durch Autoimport, Lernports oder Schnittstellen zu anderen Datenbanken
- Selbständige Erkennung der Netzwerktopologie

### 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

#### 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, Lokalisierung und Abwehr interner Angriffe

**macmon advanced security** erkennt, lokalisiert und schützt vor internen Angriffen, die mittels ARP-Spoofing, ARP-Poisoning oder manipulierten IP-Adressen erfolgen. **macmon** erkennt Adressmanipulationen anhand von Zustandsveränderungen, Vergleichen mit vorgegebenen Werten oder DHCP-Daten und kann auf diese sofort reagieren.

### 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 NAP-Architektur bereitgestellt.



# 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 Hause.

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 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 10.000 Nodes: 1HE für 19" Rack, mit AMD Opteron Quad Core 2,2GHz CPU, 2 GB RAM, 250 GB SATA2 HDD und drei 10/100/1000 BaseT 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-PC's.

## profile.

Die mikado soft gmbh entwickelt, pflegt und vertreibt IT-Sicherheitssysteme zum Schutz der Unternehmensnetzwerke. Die in den Sicherheitssystemen 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 kosteneffizienten 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.mikado-soft.de

Ihr Ansprechpartner:



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



**TOTAL Deutschland GmbH, Berlin**  
„Unser Gesamturteil: Sehr gut!“



**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.“