
... erkennt, meldet, wehrt ab und schützt!
macmon
the network security system

mikado soft

# Erhöhung der Sicherheit in Unternehmensnetzen durch Datenkonsolidierung

Wolfgang Dürr
mikado soft gmbh
CeBIT 2011

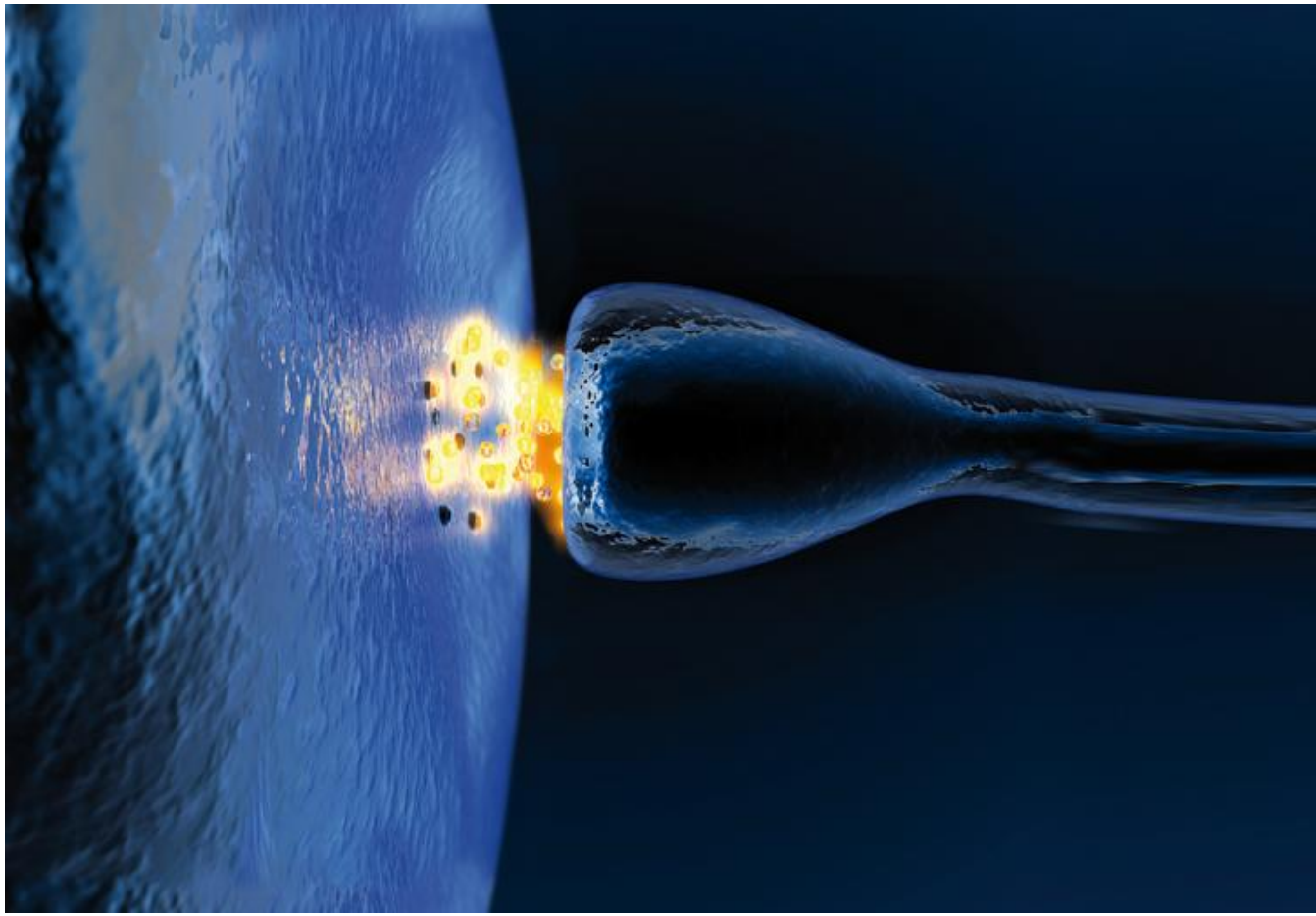
# mikado-Gruppe

Gründung
**1983**

Hauptsitz:
**Berlin**

Vertriebsbüro Süd:
**München**

Mitarbeiter:
**52 Personen**



# Leistungskatalog mikado-Gruppe

# Leistungskatalog mikado-Gruppe

## Informationssicherheit

**mikado ag**

**consulting**

**mikado ag**

**services**

**mikado soft**

**technology**

**macmon network access control (NAC)**

- advanced security
- vlan manager
- client compliance
- guest service
- macmon TP

**macmon energy**

**secure download**

# die mikado soft gmbh…

- das Technologieunternehmen der mikado-Gruppe
- Entwicklung und Vertrieb von IT-Sicherheitssoftware
- einfache Implementierung komplexer Standards für Netzwerksicherheit
- führender Anbieter herstellerunabhängiger NAC-Lösungen (Network Access Control) in Deutschland

# unsere Mission…

- **Auswahl der Technologien:**
  - Analyse der Bedrohungs-szenarien für Unternehmens-Netzwerke
  - Bewertung der Risiken
  - Bestimmung der Technologien zur Abwehr der Bedrohungen
- **Bereitstellung der Technologien:**
  - Kosten- und administrations-effiziente Produkte zur Abwehr von Angriffen gegen Unternehmens-netzwerke
  - Produkte zur Betriebs-kostensenkung von Unternehmensnetzen und IT-Arbeitsplatz-systemen
- **Weiterentwicklung der Technologien:**
  - Analyse der heutigen und zukünftigen Bedrohungsszenarien
  - Entwicklung von proaktiven Abwehr-technologien
  - Mitwirkung bei der Definition internationaler Sicherheitsstandards („Trusted Computing“)
  - enge Kooperationen mit Forschungseinrichtungen

# unsere Vision…

- Im Unternehmensnetz befinden sich nur autorisierte, authentifizierte und sicher konfigurierte Systeme.
- Die Systeme im Netz sind vertrauenswürdig und werden kosteneffizient eingesetzt.

***We assure Trusted Computing and Cost Efficiency***

**www.mikadosoft.de**

# IT Sicherheits-Situation

## Sicherheitsvorfälle verursachen erhebliche wirtschaftliche Schäden!

- Verrat von Firmengeheimnissen (Entwicklung, Angebote, Kundendaten, …)
- Datenverlust und Beschädigung von Daten
- Produktionsausfall, Ausfallzeiten
- Öffentliche Diskreditierung und Imageverlust

# Drastischer Anstieg von Sicherheitsvorfällen!

| | 2008 | 2009 | Steigerung |
|---|---|---|---|
| Von Sicherheitsvorfällen betroffene Firmen | 72% | **92%** | 28% |
| Anzahl Sicherheitsver-letzungen pro Firma (Durchschnitt) | 15 | **45** | 200% |
| **finanzieller Schaden Pfund Sterling** | zwischen 90.000 und 170.000 | **zwischen 280.000 und 690.000** | zwischen 211% und 306% |

**Quelle: Studie „Information Security Breaches Survey“, PWC, 2010**

**Für die Untersuchung befragte PWC mehr als 1.000 IT-Sicherheitsverantwortliche in britischen Unternehmen unterschiedlicher Größe. 45% beschäftigten mehr als 500 Mitarbeiter, der Rest weniger.**

## Viele Verstöße erfolgen durch Angriffe von Innen!

**Mehr als 70%** der Spione kommen aus dem eigenen Unternehmen und sind im Durchschnitt bereits 10 Jahre dort beschäftigt. So lautet das zentrale Ergebnis der „SiFo-Studie 2009/10“ des Sicherheitsforums aus Baden-Württemberg

Gefährdungen im Inneren eines Netzes ergeben sich durch

- **Missbrauch** von Zugriffsrechten
- **gezielte** Angriffe
- Bedrohung durch **Malware**

## Gefährdungen durch gezielte Angriffe

- **Sniffing:** Abhören des Datenverkehrs im Unternehmensnetzwerk
  - Ausspähen von Zugangsdaten (Benutzerkennung, Passwort)
  - Abhören von Datenströmen (VOIP)
- **Man-in-the Middle** -Angriffe
  - Manipulation und Fälschung von Datenströmen
- Sabotage durch **DoS**
  - Ausschalten von zentralen Diensten (Telefonie-Server, DHCP, ...)

*...die Durchführung solcher Angriffe erfordern kein Spezialwissen*
*...entsprechende Tools sind selbst erklärend und im Internet frei verfügbar*
***...**man braucht nur einen PC im Netz, auf dem man sie installieren kann*

# Bedrohung durch Malware

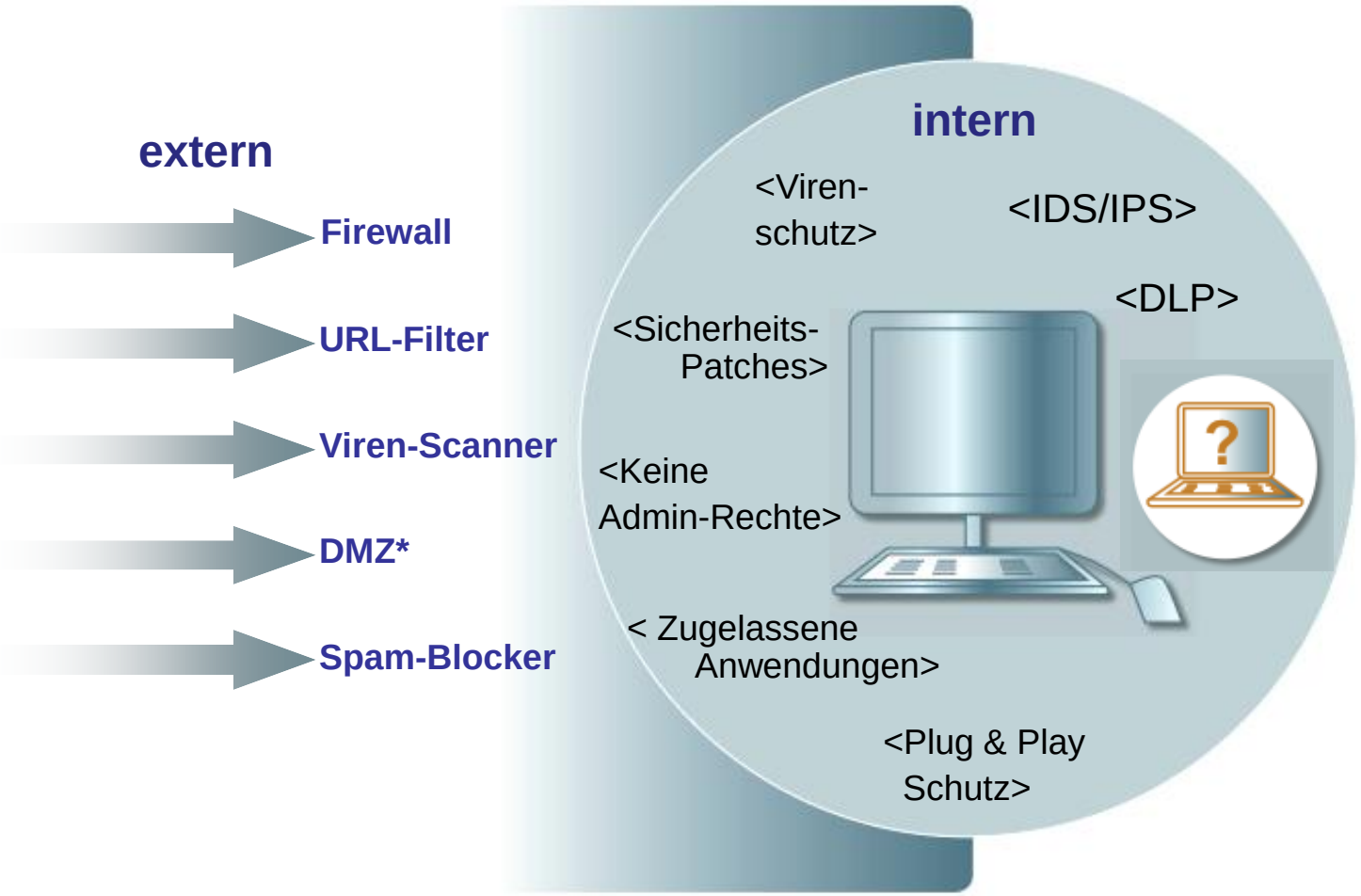
## Conficker in Kärnten: Nach der Landesregierung nun die Spitäler

Nach den Computern der Kärntner Landesregierung hat der Conficker-Wurm auch die PCs der Kärntner Krankenanstaltengesellschaft KABEG in mindestens drei Spitälern befallen.

Wie bei der Landesregierung sind auch dort **rund 3.000 Rechner** betroffen. Im Unterschied zur Landesregierung sollen die Krankenhaussysteme allerdings das einschlägige Sicherheitsupdate bereits zuvor installiert gehabt haben. Ein weiterer Unterschied ist, dass es dem Wurm gelungen sein soll, weitere Schädlinge auf die befallenen Spitals-Computer zu laden.

**Unbestätigten Informationen zufolge soll Conficker über einen Laptop in das KABEG-Netzwerk eingesickert sein.** !

# IT Sicherheits-Situation




**NAC Network Access Control:**

Schutz vor fremden und unsicheren Geräten

* Eine demilitarisierte Zone ist der Bereich des Computernetzes, in dem nur sicherheitstechnisch kontrollierte Zugriffmöglichkeiten auf Server und Dienste angeboten werden.

# NAC als Baustein für das Sicherheitsmanagement

## Was ist Network Access Control?

Im Netzwerk betriebene Geräte haben Zugriff auf LAN-Ressourcen,

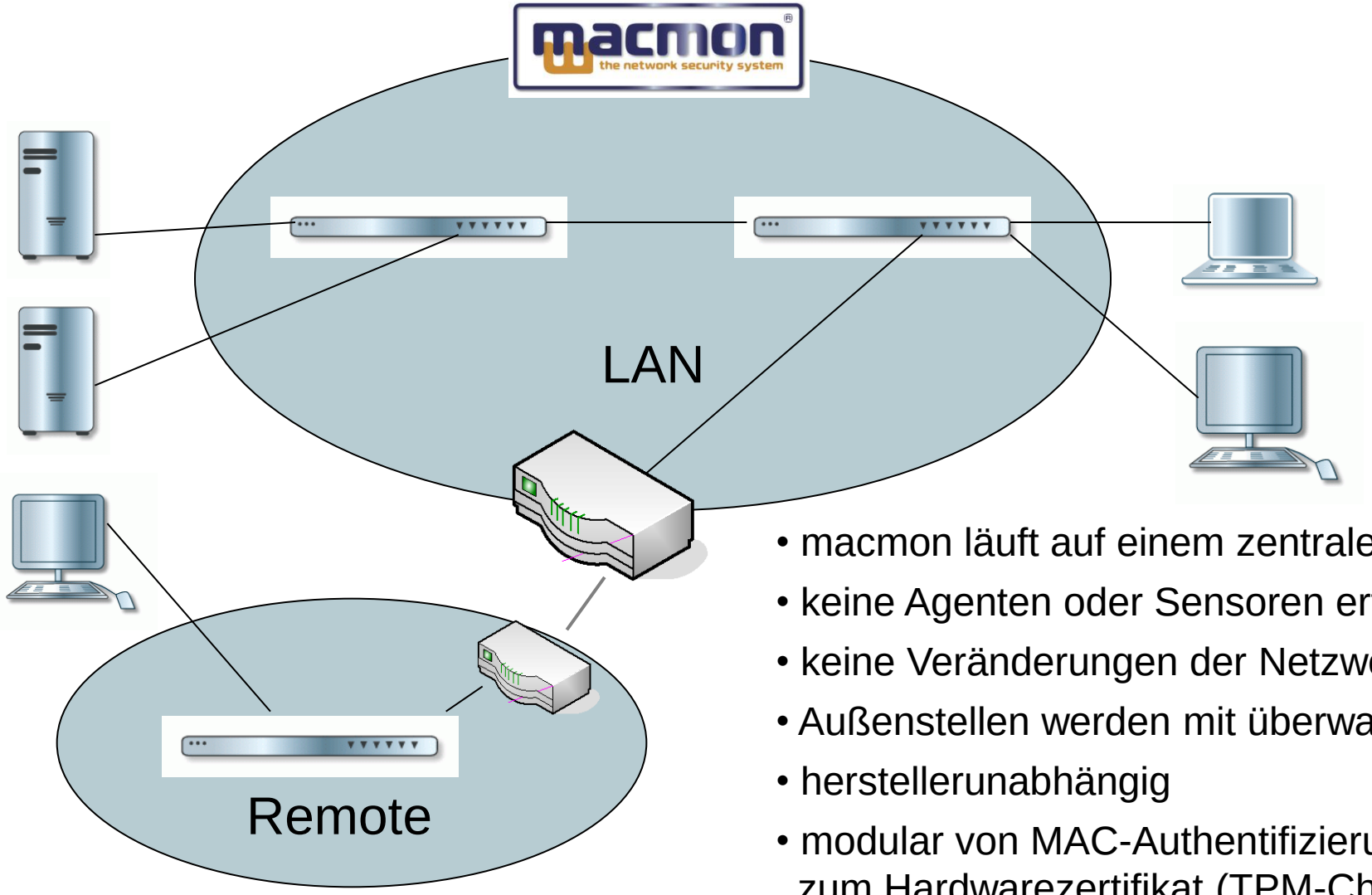
- wenn sie für diese zugelassen sind und
- wenn sie den gültigen Sicherheitsstandards genügen.

**Network Access Control ist die Umsetzung der unternehmensinternen Sicherheits-Richtlinie für alle im Netzwerk betriebenen oder zu betreibenden Geräte.**

## Security Policy LAN Access

- **Authentisierung**
  Jedes Gerät muss sich als berechtigt zu erkennen geben. Nicht berechtigte Geräte werden abgewiesen oder bekommen einen Gast-Status.
- **Compliance Check**
  Jedes Gerät muss den Sicherheitsstandards des Unternehmens genügen. Bei Nichterfüllung erfolgt eine „Quarantänisierung“ und ggf. eine automatisierte „Heilung“.
- **Autorisierung**
  Die Geräte werden klassifiziert und bekommen einen Netzwerkzugang entsprechend ihrer Authentisierung.

# Schutz vor Fremdgeräten: macmon




- macmon läuft auf einem zentralen Server
- keine Agenten oder Sensoren erforderlich
- keine Veränderungen der Netzwerkstruktur
- Außenstellen werden mit überwacht
- herstellerunabhängig
- modular von MAC-Authentifizierung bis zum Hardwarezertifikat (TPM-Chip)

# macmon Produktfamilie

## macmon vlan manager

- Dynamische VLAN-Steuerung
- Geräte Isolierung
- Automatische Netzwerk-segmentierung

## macmon advanced security

- Schutz vor IP-Adress-Manipulationen
- Schutz vor MAC-Spoofing

## macmon guest service

- Ein Voucher-System zur Steuerung des Netzwerkzugangs für Gäste
- Monitoren der Netzwerk-nutzung durch Gäste

## macmon network access control

- Schutz vor unautorisierten Geräten
- „White Listing“: nur zugelassene Geräte dürfen ins Netz
- Erkennung und Lokalisierung
- Netzwerk Monitoring und Administration

## macmon TP

- Hochsicherheitslösung zur zuverlässigen Endgeräte Identifizierung
- Fälschungssichere Authentifizierung mit dem TPM-Chip

## macmon appliance

- Die schlüsselfertige NAC-Lösung

## macmon energy

- Erkennen und beobachten von Systemen im Leerlauf
- Zeit- oder Ereignis-gesteuertes herunterfahren von Geräten im Leerlauf
- Automatisches „aufwecken“ des Arbeitsplatzrechners zum Arbeitsbeginn
- Kostenreduktion und Produktivitätssteigerung

## macmon client compliance

- Überwachung der Einhaltung der Sicherheitsvorgaben
- Isolierung von unsicheren Geräten in ein Update-Netz
- “Fingerprinting” zur Geräte-Identifizierung

# Ausgangslage

- Eine Vielzahl von Systemen wird benötigt, um Sicherheit in Unternehmensnetzwerken und Rechenzentren zu gewährleisten.
- Die Systeme sind isoliert. Jedes System erfüllt eine oder eine Reihe von spezifischen Aufgaben.

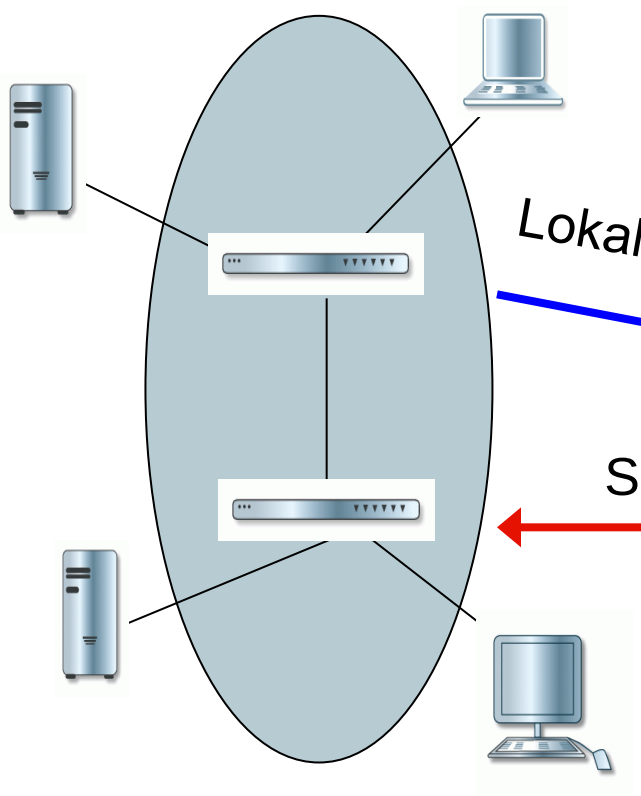
➢ Komplexe Angriffsszenarien erfordern die Zusammenarbeit der Systeme.

➢ Sicherheitssysteme sollten miteinander kommunizieren und ihre Daten konsolidieren.

# Beispiele für die Kommunikation von Sicherheitssystemen im NAC-Bereich:

# Datenkonsolidierung

Datenkonsolidierung mit dem Bestandsmanagement

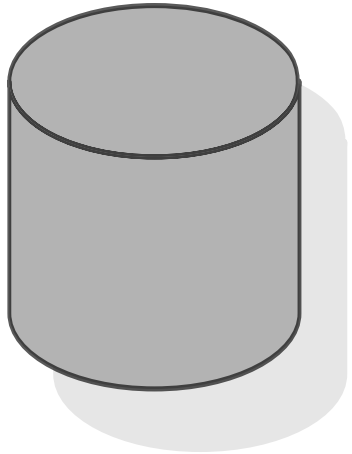


Lokalisierung

Schutz


Datenabgleich

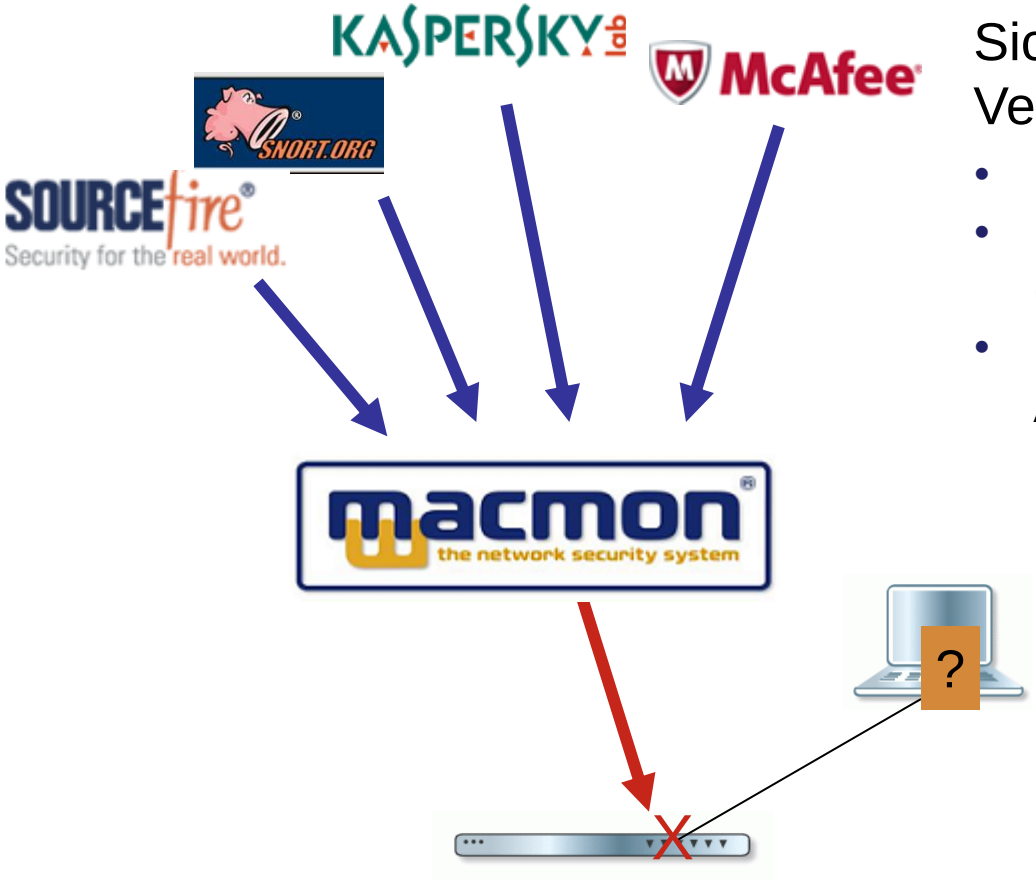
Bestandsdatenbank
Asset Management
CMDB



- Verbesserung der Datenqualität
- Automatisierung der Datenpflege

!

# macmon Active Incident Response (AIR)




Sicherheitssysteme erkennen Compliance-Verletzungen und Bedrohungen :

- Ein Virus lässt sich nicht entfernen.
- Ein bestimmter Virus taucht auf. (z. B. Conficker)
- Ein System erzeugt Datenströme mit Angriffsmustern.

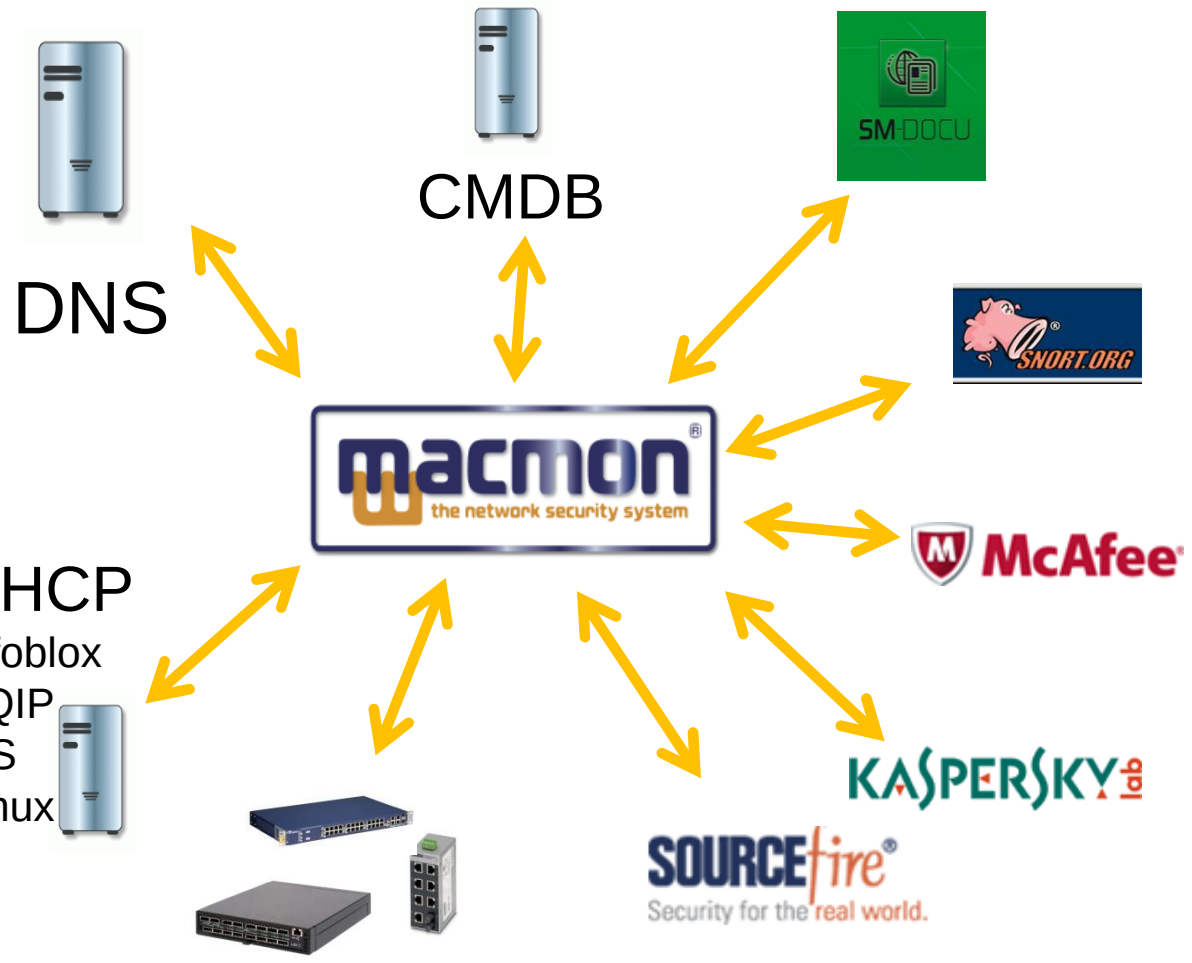
→ Sicherheitssysteme steuern macmon

→ macmon trennt das Gerät vom Netz

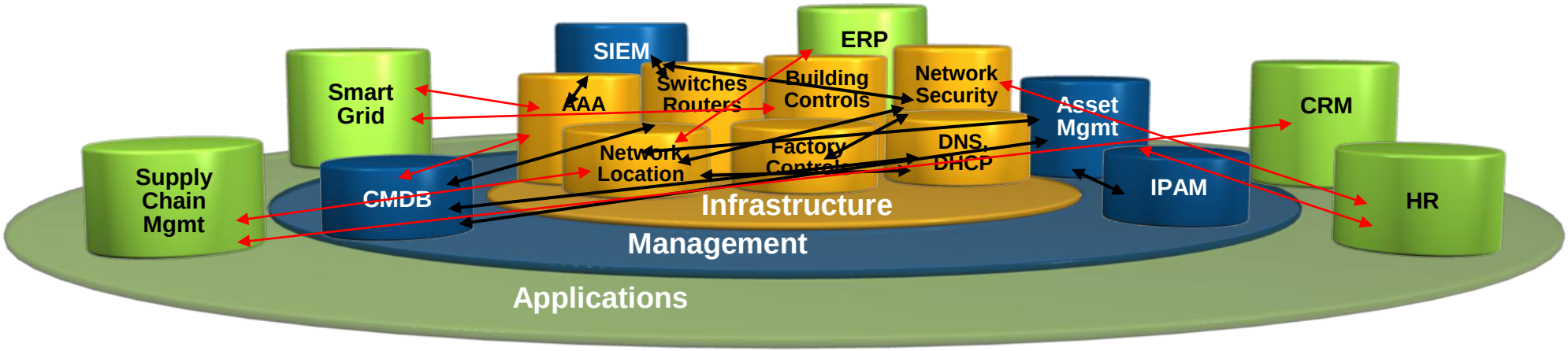
**Getestete Schnittstellen zu einer Vielzahl von Systemen verfügbar!**

# macmon Interfaces

- ***macmon kommuniziert mit einer Vielzahl von Systemen***
- ***Jede Schnittstelle muss individuell erstellt werden!***



# Datenaustausch im Unternehmen




SNMP, Syslog, Netflow

Custom Integration – API's, Scripts

- Complex
- Costly
- Brittle
- High Maintenance

# IF-MAP *Motivation*

Beschränkungen bestehender Sicherheitsverfahren:

- Isolierte Daten
- Fehlende Integration
- bestenfalls generische Schnittstellen

Herausforderung:

- Problemlose Integration vorhandener Sicherheitstools
- Erreichen einer Echtzeit Sicherheit durch Korrelation von Metadaten
- Offen für neue Technologien und Bedrohungen

# IF-MAP: Ein mächtiger neuer Standard

## IF-MAP = Interface to Metadata Access Points

- Ein offener Protokoll Standard der Trusted Computing Group
  - Unterstützt von HP, Juniper, Microsoft, McAffee, Symantec, etc.
- Enthält einen umfassenden publish/subscribe/search Mechanismus für Daten die Netzkomponenten betreffen, Status, Aktivitäten,…
- Aggregiert und assoziert automatisch Echtzeit-Informationen von vielen verschiedenen
  - Unterstützt vordefinierte Datentypen und herstellerspezifische Erweiterungen
- Ursprünglich für die Netzwerksicherheit entwickelt, bietet IF-MAP darüber hinaus eine breite Palette an Anwendungsmöglichkeiten

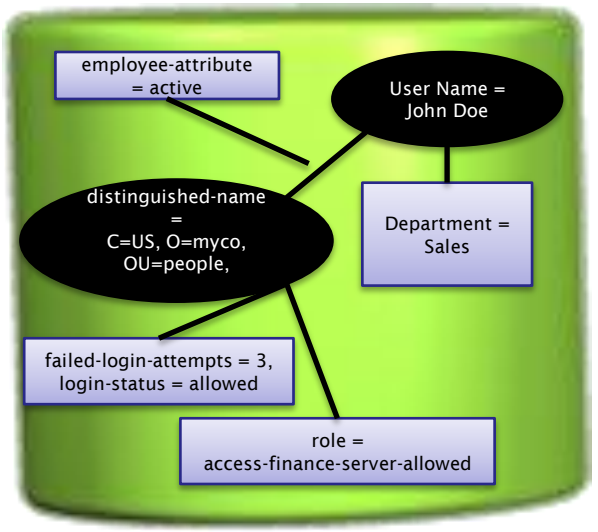
# MAP Komponenten

## MAP Client


3 MAP Operations:

*Publish*
*Subscribe*
*Search*

## MAP Server




3 MAP Objects:

*Identifiers*
*Links*
*Metadata*

# Die 3 Elemente des MAP Servers

| | |
|---|---|
| **Identifiers** | Alle Objekte werden durch eindeutige Identifier repräsentiert |
| **Links** | Mit Eigenschaften versehene Verbindung zwischen zwei Identifiern |
| **Metadata** | Attribute die Links oder Identifiers zugeordnet sein können |

- **Gängige Datentypen:**
  - Identifiers: User, IP-Adresse, MAC-Adresse, …….
  - Link: IP to MAC
  - Metadata: Status (active/inactive), Richtlinie (allowed/denied), Rolle (department/title), Aktivität (failed authentication, violated policy,..)…
    Das Metadaten-Design ist auf Erweiterbarkeit ausgelegt.

# Die 3 MAP-Client Operationen

- Publish:
  - Clients veröffentlichen Metadaten im MAP-Server
    - Beispiel: Anmeldeserver meldet, dass sich ein User angemeldet hat.

Informiere andere über…<metadata…>

- Search:
  - Clients durchsucht die veröffentlichten Metadaten associated with a particular identifier and linked identifiers
    - Beispiel: Eine Anwendung erfragt den aktuellen Standort eines Clients

Informiere mich ob…*match*(metadata Muster)

- Subscribe:
  - Asynchronen Suchanfragen: Clients erhalten Ergebnisse zu Anfragen, die erfüllt sind, sobald bestimmte Metadaten veröffentlicht wurden.
    - Beispiel: Melde mir, wenn bei einem „User“ ein Statuswechsel von “angestellt” nach “gekündigt” stattfindet

Informiere mich sobald…*match*(metadata Muster)

# IF-MAP Entwicklung

- April 2008:

  MAP 1.0 Spezifikation wird von der TCG veröffentlicht.

- April 2010:

  MAP 2.0 Spezifikation wird veröffentlicht

- In Vorbereitung:

  Veröffentlichung als IETF-Standard (RFC)

# IF-MAP Produkte

## IF-MAP Server

- Infoblox Orchestration Server
- Juniper UAC

*Open Source*

- Irond (FHH)

## IF-MAP Clients

- Infoblox NIOS
- Juniper
- Trapeze
- Hirsch
- Beacon
- Lumeta

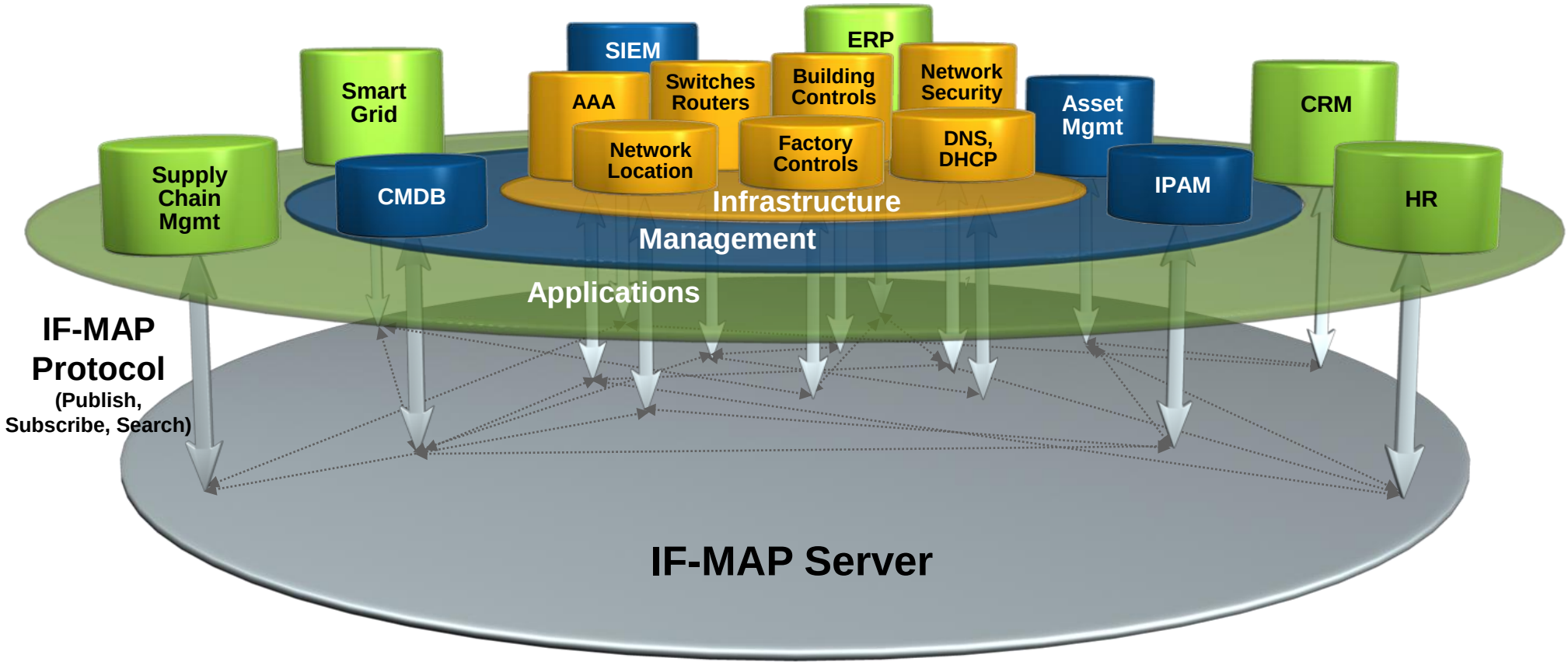
## IF-MAP Client Projekte

- macmon
- NCP
- Enterasys

*Open Source:*

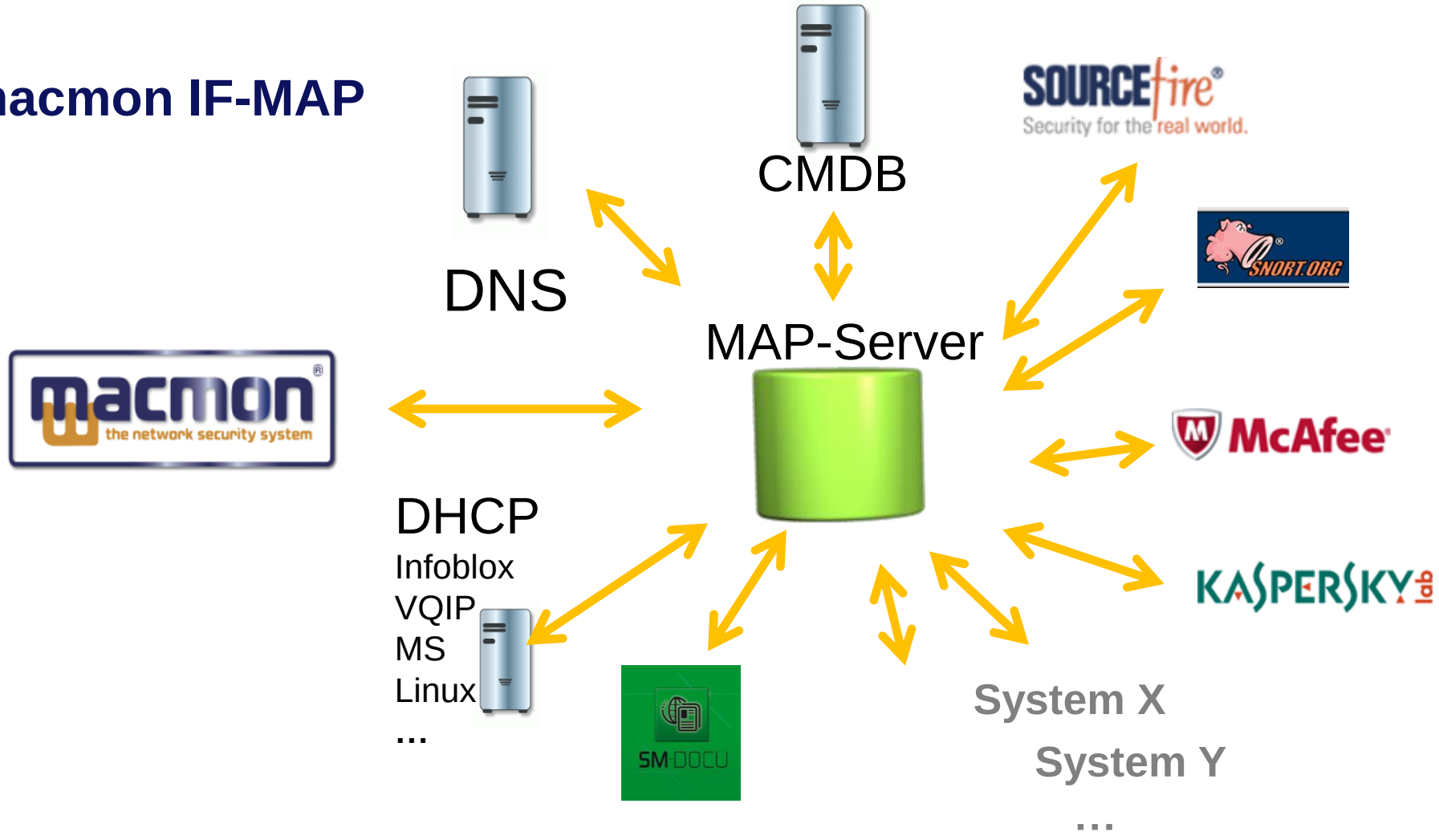
- Android
- IP-Tables
- Snort

# IF-MAP im Unternehmen




Automatically aggregates, correlates, and distributes data
to and from different systems, in real time

## macmon IF-MAP



# Forschungsprojekt ESUKoM

„**E**chtzeit **S**icherheit für **U**nternehmensnetze durch **Ko**nsolidierung von **M**etadaten“

- Verbundprojekt von drei IT-Unternehmen und zwei Wissenschaftseinrichtungen
- Projektziele:
  - Integration von Sicherheitstools
  - Konsolidierung von Metadaten
  - sichere Smartphone Anbindung
  - IF-MAP Prototypen Infrastruktur

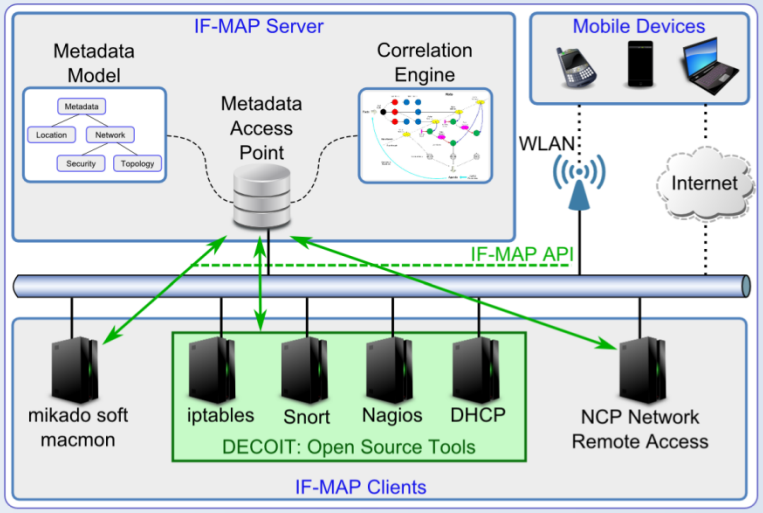
- Gefördert vom Bundesministerium für Forschung und Entwicklung

# ESUKoM Key Features

Anomaly Detection

Identity Awareness

Smartphone Awareness




Location-based Services

Single Sign-Off

Mal-App Detection

Secure Evidence

Real-time Enforcement

# IF-MAP Zusammenfassung

- Junges Protokoll mit einer guten Unterstützung im Markt
- IF-MAP bietet eine offene Architektur für den Aufbau einer **wirkungsvollen** und **herstellerübergreifenden** Verteidigung in der Tiefe.
- IF-MAP bietet als offene und „intelligente“ Schnittstelle vielfältige Einsatzmöglichkeiten
  - Logistik
  - IT-Organisation
- IF-MAP Unterstützer:
  Aruba, Avaya, Extreme, Enterasys, HP, Huawei, IBM, Infoblox, Intel, Juniper, Microsoft, Motorola, Symantec, Wave, and the NSA

## Informationen zu IF-MAP

- www.trustedcomputinggroup.org
- www.esukom.de
- www.if-map.com
- www.ifmapdev.com
- www.if-map.de

# Vielen Dank für Ihre Aufmerksamkeit.

**Nächste Vortragstermine:**

**Freitag, 04.03., 10 Uhr**

„Der neue NAC-Standard IF-MAP: Erhöhung der Sicherheit in Unternehmensnetzen durch Datenkonsolidierung“

**Freitag, 04.03., 12:30 Uhr**

„Die Zukunft der NAC-Lösungen: Nutzung der TPM-Chip-Technologie zur fälschungssicheren Authentifizierung von Endgeräten im Netzwerk“

# Live-Präsentation


**Halle 11, Stand D16**

„Security Plaza“

# Kontakt

**mikado soft gmbh**
Bülowstraße 66
10783 Berlin

Fon 030. 217 90 0
Fax 030. 217 90 200

info@mikado.de
www.mikadosoft.de