

### Ihre Lösung für...

#### ...ein umfassendes Monitoring des Behörden-Netzwerkes

> macmon überwacht und kontrolliert alle im Netz befindlichen Geräte (Live-Bestandsmanagement) und dokumentiert alle Zugriffe auf das Verwaltungsnetz, auch bei weitgefächerten Organisationsstrukturen

#### ...den Schutz sensibler personenbezogener Daten

> macmon sorgt dafür, dass sich nur autorisierte, authentifizierte und sicher konfigurierte Systeme im Netz befinden und schützt die Verwaltungs-IT vor Angriffen auf Sozialdaten und vor Datenmanipulation und -spionage

#### ...die Abwehr von Netzwerk-Angriffen

> macmon erkennt, meldet und unterbindet den Einsatz nicht autorisierter Geräte im Behörden-Netzwerk

#### ...eine differenzierte Zugangskontrolle auf ausgewählte Netzwerkbereiche/VLANs

#### ...die Sicherstellung der IT-Compliance

> macmon unterstützt die Umsetzung der BSI-Standards zum IT-Grundschutz-Katalog, der Anforderungen der LDSG und des BDSG und die Erfüllung der Auflagen des Basler Abkommens Basel II

#### ...die Umsetzung der Green-IT-Initiative des Bundes durch Einsparung von Energiekosten am PC-Arbeitsplatz



Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT), Bonn

**„Der Einsatz ist ein bedeutender Schritt in Richtung mehr Sicherheit. Wir sind mit dem Produkt sehr zufrieden.“**

## Netzwerksicherheit als wesentlicher Bestandteil der Informationssicherheit

### Anforderung: Grundschutz nach BSI

Die IT-Grundschutz-Kataloge des BSI stellen in der Öffentlichen Verwaltung den Standard für die Informationssicherheit und den Aufbau eines funktionierenden IT-Sicherheitsmanagements dar. Für die Bundesbehörden ist es mittlerweile verbindlich einen Grundschutz nach diesem Standard zu etablieren.

In seinen Maßnahmenkatalogen werden vom BSI zum Thema Netzwerksicherheit eine Vielzahl von Empfehlungen ausgesprochen, so z. B. in der Maßnahme M 2.216: „die Installation und Benutzung nicht freigegebener IT-Komponenten muss verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“ Das Einbringen von nicht autorisierten und unsicheren Geräten ins Netz ist demnach konsequent zu unterbinden.

Die von der mikado soft entwickelte Network Access Control Lösung macmon gewährleistet die Einhaltung dieser Sicherheitsregularien. macmon erkennt, meldet und unterbindet den Betrieb von Fremdsystemen im behördeneigenen Netzwerk und verhindert den Einsatz von nicht autorisierten Geräten.

macmon bietet als herstellerunabhängige Sicherheitslösung auch eine verlässliche Überwachung von Netzen mit unterschiedlichsten Netzwerkkomponenten. Da sich in der Öffentlichen Verwaltung durch Änderungen des Verwaltungszuschnitts, oder durch Ausschreibungen auch ungewollt heterogene IT-Infrastrukturumgebungen entstehen, ist die Herstellerunabhängigkeit von Sicherheitssystemen ein wichtiges Entscheidungskriterium.

### Lückenloser Datenschutz

Der Umgang mit sensiblen, personenbezogenen Daten ist in vielen Behörden, insbesondere im kommunalen Bereich Standard. Für einige der hier praktizierten Verfahren, wie z. B. ELENA existieren zum Teil erhebliche datenschutzrechtliche Bedenken der entsprechenden Datenschutzbeauftragten der Länder. Umso wichtiger ist es die vom Gesetzgeber geforderten Sicherheitsanforderungen peinlichst zu erfüllen. In den maßgeblichen Regularien, den Datenschutzgesetzen des Bundes (BDSG) und der Länder (LDSG), werden eine sichere IT und insbesondere eine verlässliche Zugangskontrolle zum Netzwerk gefordert.

So wird im BDSG in der Anlage zu § 9 Satz 1 hierzu ausgeführt: „Es sind Maßnahmen zu treffen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle).“

macmon sorgt dafür, dass sich nur autorisierte, authentifizierte und sicher konfigurierte Systeme im Netz befinden. Somit hilft macmon den Anforderungen des Gesetzgebers zu genügen und sensible Daten und personenbezogene Informationen abzusichern und zu schützen.



## Vorteile im Überblick

- > Einfache Installation und Inbetriebnahme, geringer administrativer Aufwand, leichte Integrier- und Skalierbarkeit
- > Herstellerunabhängigkeit in Bezug auf IT Infrastrukturkomponenten und Endgeräte
- > Modular erweiterbar, je nach Sicherheitsanforderungen - von der Authentifizierung über MAC-Adressen, über eine Zertifikate-basierte Lösung nach IEEE 802.1X bis hin zur Umsetzung der Sicherheitskonzepte der Trusted Computing Group
- > Unterstützung von Standards wie 802.1X, SNMP, IF-MAP
- > Lokalisierung und Überwachung nicht 802.1X-fähiger Geräte wie Drucker, Thin Clients, IP-Telefone/ Smartphones
- > Schnittstellen zu anderen Sicherheitssystemen (AntiVirus-Systeme wie McAfee, Kaspersky oder IDS/IPS)
- > Steuerung des Netzwerkzugangs für Gäste und Mobile Devices (WLAN-Support)
- > Ausfallsicherheit: beim Ausfall des Autorisierungssystems – z. B. des Radius-Servers - werden andere Anwendungen nicht beeinträchtigt
- > Ausblick: BSI-zertifizierte Netzwerkzugangsschutz-Lösung: geprüfte Sicherheitsleistungen nach Common Criteria (Q2 2011)
- > Reduzierung des administrativen Aufwands, nachweisbarer ROI

## Green IT-Betrag

Die Bundesverwaltung hat sich zum Ziel gesetzt bis 2013 den Energieverbrauch der Informationstechnik um 40 Prozent zu reduzieren. Die einzelnen Behörden sind daher aufgefordert, bei der Beschaffung und Nutzung von ITK-Technologie Ressourceneffizienzaspekte zu berücksichtigen.

Mit der Monitoring-Funktion von macmon können Sie Leerverluste, die sich durch nachts und am Wochenende laufende Geräte ergeben visualisieren und mit macmon energy können mit wenig Aufwand Energiekosten (bis zu 97 € pro PC-Arbeitsplatz im Jahr) eingespart werden. macmon energy ermittelt den Energieverbrauch, steuert individuelle Energieprofile und schaltet die PC-Arbeitsplätze systemgesteuert aus und auch wieder ein.

## Geprüfte Sicherheit nach Common Criteria

Im Rahmen ihrer Cyber-Sicherheitsstrategie (02/2011) wird die Bundesregierung Maßnahmen in verschiedenen strategischen Bereichen ergreifen. Hierzu gehört den Einsatz von IT-Komponenten zu fördern und zu fordern, die sich „einer Zertifizierung nach einem international anerkannten Zertifizierungsstandard unterzogen haben“.

macmon befindet sich aktuell im BSI-Zertifizierungsverfahren über geprüfte Sicherheitsleistungen nach dem internationalen Standard Common Criteria (CC).

Die Zertifizierung eines IT-Sicherheitsprodukts nach diesem Standard belegt, dass bereits bei der Entwicklung Kriterien für sichere und vertrauenswürdige Systeme eingehalten wurden und dass eine objektive Bewertung des Produktes von einer neutralen und kompetenten Instanz durchgeführt wurde.

**Fazit:** macmon bietet Öffentliche Verwaltungen und Behörden einen vertrauenswürdigen, zuverlässigen, abgestuften und herstellerunabhängigen Netzwerkzugangsschutz - von der Authentifizierung über MAC-Adressen, über eine Zertifikate-basierte Lösung nach IEEE 802.1X und darüber hinaus bis hin zur Umsetzung der Sicherheitskonzepte der Trusted Computing Group.

macmon vertrauen bereits:



Landratsamt  
Sigmaringen



Landesamt für Gesundheit und  
Soziales

