Was ist der Unterschied zwischen der Outbreak-Quarantäne und der Virus-Quarantäne?

Inhalt

Frage:

Was ist der Unterschied zwischen der Outbreak-Quarantäne und der Virus-Quarantäne?

Antwort:

AsyncOS-Quarantänen enthalten zwei integrierte Quarantänebereiche, die nicht gelöscht werden können: Outbreak und Virus.

Die Outbreak-Quarantäne wird nur von Virus-Outbreak-Filtern verwendet (sofern aktiviert).

Nachrichten, die den konfigurierten Schwellenwert für die Virenbedrohungsstufe der Cisco E-Mail Security Appliance (ESA) erfüllen oder darüber hinausgehen, werden in der Outbreak-Quarantäne aufbewahrt, anstatt zugestellt zu werden. Nachrichten können nach Ermessen des Quarantäne-Managers aus der Outbreak-Quarantäne freigegeben oder gelöscht werden. Nachrichten verlassen die Quarantäne auch, wenn die konfigurierten Zeit- oder Größenbeschränkungen überschritten werden, und sie werden mit der Standardrichtlinieneinstellung der Quarantäne behandelt, um sie zu löschen oder freizugeben, wenn diese Grenzwerte erreicht werden.

Nach der Veröffentlichung aus dem Outbreak-Quarantänebereich werden die Nachrichten vom Antivirus-Modul erneut gescannt, und die entsprechenden Maßnahmen werden gemäß den Virenschutzrichtlinien ergriffen. Je nach Richtlinie kann eine Nachricht zugestellt, gelöscht oder mit Virenanhängen zugestellt werden. Es wird erwartet, dass Viren häufig während des erneuten Scans nach der Freisetzung aus der Outbreak-Quarantäne gefunden werden. Mithilfe der E-Mail_Logs-Dateien oder der Nachrichtenverfolgung der ESA kann ermittelt werden, ob eine einzelne Nachricht, die in der Quarantäne aufgezeichnet wurde, eine Viruslast aufweist und ob und wie sie zugestellt wurde.

Der Virus-Quarantänebereich ist für den Empfang von Nachrichten verfügbar, die Sophos als mit Viren infiziert, verschlüsselt oder nicht scannbar klassifiziert. In jedem dieser Fälle ist die Nachricht viral oder potenziell viral. Nachrichten, die an die Virenquarantäne gesendet werden, verbleiben dort, bis entweder der Quarantänemanager entscheidet, sie freizugeben oder zu löschen, oder die konfigurierte Größe oder Zeitbeschränkung der Quarantäne erreicht ist. Die Standardaktion ist konfigurierbar, wenn die Quarantänegrenzen erreicht sind.

Von der Quarantäne freigegebene Nachrichten werden nicht vom Antivirus-Modul erneut

gescannt. Während der Quarantäne kann der Quarantäne-Manager jedoch eine einzelne Nachricht scannen, um festzustellen, ob sie gemäß der aktuellen Gruppe von Virus-IDEs, die auf der ESA geladen sind, viral ist.

Hinweis: Neue Viren werden in Quarantäne gestellt, aber die ältesten Nachrichten in der Quarantäne werden geleert, um Platz für die neuen zu schaffen. Dies ist eine "First in, First Out"-Richtlinie. Die Löschung der ältesten Nachrichten basiert jedoch auf der Konfiguration der Quarantäne, d. h. die Nachrichten werden entweder vorzeitig gelöscht oder vorzeitig freigegeben.

Obwohl die integrierten Quarantänen nicht gelöscht werden können, kann der ihnen zugewiesene Speicherplatz neu konfiguriert werden. Der für Quarantänen verfügbare Speicherplatz variiert je nach ESA-Modell und wird auf der Seite Monitor->Quarantänebereiche->Quarantäneverwaltung in der GUI angezeigt. Die Mindestgröße für eine Quarantäne beträgt 250 MB. Durch eine feste Obergrenze für die Quarantäne wird sichergestellt, dass eine plötzliche Zunahme der Quarantäneaktivität die E-Mail-Warteschlangen der ESA nicht beeinträchtigen und die normale Nachrichtenzustellung nicht beeinflussen kann.