ANWENDERBERICHT
ISAS

macmon
nac intelligent einfach

Das ISAS sorgt vor:
macmon für nachhaltigen Schutz der Forschungs- und Verwaltungsdaten

Mit dem Einsatz von macmon schützt das Leibniz-Institut für Analytische Wissenschaften (ISAS) nicht nur heute zuverlässig seine kritischen Daten, sondern ist auch für die künftigen Sicherheitsanforderungen bestens gerüstet.

Das Leibniz-Institut für Analytische Wissenschaften e.V. (ISAS) ist ein unabhängiges Forschungsinstitut für physikalisch-chemische Analytik mit Schwerpunkten in der Bioanalytik, Materialanalytik und Spektroskopie. Am ISAS sind ständig zwischen 170 und 200 Mitarbeiter an insgesamt drei Standorten in Dortmund (zwei) und Berlin (einer) tätig. Es sind 500 Arbeitsplatz- bzw. Laborrechner, 1.100 Ports, 90 Server, 60 Switches, 30 Drucker und 80 netzwerkfähige Messgeräte im Einsatz.

Leibniz-Institut für Analytische Wissenschaften (ISAS), Standort Dortmund, Campus der TU

Ein VLAN-Management für verschiedene Standorte

Institutsnetze bergen wegen der Heterogenität ihrer Systeme und der verteilten Verantwortlichkeiten ein besonders hohes Risiko für das Ausspähen schutzbedürftiger Forschungs- und Verwaltungsdaten. Der Schutz dieser Daten in den verschiedenen Netzwerken an unterschiedlichen Standorten mit vereinheitlichten Regeln gehört zu den wichtigsten Anforderungen an die IT-Sicherheit im ISAS. Der Wunsch nach einem sicheren und geschützten Zugriff auf die spezifischen Netzwerk-Ressourcen der verschiedenen Bereiche und Forschungsprojekte von den verschiedenen Standorten aus, waren der Anlass für die Beschaffung einer NAC-Lösung, die ein einfaches VLAN-Management und einen sicheren Netzwerkzugriffsschutz anbietet. Kollegen anderer Institutsstandorte, die uns besuchen, sollten sofort auf ihre Ressourcen zugreifen können. Unser Wunsch war hier eine dynamische VLAN Schaltung anhand vordefinierter Geräteparameter. Unabhängig vom Standort muss ein korrektes Abfahren von Zuweisungsreaktionen erfolgen, so Jens Hinrichs, Leiter IT-Service am ISAS.

Die IT-Security-Software macmon der macmon secure GmbH (zuvor mikado soft) ermöglicht die Einführung und Bereitstellung solcher Sicherheitsstrukturen und eine flexible Zugangskontrolle zu Netzwerkressourcen. Darüber hinaus können Besucher- und Quarantänenetzwerke für die Zuweisung nicht vertrauenswürdiger Geräte bereitgestellt werden. Statische und dynamische VLANs können leicht implementiert und betrieben werden.

Durchsetzung von Sicherheitsrichtlinien für alle Geräte

„Mit macmon haben wir eine herstellerunabhängige Geräteunterstützung auf Switch- und Endgeräteseite und die Möglichkeit, auch Geräte, auf denen sich keine NAC-Client-Software installieren lässt, wie z.B. Massenspektrometer, digitale Analysegeräte oder Oszilloskope, mit einzubeziehen. Zuvor hatten wir eine Client-basierte NAC-Lösung im Einsatz. Da wir viele Geräte verwenden, wo kein Client installiert werden konnte, mussten diese mit Mehraufwand als Ausnahmen verwaltet werden. Bisher erforderte das händische Sperren von Ports bei Zugriffen sicherheitskritischer Geräte einen hohen Zeitaufwand.
Mit macmon können wir nun Sicherheitsrichtlinien auf jedem Gerät im Netzwerk ohne großen administrativen Aufwand durchsetzen und unser gesamtes Netzwerk von der macmon-Appliance kontrollieren lassen."

„macmon unterstützt uns bei der Optimierung unseres Netzwerkes und hilft uns, den gesteigerten Sicherheitsanforderungen durch ein transparentes und leicht zu administrierendes System auch in Zukunft gerecht zu werden."

Jens Hinrichs, Leiter IT-Service,
Leibniz-Institut für Analytische Wissenschaft

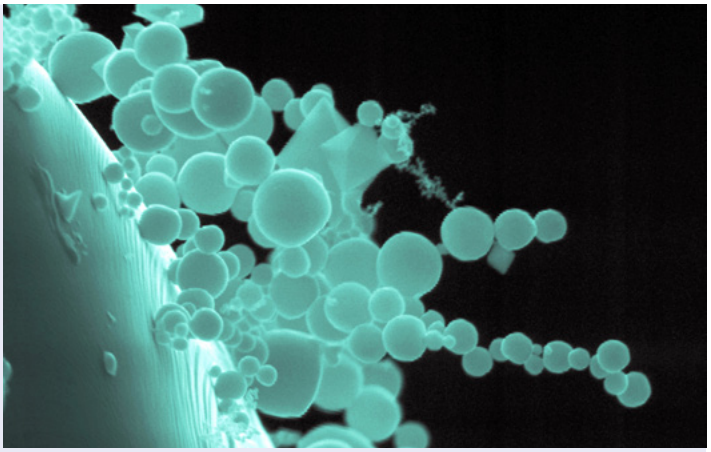
Stand: 09/2011

Modulares Konzept für sukzessiven Ausbau des Sicherheitslevels bis hin zum Gästemanagement für Mobile Devices

macmon bietet dem ISAS durch das modulare Konzept die Möglichkeit, hinsichtlich der künftig weiterhin wachsenden Anforderungen an IT-Sicherheit und Datenschutz, die Sicherheit in einzelnen Netzwerken bei Bedarf noch zu steigern. So soll in 2012 ein WLAN-Management für einen wirkungsvollen Zugangsschutz zum institutsinternen WLAN für mobile Endgeräte auch von Gästen umgesetzt werden. Es soll eine einheitliche WLAN-Policy für alle Standorte mit Hilfe von macmon umgesetzt werden. „Wir haben am Institut außerdem auch viele Studenten. Hier reicht ein WLAN-Zugriff mit einem einheitlichen Passwort nicht aus.
Darum sind wir von der temporären Ticket-Lösung und Gästeverwaltung mit macmon so begeistert ", so Hinrichs. Der macmon guest service bietet dafür alle Voraussetzungen: das Management- und Reporting-System gewährleistet auch für Besucher mit Geräten wie Smartphones, Netbooks oder iPads einen kontrollierten und zeitlich steuerbaren Netzwerkzugang.

Teil der Gerätelandschaft im Leibniz-Institut für Analytische Wissenschaften Dortmund: Massenspektrometer und digitale Analysegeräte

Dies ist besonders wichtig für die mit spezifischen Sicherheitsrisiken behafteten Mobile Devices. Die Netzwerkzugriffsrechte werden über ein Vouchersystem gesteuert. Hier kann der Admin definieren, auf welche Netze und innerhalb welchen Zeitraumes der Gast Zugang erhält. Die macmon 802.1X-Option bietet darüber hinaus eine 802.1X-Authentifizierung – wahlweise über Zertifikate oder über eine Anmeldung – die besonders für den WLAN-Bereich zu empfehlen ist, da hier MAC-Adressen keinen ausreichenden Schutz bieten. Darüber hinaus war auch die kommende BSI-Zertifizierung von macmon



Beim ISAS im Einsatz: Elektronenmikroskope (Aufnahme Glühwendel Überreste, Quelle: Dr. Alex von Bohlen und Maria Becker, ISAS)

ein Faktor, der das ISAS bei der Entscheidung für macmon beeinflusst hat. Jens Hinrichs stellte fest: „Mit macmon haben wir künftig eine nach führendem internationalem Standard überprüfte Komponente im Einsatz, deren Sicherheit wir nicht mehr selber evaluieren müssen.
Auch unser Datenschutzbeauftragter begrüßte den Einsatz von macmon, da uns dieses Tool schon jetzt im Rahmen der Umsetzung des BSI-Grundschutzes mit einer einheitlichen Dokumentation der IT-Gerätelandschaft, wie vom BSI in der Maßnahme M 2.10 gefordert, unterstützt und ein Einbringen nicht autorisierter und unsicherer Geräte ins Netz konsequent unterbunden wird (Maßnahme M 2.216)."

Einfache Implementierung und hervorragende Usability

„Die Implementierung nach vorangegangener Testphase dauerte gerade mal 2 Tage und war denkbar einfach. Wir ließen macmon zunächst alle eingesetzten Netzwerkgeräte erkennen. Danach konnten wir, ohne große Benutzereinschränkung, das System in Produktion nehmen. Überzeugend war hier die überaus hohe Benutzerfreundlichkeit von macmon: die Lösung ist so selbsterklärend, dass Anwender auch ohne Schulung sofort mit der Software arbeiten können. Die Akzeptanz der neuen NAC-Lösung bei den Kollegen ist groß, die Mitarbeiter können mit ihren Geräten nun auch standortübergreifend umziehen und landen automatisch in ihrem richtigen VLAN, ohne dass die IT hier groß eingreifen muss."

Kontakt macmon secure GmbH | Alte Jakobstraße 79-80 | 10179 Berlin | Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Stand: 09/2011