MACMON ANTIVIRUS CONNECTOR

Automatische Isolation infizierter Endgeräte

Als kundennaher Entwickler von IT-Sicherheitstechnologien haben wir in vielen Kundenumgebungen die Anforderung gesehen, schnellstmöglich auf kritische Situationen reagieren zu können. Conficker und andere Malware-Ausbrüche haben gezeigt, dass in der Regel jede manuelle Reaktion oft zu spät erfolgt. macmon bietet durch die zentrale Kontrolle der Netzwerkzugänge und seine offene Architektur die machtvolle Position, genau hier automatisiert zu unterstützen.

Mehrwert zu gängigen Antivirus-Systemen

Virenscanner können die permanent neuen Malware-Bedrohungen und modifizierten Schädlinge nicht immer vollständig abwehren - neben der Erkennung muss aber 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, in der Regel ist der Aufwand, all diese Systeme zu managen und aktuell zu halten, jedoch so groß, dass nicht alles eingesetzt oder die Pflege vernachlässigt wird. Der macmon Antivirus Connector ist daher die Antwort auf die Anforderung nach einer Lösung, die automatisch reagiert, wenn der Virenscanner einer Bedrohung einmal nicht mehr Herr werden 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. Je nach genutztem Antivirus-System werden unterschiedliche Informationen geliefert, die durch den Antivirus Connector ausgewertet werden. Die Reaktion darauf kann, angefangen von der reinen Benachrichtigung über die Zuweisung eines neuen VLANs, bis hin zur absoluten Isolierung des Systems, selbst definiert werden.

Key facts

- ✓ Schnelle Isolation von Infektionsquellen von Ihrem Netzwerk
- ✓ Umgehende Information über die Maßnahme und zur Bedrohungssituation
- ✓ Das Live-Bestandsmanagement von macmon informiert, um welches Endgerät es sich handelt und wo es sich befindet.
- ✓ Betroffene Systeme können basierend auf den System-Informationen in aller Ruhe gesäubert und wieder in Betrieb genommen werden.

Als Auslöser können beliebige Events des Virenschutzes verwendet werden. Grundlegend nutzt der macmon Antivirus Connector jedoch die folgenden Situationen:

- ✓ Objekt konnte nicht gesäubert und nicht gelöscht werden,
- ✓ eine Malware wurde innerhalb einer bestimmten Zeitspanne eine definierte Menge mal entfernt,
- ✓ eine bestimmte Malware (definierbar) wurde entdeckt.

Aufgrund der unterschiedlichen Systeme sind auch unterschiedliche Ereignisse sichtbar. So bietet die Kombination mit McAfee beispielsweise zusätzlich die Möglichkeit, auf „Angriffe“ zu reagieren. Versucht ein System (egal ob ein eigenes oder ein fremdes) eine Malware auf eines Ihrer Systeme zu kopieren, so wird dies als Angriff protokolliert. Durch diese Information kann macmon das „angreifende“ Endgerät entsprechend behandeln, selbst wenn es ein temporär zugelassener Gast ist. macmon Antivirus Connector ist ein Add-On zur Netzwerkzugangskontrolllösung von macmon und ist Bestandteil des Premium Bundles. Die Lizenzierung erfolgt pro überwachter Antivirus-Management-Instanz. Aktuell werden die Produkte der Hersteller G-Data, F-Secure, Kaspersky, McAfee, Sophos, Symantec und Trend Mirco unterstützt. Weitere Hersteller sind bereits in direktem Kontakt mit der macmon Entwicklung und werden ebenfalls in Kürze eingebunden.

Kontakt

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