Wie kann ich eine Webseite auf der Cisco Web Security Appliance (ab Version 5.2.0) manuell Whitelist erstellen, sodass die Scans von WBRS, WebRoot oder McAfee umgangen werden?

Inhalt

Frage:

Wie kann ich eine Webseite auf der Cisco Web Security Appliance (ab Version 5.2.0) manuell Whitelist erstellen, sodass die Scans von WBRS, WebRoot oder McAfee umgangen werden?

Symptome:

Der Benutzer versucht, auf eine legitime Website zuzugreifen, wird jedoch aufgrund einer niedrigen WBRS-Bewertung (Virusinfektion des Webservers, Spam, der über die Webserver-IP gesendet wird usw.) oder aufgrund eines der Anti-Malware-Engines blockiert.

Wenn der Benutzer aufgrund eines niedrigen WBRS blockiert wird, wird die Meldung MALWARE_GENERAL block (MALWARE_GENERAL-Block) angezeigt. Die Zugriffsprotokolle zeigen an, dass das WBRS unter dem Blockierungsgrenzwert liegt (Standardwert: -6,0).

Wenn Sie eine permanente Lösung benötigen, wenden Sie sich bitte an das Cisco TAC, damit die Seite überprüft werden kann, um das WBRS anzupassen oder falsche Positivmeldungen an die Antivirus- und Anti-Malware-Anbieter zu melden.

Sie können sich auch an das Cisco TAC wenden, um weitere Informationen über die Blockierung der Website zu erhalten, sodass der technische Kontakt oder Administrator der Website benachrichtigt werden kann und die erforderlichen Schritte ausführen kann.
Stellen Sie sicher, dass Sie die entsprechenden Blockierungscodes und Zugriffsprotokollleitungen angeben, wenn Sie sich an das Cisco TAC wenden.

So umgehen Sie WBRS:

4. Klicken Sie auf den Link in der Spalte "Webreputation und Anti-Malware-Filterung" Ihrer neu erstellten Web-Zugriffsrichtlinie (die bis jetzt "globale Richtlinie" lautet).
5. Wählen Sie "Webreputation und benutzerdefinierte Einstellungen für Anti-Malware definieren".

Hinweis: Wenn Sie die Aktion in der URL-Kategorie auf "Zulassen" setzen, wird die Anti-Malware-

/Virus-Prüfung umgangen.

So umgehen Sie WBRS und Anti-Malware-Scanning:

Hinweis: Die Deaktivierung von Anti-Malware-Scans (Webroot und/oder McAfee) kann ein potenzielles Sicherheitsrisiko darstellen. Dies sollte nur für Sites durchgeführt werden, bei denen es vertrauenswürdig ist, Malware nicht einzudämmen.