Cisco Email Security Appliance (ESA) Checkliste zur Wirksamkeit von Spam-Schutz

Inhalt

Einführung

Die folgenden Verfahren und Empfehlungen sind "Best Practices" zur Reduzierung der Spam-Aufkommen durch die ESA. Beachten Sie, dass sich jeder Kunde unterscheidet und dass einige dieser Empfehlungen die Anzahl der als Spam klassifizierten legitimen E-Mails (Fehlalarme) erhöhen können.

Grundlegende Einrichtung

1. Stellen Sie sicher, dass Anti-Spam aktiviert ist:

   Überprüfen Sie, ob alle Ihre MX-Datensätze (einschließlich MX-Datensätze mit niedrigerer Priorität) E-Mails über ESAs weiterleiten.Vergewissern Sie sich, dass Ihre Appliances einen gültigen Anti-Spam-Feature-Schlüssel haben.Stellen Sie sicher, dass Anti-Spam für alle entsprechenden Richtlinien für eingehende E-Mails aktiviert ist.

2. Überprüfen Sie, ob Sie Regelaktualisierungen für Antispam-Regeln erhalten. Überprüfen Sie, ob die **aktuellsten** Zeitstempel für Updates unter Security Services > Anti-Spam innerhalb der letzten 2 Stunden abgelaufen sind.

3. Stellen Sie sicher, dass Nachrichten von Anti-Spam gescannt werden:

   Überprüfen Sie ein Beispiel für verpasste Spam-Nachrichten für die folgende Überschrift: X-IronPort-Anti-Spam-Ergebnis:Wenn dieser Header fehlt:

   Vergewissern Sie sich, dass Sie keine zulässigen Einträge oder Filter haben, die dazu führen, dass Spam den Spam-Scan umgeht (siehe unten).Stellen Sie sicher, dass die Nachrichten den Scanvorgang nicht umgehen, da sie die maximale Größe für den Nachrichtenscan überschreiten (Standardwert: 262144 Byte). Eine Reduzierung dieser Einstellung verbessert die Leistung nicht erheblich und kann zu einem verpassten SPAM führen. Bei einer Evaluierung ist es außerdem wichtig, sicherzustellen, dass die IPAS-Einstellung mit den anderen getesteten Produkten übereinstimmt.Gehen Sie jeden HAT-Eintrag durch, und bestätigen Sie, dass "spam_check=on" für alle Richtlinien zum Durchfluss eingehender E-Mails gilt. Solange der Standardwert "spam_check= on" hat und keine der Mail-Flow-Richtlinien ihn explizit ausschalten, wird dies korrekt konfiguriert. Achten Sie

besonders auf die TRUSTED/allowLIST-Einstellungen. Häufig fügen Kunden versehentlich einen Absender zu ihrer zulässigen Liste hinzu, der Spam weiterleitet - beispielsweise durch Hinzufügen der Domäne eines ISP oder Partners, der sowohl Spam als auch legitime E-Mails an die Absendergruppe allowLIST weiterleitet.

Überprüfen Sie schnell die Nachrichtenfilter, um sicherzustellen, dass keine Filter vorhanden sind, die "spamcheck überspringen". Falls ja, stellen Sie sicher, dass der Gesprächspartner das tut, was er tun sollte (beachten Sie, dass die Zuordnung eines einzelnen rcpt-to bei Nachrichten mit mehr als 30 Empfängern möglich ist).

Suchen Sie ein aktuelles SPAM-Beispiel (Uhrzeit, Datum, Punkt usw.), und verweisen Sie auf die mail_logs, um zu sehen, was passiert ist. Bestätigen Sie, dass Anti-Spam ein negatives Urteil zurückgibt.

4. Stellen Sie sicher, dass Sie die gewünschten Maßnahmen für Spam-positive Nachrichten ergreifen. Überprüfen Sie in den Richtlinien für eingehende E-Mails, wie Anti-Spam-Verdicts gehandhabt werden. Stellen Sie sicher, dass Spam-positive und verdächtige Nachrichten in der Standardrichtlinie verworfen oder unter Quarantäne gestellt werden und dass alle anderen Richtlinien entweder das Standardverhalten verwenden oder den Standardwert bewusst überschreiben.

5. Anwendung aggressiverer Spam-Schwellenwerte, wenn Fehlalarme weniger Besorgnis erregend als Spam-Nachrichten sind:

   Verringern Sie den Schwellenwert für positive Spam-Mails auf 80 (Standardwert ist 90), wenn Fehlalarme nicht die 'bestimmte' Grenze überschreiten.

   Verringern Sie den Schwellenwert für verdächtige Spam-Mails auf 40 (Standardwert ist 50), wenn Fehlalarme bei der Schwellenwertangabe keine Rolle spielen.

   Wenn die meisten Ihrer Spam-Beschwerden von einer Teilgruppe von Empfängern stammen, können Sie eine separate Mail-Richtlinie für diese Benutzer mit niedrigeren Spam-Schwellenwerten erstellen, um diese gezielt für diese Empfänger zu filtern.

   Änderungen an diesen Werten sollten nicht auf die leichte Schulter genommen und auch nicht ohne harte Daten umgesetzt werden, um festzustellen, wie die rePurcussive-Effekte aussehen werden.

   Stellen Sie außerdem nicht unbedingt Werte in die andere Richtung ein, nur um Fehlalarme zu vermeiden.Stellen Sie sicher, dass Fehlalarme und Fehlalarme an das TAC gesendet werden.

6. SBRS-Einstellungen und HAT-Richtlinien optimieren:

   Die meisten Unternehmen möchten SBRS -10 zu -3.0 zu ihrer Sperrliste und SBRS -3.0 zu -1.0 zu ihrer SUSPECTLIST hinzufügen. Aggressivere Kunden können SBRS -10 bis -2.0 blockieren und -2.0 bis -0.6 zur SUSPECTLIST hinzufügen.

In einigen Fällen belegt die Tatsache, dass ein Absender noch keine SenderBase-Reputationsbewertung hat, dass es sich bei diesem Absender möglicherweise um einen Spammer handelt. Sie können SBRS "none" direkt zu einer Absendergruppe hinzufügen, die die Richtlinie "Throttling" erhält, z. B. zu Ihrer SUSPECT-Absendergruppe.

Ändern Sie die maximale Anzahl von Empfängern pro Stunde in 5 für die Richtlinie "Throttling".

Erwägen Sie die Erstellung von mehr als einer Richtlinie für "gedrossene" Nachrichten, um unterschiedliche Empfänger pro Stunde durchzusetzen - z. B. Sender mit einer SBRS-Rate zwischen -2 und -1 bis 5 Empfängern pro Stunde und Absender mit einer SBRS-Rate zwischen -1 und 0 bis 20 Empfängern pro Stunde.

7. Sender Verification für die Richtlinie "Throtred" Mailflow aktivieren:

   Kunden können Absender mit nicht vorhandenem oder falsch konfiguriertem DNS zur SUSPECTLIST-Absendergruppe hinzufügen.

   Der PTR-Datensatz des verbindenden Hosts ist im DNS nicht vorhanden.Die PTR-Datensatzsuche des angeschlossenen Hosts schlägt aufgrund eines temporären DNS-Ausfalls fehl.

   Die umgekehrte DNS-Suche (PTR) des verbindenden Hosts stimmt nicht mit der vorwärts gerichteten DNS-Suche (A) überein.

   Es besteht ein gewisses Risiko von Fehlalarmen von Absendern mit falsch konfiguriertem DNS, sodass Kunden möglicherweise eine separate Mailflow-Richtlinie einrichten möchten, die eine benutzerdefinierte 4xx-Antwort zurückgibt, die angibt, warum Nachrichten abgelehnt werden.

   Weitere Informationen zur Absenderverifizierung finden Sie in der Online-Hilfe oder im AsyncOS-Benutzerhandbuch.

8. LDAP Accept und Directory Harvest Attack Protection aktivieren:

   Viele Spammer senden E-Mails an eine große Anzahl ungültiger Adressen, sodass das Blockieren von Absendern, die an ungültige Empfänger senden, auch Spam verringert.

   Wenn LDAP Accept bereits aktiviert ist, stellen Sie sicher, dass der DHAP (Directory Harvest Protection) auch für jeden eingehenden Listener konfiguriert ist, bei dem maximal ungültige Versuche zwischen 5 und 10 pro IP zulässig sind.

9. Content-Wörterbücher aktivieren:

   Ihre ESA umfasst zwei Content-Wörterbücher: profanity.txt und sexuelle_content.txt. Die Verwendung dieser Wörterbücher kann zwar Fehlalarme hervorrufen, einige Kunden haben jedoch festgestellt, dass das Filtern ihres E-Mail-Streams nach ungeeigneten Wörtern das Risiko verringern kann, dass die "falsche Person" die "falsche E-Mail" erhält. Diese Filter

können nur auf die "squeaky-Räder" angewendet werden, indem sie eine Benutzergruppe in einer bestimmten Mail-Richtlinie aktivieren.

10. Melden Sie falsch klassifizierte Nachrichten an das Cisco TAC.

11. Um eine große Anzahl von Fehlalarmen zu verhindern, sollte SBRS für das Scannen nach außen deaktiviert werden. Der Grund hierfür ist, dass SBRS die Reputation eingehender IPs untersucht und die meisten dieser IPs in einem internen Netzwerk dynamisch sind. Befolgen Sie die Schritte im nächsten Abschnitt.

SBNP aktivieren

1. Stellen Sie sicher, dass eingehende und ausgehende E-Mails auf separaten Listenern gespeichert sind.

2. SenderBase-Suchvorgänge für ausgehende E-Mails pro unten deaktivieren Gehen Sie zu Network > Listeners (Netzwerk > Listener), wählen Sie alle ausgehenden Listener aus, wählen Sie "Advanced" (Erweitert) aus, und deaktivieren Sie das Kontrollkästchen neben "Use SenderBase IP profiling" (SenderBase-IP-Profilerstellung verwenden).

   SenderBase Network Participation (SBNP) kann die Effektivität von Reputationsfiltern, Anti-Spam- und Virus-Outbreak-Filtern erheblich steigern. Bei Aktivierung von Anti-Spam hat SBNP zudem keine spürbaren Leistungseinbußen und ist zudem äußerst sicher.

   Hinweis: Das Spam-Volumen in Ihrem Unternehmen wird sich mit der Zeit ändern. Es ist möglich, dass mehr Spam die ESAs passieren, weil Sie mehr Spam erhalten als in der Vergangenheit. Sie können dieses Verhalten im Laufe der Zeit verfolgen, indem Sie die Seite Übersicht über eingehende E-Mails sehen und die Posten "Stopped by Reputation Filtering" (Durch Reputationsfilterung gestoppte Nachrichten) und "Spam detected" (Spam-Nachrichten erkannt) hinzufügen.

SBRS-Begründung

Die große Sorge bei Fehlalarmen ist, dass wichtige E-Mails verloren gehen könnten. In diesem Zusammenhang ist die Praxis, Spam-E-Mails zu isolieren oder zu versenden, problematisch. Wenn eine legitime E-Mail an eine Quarantäne oder einen Spam-Ordner gesendet wird, muss eine proaktive Suche ausgeführt werden, um festzustellen, dass der Schinken fälschlicherweise als Spam klassifiziert wurde.

Im Gegensatz dazu werden blocklist- und rate-limitierte E-Mails so blockiert, dass der Absender sofort benachrichtigt wird. Wenn es sich bei diesem Absender NICHT um einen Spammer handelt, wird er wahrscheinlich eine andere Möglichkeit finden, mit Ihnen in Kontakt zu treten. Tatsächlich ist eine allgemeine Richtlinie, die standardmäßig blockiert und dann vertrauenswürdige Partner auf Anfrage akzeptiert, eine bessere Position für einige Unternehmen.

Eine Drosselung, wenn sie richtig festgelegt wird, sollte nur selten, wenn überhaupt, Partner betreffen, bietet jedoch Schutz vor Domänen, die mit Viren infiziert sind. Die Drosselung wird Spammern ebenfalls entlasten. Wir kennen eine Spammer-Technik, um eine große Anzahl von IP-

Adressen zu erwerben, genug "gute" E-Mails zu generieren, um eine anständige SBRS-Bewertung zu erhalten, und dann Spamming zu starten. Ein größerer verdächtiger Listenbereich sollte diese auffangen, den Schaden begrenzen, den sie verursachen, und eventuell dazu führen, dass sie Spam nicht mehr an Ihre Domain senden.