



Ihre Lösung für...

- ...ein umfassendes Monitoring des Banken-Netzwerkes
- ...den Schutz sensibler Daten
- ...die Abwehr von Netzwerk-Angriffen
- ...eine differenzierte Zugangskontrolle auf ausgewählte Netzwerkbereiche/VLANs/WLANs
- ...die Sicherstellung der Banken-IT-Compliance
- ...die Umsetzung der Green-IT-Initiative des Bundes durch Einsparung von Energiekosten am PC-Arbeitsplatz

macmon vertrauen u.a.:



Netzwerksicherheit als wesentlicher Bestandteil der Banken-IT

Höchste Sicherheitsanforderungen im Bankenumfeld

Banken und Sparkassen gehören zu den Branchen mit den höchsten Anforderungen an die Informationssicherheit. Dies hängt zum einen daran, dass nahezu alle Geschäftsprozesse IT-gestützt sind und es darum eine große Abhängigkeit von der Verfügbarkeit der immer komplexer werdenden Systeme gibt. Zum anderen steigen die Bedrohungen durch die Cyber-Kriminalität erheblich. Diese wachsende Verwundbarkeit und Gefahr wirtschaftlicher Schäden in Folge von IT-Risiken erhöhen den Handlungsdruck für ein aktives IT-Sicherheitsmanagement in Banken und Sparkassen.

Einhaltung gesetzlicher Vorgaben und Bestimmungen

Inzwischen berücksichtigt der Gesetzgeber die ansteigenden Bedrohungen im Bereich der Informationstechnologie und es gibt eine Reihe von Regularien und gesetzlichen Auflagen zur Risikominimierung. So werden in Deutschland Banken, Versicherungen, Finanzdienstleister und Börsen den *Kritischen Infrastrukturen (KRITIS)* zugeordnet. Die Bundesregierung sieht "den Schutz Kritischer Infrastrukturen von Bundesregierung und Wirtschaft als wichtige nationale Aufgabe an, weil die Innere Sicherheit immer stärker von der IT-Sicherheit beeinflusst wird."

Die von der Bundesanstalt für Finanzdienstleistungsaufsicht (**BaFin**) herausgegebenen Mindestanforderungen an das Risikomanagement (**MaRisk**) fordern „für die IT-Systeme und die zugehörigen IT-Prozesse die Sicherstellung der Integrität, der Verfügbarkeit, der Authentizität sowie der Vertraulichkeit der Daten.“ Es wird empfohlen, bei der Ausgestaltung der Sicherheit der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards wie die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnologie (**BSI**) oder die entsprechende **ISO-Norm 17799** zu setzen. In diesen Standards findet sich eine Vielzahl von Empfehlungen zur Netzwerksicherheit. So muss „die Installation und Benutzung nicht freigegebener IT-Komponenten verboten und die Einhaltung dieses Verbotes regelmäßig kontrolliert werden.“ (**BSI M 2.216**). Das Einbringen von nicht autorisierten und unsicheren Geräten ins Netz ist 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 Netzwerk und verhindert den Einsatz von nicht autorisierten Geräten. macmon bietet eine flexible Lösung, die zum einen den Standard 802.1X unterstützt, zum anderen aber auch dazu in der Lage ist, für Spezial-Geräte, wie z. B. Geldautomaten, eine verlässliche Geräteerkennung durchzuführen.

Bankgeheimnis: Lückenloser Datenschutz

Der Datenschutz und der verantwortungsvolle Umgang mit vertraulichen Daten hat im Umfeld von Banken und Sparkassen eine besonders hohe Bedeutung. Die Kunden



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 Zertifikatebasierte Lösung nach IEEE 802.1X bis hin zur Umsetzung der Sicherheitskonzepte der Trusted Computing Group
- > Unterstützung von Standards wie 802.1X, SNMP, IP-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)

setzen voraus, dass das Bankgeheimnis und der Schutz persönlicher Daten stets gewahrt werden. Die unerwünschte Offenbarung vertraulicher Kunden- und Konten-Daten stellt somit ein erhebliches Risiko dar. Die rechtlichen Folgen reichen bis zur persönlichen Haftung der Vorstände, welche nach §§91 Abs.2 AktG geregelt ist. Viel schwerer als der wirtschaftliche oder strafrechtliche Schaden wiegt jedoch oft der damit verbundene Imageschaden. Dies zeigen in besonderem Maße die in den vergangenen Jahren bekanntgewordenen Fälle von Datenraub bei Liechtensteiner und Schweizer Banken.

Ein wichtiger Baustein für den Schutz der Daten ist die Netzwerk-Zugangskontrolle. macmon sorgt dafür, dass sich nur autorisierte, authentifizierte und sicher konfigurierte Systeme im Netz befinden. Somit hilft macmon, ein Eindringen in die Informationssysteme zu verhindern und sensible Daten und personenbezogene Informationen abzusichern und vor unberechtigten Zugriffen zu schützen.

Intelligenter Green IT-Betrag mit hohem Einsparpotenzial

„IT birgt enormes „grünes“ Potenzial.“ Mit optimierter IT sind Energiekosten-Einsparungen von 75% für Arbeitsplätze und Serverraum möglich, so die gemeinsame Studie der Deutschen Bank Research und des BITKOM green it Beratungsbüros vom November 2010.

Mit der Monitoring-Funktion von macmon können Sie Leerverluste, die sich durch nachts und am Wochenende laufende Geräte ergeben, visualisieren. Die macmon-Komponente **macmon energy** erlaubt mit wenig Aufwand eine signifikante Reduzierung des Energieverbrauchs von PC-Arbeitsplätzen. Hierfür wurde das Produkt 2010 mit dem Innovationspreis IT der „initiative mittelstand“ in der Kategorie „Green-IT“ ausgezeichnet. macmon energy ermittelt den Energieverbrauch, steuert individuelle Energieprofile und schaltet ungenutzte PC-Arbeitsplätze systemgesteuert aus. Aufgrund der integrierten „Start-up“-Funktion ist der Arbeitsplatz für den Nutzer bei Arbeitsbeginn sofort betriebsbereit. Dies führt zu einer besseren Arbeitszeitauslastung und erhöhter Produktivität.

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 Banken und Sparkassen einen vertrauenswürdigen, zuverlässigen, abgestuften und herstellerunabhängigen Netzwerkzugangsschutz - von der Authentifizierung über MAC-Adressen, über eine Zertifikatebasierte Lösung nach IEEE 802.1X bis hin zu einer fälschungssicheren Authentifizierung unter Nutzung des TPM-Chips.