

macmon client compliance Option

Sicherheit von Windows Clients

Das Unternehmensnetz muss vor Gefährdungen durch Viren, Würmer und andere Schädlinge geschützt werden. Diese können durch den Austausch von Daten über das Internet oder per Email entstehen. In vielen Fällen gehen diese Gefährdungen auch von Notebooks aus, die von Mitarbeitern außerhalb des Unternehmens genutzt werden und die dort einem Malware-Angriff zum Opfer gefallen sind. Nimmt der Anwender dann sein Notebook in der Firma wieder in Betrieb, kann sich die Malware im Unternehmens-Netz ungehindert auf die Suche nach neuen Opfern begeben.

Zentrale Schutzinstanzen für das Firmennetz kommen bei internen Angriffen nicht mehr zum Zuge. Jetzt muss sichergestellt sein, dass auf allen Geräten interne Abwehrmechanismen funktionsfähig verfügbar sind, um eine Ausbreitung der Schadsoftware zu vermeiden.

Zu den grundlegenden Sicherheitsmechanismen gehören die Verfügbarkeit einer aktuellen Antiviren-Software, das Installieren von Sicherheits-Patches, das Betreiben einer Personal Firewall und das Arbeiten mit eingeschränkten Rechten.

macmon client compliance

Mit der macmon client compliance Option kann sichergestellt werden, dass alle Netzwerkarbeitsplätze die vom Administrator vorgegebenen Sicherheitseinstellungen einhalten. Geräte die diese Vorgaben nicht erfüllen, werden von macmon lokalisiert und es werden über das Regelwerk festgelegte Aktionen ausgeführt. Dies reicht von der Information des Anwenders und des Administrators, bis hin zur automatischen Isolierung der Geräte.

Unsichere Geräte können automatisch in ein Remediation-VLAN gebracht werden, um sie in einem geschützten Umfeld zu aktualisieren. Nach erfolgreicher Behandlung werden sie wieder ihrer Produktiv-Umgebung zugewiesen.

Die macmon client compliance Option unterstützt den Administrator bei der Durchsetzung der Sicherheitsrichtlinien seines Unternehmens.

Funktionalität

Die macmon client compliance Option kontrolliert sicherheitsrelevante Einstellungen von Windows Clients. Der mitgelieferte Compliance Agent führt periodische Überprüfungen des Arbeitsplatzes durch. Die Prüfjobs werden vom macmon Server verwaltet und lassen sich jederzeit verändern oder erweitern.

Die Bewertung der Daten erfolgt durch den macmon Server entlang der vereinbarten Regeln. Wird ein Client als 'noncompliant' bewertet, kann über das Regelwerk ein

macmon client compliance Option

automatisierter Prozess gestartet werden, um zu verhindern dass Schaden von dem System ausgeht. Das Gerät kann zur „Heilung“ in ein separates Netz verbracht werden. Auch der Benutzer wird über das Sicherheitsrisiko informiert.

Überprüfungen

Für die grundlegenden Sicherheitsauswertungen wird eine Reihe von Prüfjobs mitgeliefert. Es wird ermittelt, ob der angemeldete Nutzer Administrator ist, ob der Update-Service entsprechend den Vorgaben konfiguriert wurde, ob der Virenschutz funktionsfähig ist und ob die IP-Adresse manuell oder per DHCP vergeben wurde.

Die bereitgestellten Prüf-Jobs sind als offene Skripte realisiert und können von Hersteller, Partner oder Kunden jederzeit ergänzt werden, um den Prüfumfang zu erweitern.

CC Devices							
Status	Host	OS	Agent IP	Geprüft	Nächster Scan	MAC	
●	nb-harry01	Microsoft Windows XP Pro 5.1	10.1.1.148	2008-02-20 16:14:04	2008-02-20 17:14:04	00-17-08-37-1E-06	10.1.1.148
●	nbdentschev01	Microsoft Windows XP Pro 5.1	10.1.1.150	2008-03-11 14:50:04	2008-03-11 15:50:04	00-02-A5-B7-C6-4F	10.1.1.150
●	nbdietrich02	Microsoft® Windows Vista 6.0	10.1.1.180	2008-02-29 16:12:26	2008-02-29 17:12:26	00-FF-6F-66-20-18	0.0.0.0
00-50-56-C0-00-01						192.168.134.1	
00-17-A4-DD-72-CB						10.1.1.180	
●	nbgordon01	Microsoft® Windows Vista 6.0	10.1.1.198	2008-03-07 09:03:29	2008-03-07 09:13:29	00-50-56-C0-00-08	192.168.47.1
00-0A-E4-EB-51-38						10.1.1.198	
00-50-56-C0-00-01						192.168.5.1	
●	NBVERTRIEB01	Microsoft Windows XP Pro 5.1	10.1.1.138	2008-03-11 14:37:11	2008-03-11 15:37:11	00-17-A4-E7-8B-8B	10.1.1.138
●	WSAlbrecht01	Microsoft Windows XP Pro 5.1	10.1.1.178	2008-02-26 16:07:41	2008-02-26 17:07:41	00-04-75-B1-04-BE	0.0.0.0
00-10-4B-6A-E3-02						10.1.1.178	
00-50-56-C0-00-08						192.168.40.1	
00-50-56-C0-00-01						192.168.153.1	
00-50-56-C0-00-08						192.168.40.1	
●	wsaltenhein02	Microsoft Windows XP Pro 5.1	10.1.1.137	2008-03-11 15:15:54	2008-03-11 15:25:54	00-50-56-C0-00-04	192.168.139.1
00-50-56-C0-00-08						192.168.126.1	
00-50-56-C0-00-01						192.168.149.1	
00-50-56-C0-00-08						192.168.126.1	
00-14-2A-18-60-B8						10.1.1.137	

Der Status der Clients lässt sich über die WEB-GUI auf dem macmon-Server abfragen und die Abfrageregeln lassen sich jederzeit zentral anpassen. Auch über die Report- und die Statistik-Funktion bietet die client compliance Option eine umfassende Übersicht über den Sicherheitszustand der Geräte.

Voraussetzung und Lizenzierung

Voraussetzung für die Implementierung der client compliance Option ist das macmon network bundle.

Die Lizenzierung erfolgt über die Anzahl der von macmon abzufragenden Endgeräte, wobei Lizenzpakete für 100, 250, 500, 1000, 5000 und 10.000 Clients erwerbbar sind.

Im Client-Bereich werden die Microsoft Betriebssysteme Windows XP und Windows 2000 Professional unterstützt.