Richten Sie eine benutzerdefinierte SvD-Policy ein, um formatierte und unformatierte Sozialversicherungsnummern zu erkennen.

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine benutzerdefinierte SvD-Policy einrichten, um formatierte und unformatierte Sozialversicherungsnummern (SSN) auf der Cisco E-Mail Security Appliance (ESA) zu erkennen.

Richten Sie eine benutzerdefinierte SvD-Policy ein, um formatierte und unformatierte Sozialversicherungsnummern zu erkennen.

Die DLP-Scan-Engine erkennt formatierte Sozialversicherungsnummern nur. Dies liegt an der hohen Anzahl an Fehlalarmen, die durch 9-stellige Zahlen in Daten in verschiedenen Branchen verursacht werden. Beispielsweise sind die Banking-ABA-Weiterleitungsnummern neunstellig und würden beim Scannen nach einer unformatierten Sozialversicherungsnummer ausgelöst. Daher wird empfohlen, keine unformatierten Sozialversicherungsnummern zu durchsuchen, es sei denn, dies wird von Ihrem Unternehmen ausdrücklich gefordert. Wenn es erforderlich ist, dass Ihr Unternehmen nach unformatierten Sozialversicherungsnummern sucht, können Sie eine benutzerdefinierte SvD-Policy erstellen, indem Sie die in der unten stehenden Lösung beschriebenen Schritte ausführen.

AsyncOS bietet die Möglichkeit, mithilfe von Klassifizierungen, die von RSA oder Ihrem Unternehmen entwickelt wurden, eigene Richtlinien von Grund auf zu erstellen. Diese Option wird als erweitert angesehen und sollte nur in seltenen Fällen verwendet werden, wenn die vordefinierten Richtlinienvorlagen nicht die spezifischen Anforderungen Ihrer Netzwerkumgebung

erfüllen.

Erstellen einer benutzerdefinierten Richtlinie

1. Über die GUI: **Mail-Policys > SvD-Policy-Manager**.
2. Klicken Sie auf **SvD-Policy hinzufügen...** -Taste.
3. Wählen Sie am unteren Bildschirmrand die Option **Benutzerdefinierte Richtlinie** aus, und klicken Sie neben Benutzerdefinierte Richtlinie auf **Hinzufügen**.
4. Geben Sie einen SvD-Policy-Namen ein. Beispiel: *Benutzerdefinierte SSN-Richtlinie*.

Klassifizierung erstellen

Durch das Erstellen benutzerdefinierter Klassifizierer können Sie die gescannten Kriterien in der DLP-Engine flexibel festlegen. Dies dient zu unserem Vorteil, um sowohl formatierte SSN als auch unformatierte SSN zu prüfen.

1. Wählen Sie im Dropdown-Menü Klassifizierung für Inhaltszuordnung die Option **Klassifizierung erstellen aus**, und klicken Sie auf die Schaltfläche **Hinzufügen**.
2. Geben Sie einen Klassifizierungsnamen für die Inhaltszuordnung ein. Beispiel: *Alle Formate SSN.*
3. Legen Sie im Abschnitt Regeln die Dropdown-Liste von Wörtern oder Kennzeichenfolgen auf **Entität fest**.
4. Wählen Sie die Entität aus: **US Sozialversicherungsnummer, formatiert**.
5. Klicken Sie auf **Regel hinzufügen**.
6. Wählen Sie erneut **Entität aus**.
7. Wählen Sie die Entität aus: **US Sozialversicherungsnummer, unformatiert**.
8. Klicken Sie auf **Senden**.

Festlegen der Schweregradeinstellungen

Die folgenden Einstellungen sind ein guter Ausgangspunkt, dienen jedoch lediglich als Richtlinie, um Ihnen zu helfen. Möglicherweise sind einige Kalibrier- oder andere Konfigurationseinstellungen erforderlich, die auf die Anforderungen Ihres Unternehmens abgestimmt sind.

- **Einstellungen für kritischen Schweregrad**
  Auf Nachrichten angewendete Aktion: **Quarantäne**
  Verschlüsselung aktivieren (aktiviert)
  Verschlüsselungsregel: **Nachrichtenverschlüsselung immer verwenden**
  Verschlüsselungsprofil (wählen Sie Ihr konfiguriertes Verschlüsselungsprofil aus dem Dropdown-Menü aus)
  Betreff der verschlüsselten Nachricht: **$Thema**
- **Einstellungen für hohen Schweregrad**
  Auf Nachrichten angewendete Aktion: **Bereitstellung**
  Verschlüsselung aktivieren (aktiviert)
  Verschlüsselungsregel: **Nachrichtenverschlüsselung immer verwenden**
  Verschlüsselungsprofil (wählen Sie Ihr konfiguriertes Verschlüsselungsprofil aus dem

Dropdown-Menü aus)
Betreff der verschlüsselten Nachricht: **$Thema**

- **Einstellungen für mittleren Schweregrad**
  Auf Nachrichten angewendete Aktion: *Bereitstellung*
  Verschlüsselung aktivieren (aktiviert)
  Verschlüsselungsregel: **Nachrichtenverschlüsselung nur verwenden, wenn TLS fehlschlägt**
  Verschlüsselungsprofil (wählen Sie Ihr konfiguriertes Verschlüsselungsprofil aus dem Dropdown-Menü aus)
  Betreff der verschlüsselten Nachricht: **$Thema**
- **Einstellungen für niedrigen Schweregrad**
  Auf Nachrichten angewendete Aktion: **Bereitstellung**
  Verschlüsselung aktivieren (deaktiviert)

Schweregrad festlegen

Auch hier stellen die folgenden Einstellungen einen guten Ausgangspunkt dar. Sie dienen jedoch lediglich als Richtlinie, um Ihnen zu helfen, und erfordern möglicherweise einige Kalibrier- oder andere Konfigurationseinstellungen, die auf die Anforderungen Ihres Unternehmens abgestimmt sind.

1. Klicken Sie rechts neben dem Schweregraddiagramm auf **Skalierung bearbeiten**.
2. Schieben Sie den ersten Griff, bis IGNORE = 0 ist.
3. Schieben Sie den zweiten Griff bis NIEDRIG = 1 bis 9.
4. Schieben Sie den dritten Griff bis MEDIUM = 10 bis 50.
5. Schieben Sie den vierten Griff bis HIGH = 60 bis 89.
6. Wenn Sie diese Einstellung korrekt eingestellt haben, wird CRITICAL automatisch auf 90 bis 100 eingestellt.
7. Klicken Sie abschließend auf **Fertig**.

Änderungen senden und bestätigen

Um die Erstellung dieser Richtlinie abzuschließen, klicken Sie auf die Schaltfläche **Senden**. Klicken Sie in der rechten oberen Ecke der GUI auf die Schaltfläche **Änderungen bestätigen**. Sie gelangen zum Bildschirm "Unbestätigte Änderungen", und klicken Sie auf **Änderungen bestätigen**. Wenn **die** GUI erfolgreich ist, sollten Sie in der oberen rechten Ecke der GUI die Option **Keine Änderungen ausstehend** sehen.

Abschließende Schritte

Sie müssen jetzt die SvD-Policy für eine Mail-Policy für \"Ausgehend\" unter **Mail-Policys->Mail-Policys für \"Ausgehend\"** aktivieren. Zum Testen außerhalb der Produktion können Sie eine benutzerdefinierte Richtlinie für ausgehende Nachrichten erstellen, die Sie als Absender festgelegt haben, und die SvD-Richtlinie für diese Testrichtlinie aktivieren.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems