MACMON COMPLIANCE

Automatisierte Durchsetzung der zentralen Unternehmens- und IT-Sicherheitsrichtlinien

Neben der Netzwerkzugangskontrolle wird auch die detaillierte Überprüfung der zugelassenen Systeme auf Einhaltung der Sicherheitsrichtlinien immer wichtiger. In vielen Situationen reichen schon „kleine Sicherheitsverstöße", um leicht erreichbare Angriffsflächen zu bieten. Eine permanente Überprüfung des „Compliance-Status" und die automatisierte Durchsetzung der Vorgaben, ist damit unumgänglich. Als Spezialist für Netzwerkzugangskontrolle hat macmon secure diese Anforderung erkannt und bietet mit der macmon compliance als erster Hersteller die Option an, mehrere, verknüpfbare Komponenten zu nutzen, um die Unternehmensrichtlinien effektiv durchzusetzen.

Nutzung beliebiger, herstellerunabhängiger Quellen zur Ermittlung des Compliance -Status

Entscheidend ist dabei, dass 99% der Unternehmen bereits Systeme im Einsatz haben, die in der Lage sind, den Compliance-Status der Endgeräte zu ermitteln und die Administratoren über Abweichungen zu informieren. Fast alle haben jedoch gemein, dass die effektive Durchsetzung der Richtlinien in der Regel von Hand oder zumindest reaktiv erfolgen muss.

Key facts

- ✓ Flächendeckende Abbildung der Compliance-Zustände durch beliebige, herstellerunabhängige Datenlieferanten und wahlweise den macmon-Agenten
- ✓ Proaktive Reaktion auf Infektionsquellen
- ✓ Schnelle und automatisierte Isolation von unsicheren Systemen im Netzwerk
- ✓ Einfaches und schnelles Implementieren, da keine Veränderung der Infrastruktur erforderlich ist
- ✓ Sofortige Erhöhung des ROI durch das Nutzen aller bereits vorhandenen Systeme und Investitionen

Genau hier bietet die Network Access Control Lösung macmon die entscheidende Unterstützung: Das Add-On Modul macmon Compliance beinhaltet vier verschiedene Komponenten:

Je nach Anforderung kann der Compliance-Status von externen Quellen empfangen, durch die Anbindung fremder Datenbanken aktiv eingeholt oder aktiv durch den macmon-Agenten ermittelt werden. Zusätzlich kann macmon Meldungen aus der Nutzung der integrierten IF-MAP Technologie verwenden.

Die Schlüsselfunktion übernimmt dabei die offene Schnittstelle von macmon, die beliebige, herstellerunabhängige Quellen verwenden kann, um macmon den Compliance-Status eines Endgerätes zu übermitteln. Auch das Anbinden mehrerer unterschiedlicher Quellen auf einmal ist ohne Weiteres möglich.

Innerhalb der macmon-GUI wird zu jedem Endgerät der Compliance-Status angezeigt. Wird dieser durch ein anderes System, wie beispielsweise Endpoint Security, Intrusion Prevention, Security Incident and Event Management, Patch Management oder Schwachstellen-Management verändert, so wird die Änderung, einschließlich der Angabe der Quelle und des Grundes, ebenfalls angezeigt.

Das flexible macmon-Regelwerk erlaubt dann, auf gewohnt einfache Weise, eine Konfiguration der Reaktion auf die Status-Änderung. Endgeräte, die nicht mehr compliant sind, werden dann beispielsweise automatisch in Quarantäne und nach erfolgter Heilung und entsprechend erneuter Status-Veränderung wieder in ihren ursprünglichen Netzwerkbereich verschoben.

Die Kombinationsmöglichkeiten sind dabei frei von Einschränkungen und erlauben Ihnen, macmon als zentrale Macht im Netzwerk zu nutzen. Gerade die völlige Herstellerunabhängigkeit sorgt an dieser Stelle dafür, dass von Ihnen bereits getätigte Investitionen nochmal an Wert gewinnen. Vorhandene Systeme mit der Funktion der Richtlinienüberprüfung erhalten durch macmon eine automatisiert ausführende Instanz.

Ein entscheidender Vorteil der Kombination verschiedener Lösungen ist dabei, dass die Zuständigkeiten der einzelnen IT-Bereiche nicht verändert werden. Wie und wann auf einen Richtlinienverstoß reagiert wird, entscheidet der Administrator des jeweiligen Systems. Die Netzwerkabteilung bietet mit macmon einen Automatismus zur Erfüllung von Isolationsaufgaben an. Sie muss in keiner Weise selber eingreifen, da die Isolierung und das Zurückführen automatisiert durch das Regelwerk erfolgen.

Mehrwert zu gängigen Antivirus-Systemen: Automatische Isolation infizierter Endgeräte

Die zweite Komponente der macmon Compliance besteht aus dem macmon-eigenen Antivirus Connector. Diese aktive Komponente erlaubt Ihnen das Anbinden diverser Antivirus-Systeme wie beispielsweise F-Secure®, G-Data® Kaspersky®, McAfee®, Sophos®, Symantec ®, oder TrendMicro® und weitere, um auf kritische Events reagieren zu können, ohne notwendige Konfigurationen am Antivirus-Management selbst vornehmen zu müssen.

Virenscanner können die permanent neuen MalWare -Bedrohungen und modifizierte Schädlinge nicht immer vollständig abwehren und neben der Erkennung muss auch das Säubern gewährleistet sein. Regelmäßiges Patchen, aktuelle Virenscanner und zusätzliche Technologien wie Desktop Firewall, Host Intrusion Prevention oder Application Control bieten zwar bereits hervorragenden Schutz, dennoch gibt es Situationen, in denen der Virenscanner nicht mehr adäquat auf eine Bedrohung reagieren kann. Wenn das Antivirus auf einem Endgerät meldet, dass eine MalWare nicht gesäubert und nicht gelöscht werden konnte, möchte man das betreffende System möglichst schnell finden und isolieren, um händisch eingreifen zu können. Der macmon Antivirus Connector erkennt diese Situation und isoliert direkt das betreffende Endgerät oder verändert seinen Status auf „Non-Compliant“. Damit greift wieder das macmon-Regelwerk, wodurch das Endgerät isoliert oder lediglich ein bestimmter Personenkreis informiert wird, um die weitere Verbreitung zu vermeiden.

Aktive Statusänderung durch den macmon-Agenten

Die dritte Komponente der macmon Compliance besteht aus dem macmon-eigenen Compliance-Agenten, der zentral über die macmon-GUI verwaltet wird. Ist also bisher nur eine teilweise oder noch keine Lösung im Einsatz, die die Richtlinienkonformität der Endgeräte überprüft, so wird der macmon-Agent eingesetzt.

Verteilt auf die Windows-Endgeräte des Unternehmens, ermittelt er zyklisch den Status des Virenschutzes, der Firewall, des Patchlevels und weiterer konfigurierbarer Eigenschaften. Entspricht das Endgerät nicht den Vorgaben, so wird – wie beim Antivirus Connector oder durch ein anderes vorhandenes Compliance-System – der Status geändert und das Endgerät entsprechend des Regelwerkes isoliert.

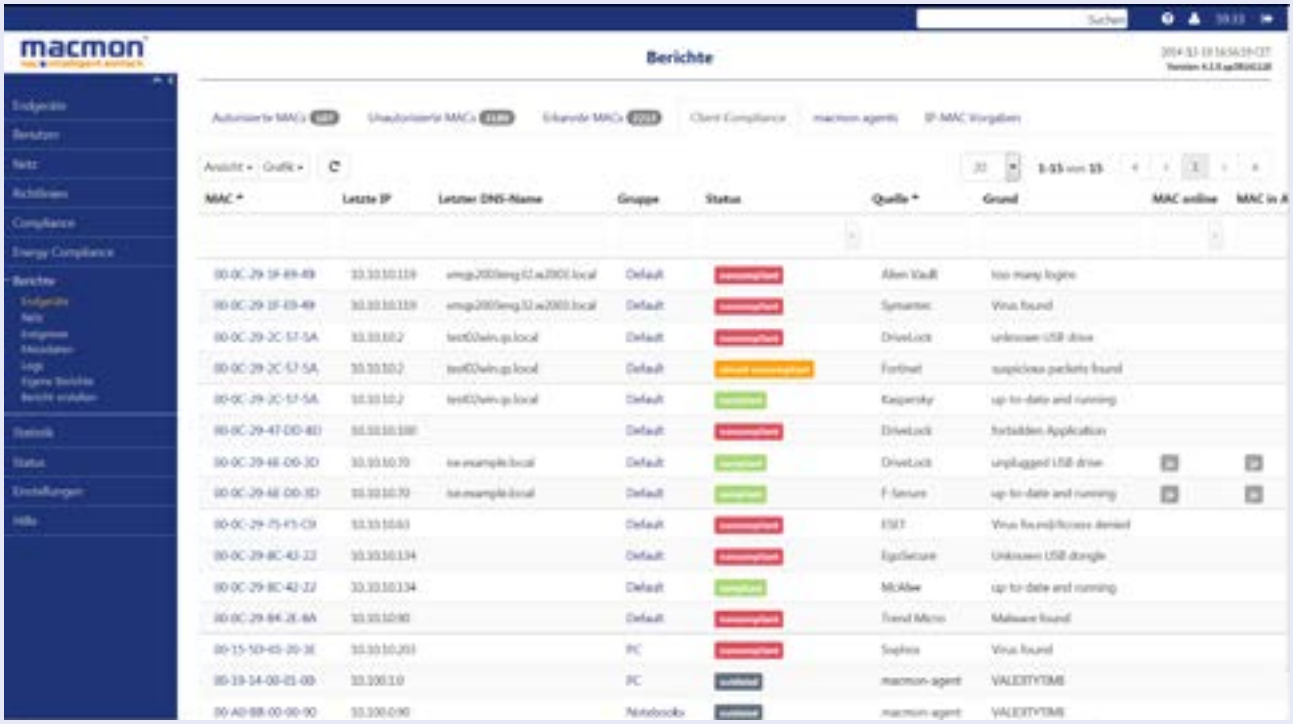
Egal, welche der drei Komponenten genutzt wird: Als unsicher eingestufte Endgeräte werden selbsttätig in ein Quarantäne-VLAN oder auch Remediation-LAN verschoben, um sie in diesem geschützten Umfeld hinsichtlich des Sicherheitsstatus zu aktualisieren. Nach erfolgreicher Aktualisierung werden die Systeme unmittelbar wieder ihrer ursprünglichen Produktiv-Umgebung im Netzwerk zugewiesen.

Über die Report- und die Statistik-Funktionen bietet die macmon Compliance eine umfassende Übersicht über den Sicherheitszustand, die übermittelnden Quellen zum Compliance-Status und Informationen zu Sicherheitsabweichungen der verwalteten Endgeräte.

Für die vierte Komponente wurde die zukunftsweisende Technologie IF-MAP integriert, die gemeinsam von der Trusted Computing Group, macmon secure und weiteren Partnern in Forschungsprojekten entwickelt wurde.
Darüber können teilnehmende Produkte ihren Status im Netzwerk publizieren, während macmon zusätzlich auf

entsprechende Meldungen reagieren kann und wiederum gefährliche Systeme vom Netzwerk isoliert.

Detailliertere Informationen finden Sie auch unter www.esukom.de.



Kontakt

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