



Sicherheit von Windows Clients

Unternehmensnetze sollten vor externen Gefährdungen wie beispielsweise Viren, Würmer, Trojaner und andere Angriffe geschützt werden. Sicherheitsrisiken entstehen hierbei insbesondere beim Austausch von Daten über das Internet oder im Bereich des Email-Verkehrs. Ein nicht zu unterschätzendes Sicherheitsrisiko stellt zudem der Einsatz von Notebooks dar, denn mobile Geräte sind häufig Malware-Angriffen ausgesetzt. Wird das mobile Gerät später wieder im internen Netzwerk in Betrieb genommen, so kann sich die Malware ungehindert im gesamten Unternehmensnetz verbreiten, mit den hinlänglich bekannten Folgen. Bei einem solchen intern durchgeführten Angriff gewährleisten die zentralen Schutzinstanzen des Firmennetzwerkes meistens keine Sicherheit mehr, so dass gewährleistet werden muss, dass auf allen vorhandenen Endgeräten interne Abwehrmechanismen zur Verfügung stehen. Nur so kann die Ausbreitung schädlicher Software im Firmennetzwerk unterbunden werden.

Zu den grundlegenden Sicherheitsmechanismen gehört die Verfügbarkeit einer aktuellen Antiviren-Software, die Installation von Sicherheits-Patches, der Betrieb einer Personal Firewall und das Arbeiten mit personenbezogenen Rechten.

macmon client compliance

Die macmon client compliance sorgt dafür, dass alle Netzwerkarbeitsplätze den vorgegebenen Sicherheitseinstellungen tatsächlich entsprechen. macmon erkennt mit Hilfe des compliance Agenten Endgeräte, die die Sicherheitsvorgaben nicht erfüllen, und kann diese auch sofort isolieren. Entsprechende Vorfälle werden dem Administrator gemeldet.

Als unsicher eingestufte Geräte werden selbsttätig in ein Quarantäne-VLAN oder auch Remediation-VLAN verschoben, um sie in diesem geschützten Umfeld hinsichtlich der Sicherheitsstände zu aktualisieren. Nach erfolgreicher Aktualisierung werden die Clients unmittelbar ihrer ursprünglichen Produktiv-Umgebung im Netzwerk wieder zugewiesen.

Die macmon client compliance unterstützt somit den Netzwerkadministrator wirkungsvoll bei der Durchsetzung der IT-Sicherheitsrichtlinien des Unternehmens.

Funktionalität

Die macmon client compliance Option überprüft alle sicherheitsrelevanten Einstellungen der Windows Clients, wobei der compliance Agent hierzu periodische Kontrollen auf den Endgeräten durchführt. Die Prüfvorgänge werden zentral vom macmon Server verwaltet und können gemäß der bestehenden Sicherheitsrichtlinien ausgeführt werden. Die Beurteilung der erzielten Prüfdaten erfolgt durch den macmon Server anhand der vorbestimmten Regeln. Wird ein Client hierbei als ‚noncompliant‘ eingestuft, wird das Endgerät sofort isoliert, um eine weitere Gefährdung des Firmennetzes auszuschließen.



Überprüfung

Für die grundlegenden Sicherheitsauswertungen wird eine Reihe von Prüfjobs zur Verfügung gestellt. So kann beispielsweise ermittelt werden, ob der angemeldete Nutzer Administrator ist, ob der Update-Service gemäß den Vorgaben konfiguriert wurde, ob der Virenschutz aktuell und funktionsfähig ist sowie ob die IP-Adressen manuell oder per DHCP vergeben wurden. Die Prüfjobs sind als offene Skripte realisiert und können vom Hersteller, von Partnern oder direkt vom Kunden jederzeit ergänzt werden, um den Prüfumfang zu verändern. Der Client-Status lässt sich über die WEB-GUI auf dem macmon Server abfragen und die Abfragerregeln lassen sich zentral anpassen. Über die Report- und die Statistik-Funktion bietet die macmon client compliance eine umfassende Übersicht über den Sicherheitszustand der verwalteten Endgeräte.

Client Fingerprint Check

Zur Feststellung von Veränderungen am Client oder um Angriffe durch MAC-Spoofing zu verhindern, wird über frei definierbare Parameter ein Fingerabdruck des Endgerätes erstellt, der bei jeder Abfrage durch den compliance Agent auf Abweichungen überprüft wird. Zur Bestimmung des gerätebezogenen Fingerabdruckes können beliebige Parameter herangezogen werden, die von der CPU-ID bis zu kundenspezifischen Registry-Einträgen reichen. Rechner mit einem manipulierten Fingerprint werden automatisch lokalisiert und entsprechend isoliert.

Voraussetzung und Lizenzierung

Die Implementierung der macmon client compliance setzt eine macmon network bundle Lizenz voraus. Die Lizenzierung richtet sich nach der Anzahl der abzufragenden Endgeräte, wobei die Microsoft Betriebssysteme Windows XP, Windows 7 und Vista unterstützt werden.

