Trigger een DLP-overtreding om een HIPAA-beleid op de ESA te testen

Inhoud

Inleiding

In dit document wordt beschreven hoe u HIPAA-gegevensverliespreventie (DLP) kunt testen om een ziektekostenverzekering en verantwoording af te leggen nadat u DLP hebt ingeschakeld voor uw uitgaande e-mailbeleid op uw Cisco-e-mail security applicatie (ESA).

Trigger een DLP-overtreding om een HIPAA-beleid te testen

Dit artikel bevat enige reële inhoud, die is aangepast om de mensen te beschermen, om te testen tegen het DLP-beleid op uw ESA. Deze informatie is bedoeld om het DLP-beleid van de HIPAA en de Health Information Technology for Economic and Clinical Health (HITECH) op gang te brengen en tevens andere DLP-beleidslijnen zoals Social Security Number (SSN), CA AB-1298, CA SB-1386, enzovoort in gang te zetten. Gebruik de informatie wanneer u een test-e-mail via de ESA verstuurt of wanneer u het traceringstool gebruikt.

> **Opmerking**: U moet een geldig of vaak misbruikt SSN gebruiken in de uitvoer waar dit is geblokkeerd.

> **Opmerking**: voor het HIPAA- en HITECH DLP-beleid dient u ervoor te zorgen dat u aangepaste identificatienummers hebt ingesteld zoals aanbevolen. Identificatienummers van de patiënt (aan te passen aan aanbevolen) of US National Provider Identifier of US Social Security Number en Healthcare Dictionaries. Dit moet zo zijn ingesteld dat u het programma correct kunt activeren.

```
Procedure Notes
Progress Notes
Archie M Johnson Tue Jun 30, 2009 10:31 AM Pended
June 30, 2009
Patient Name: Gina, Lucas DOB: 01/23/1945
Telephone #: (559) 221-2345
SS#: [[[PLACE SSN HERE]]]
--------------------------------------------------------------------------------
Insurance: UHC
How was the patient referred to the office: *** ({:20})
Is a family member currently being seen by the requested physician? {YES/NO:63}
If yes, what is the family members name : ***
```

```
Previous PCP / Medical Group? ***
Physician Requested: Dr. ***
REASON:
1) Get established, no current problems: {YES/NO:63}
2) Chronic Issues: {YES/NO:63}
3) Specific Problems: {YES/NO:63}
Description of specific problem and/or chronic conditions:
{OPMED SYMPTOMS:11123} the problem started {1-10:5044} {Time Units:10300}.
Any Medications that may need a refill? {YES/NO:63}
Current medications: ***
--------------------------------------------------------------------------------
Archie M Johnson
Community Health Program Assistant Chief
Family Practice & Community Medicine
(559) 221-1234
Lucas Gina Wed Jul 8, 2009 10:37 AM Pended
ELECTIVE NEUROLOGICAL SURGERY
HISTORY & PHYSICAL
CHIEF COMPLAINT: No chief complaint on file.
HISTORY OF PRESENT ILLNESS: Mary A Xxtestfbonilla is a ***
Past Medical History
Diagnosis Date
• Other Deficiency of Cell-Mediated Immunity
Def of cell-med immunity
• Erythema Multiforme
• Allergic Rhinitis, Cause Unspecified
Allergic rhinitis
• Unspecified Osteoporosis 12/8/2005
DEXA scan - 2003
• Esophageal Reflux 12/8/2005
priolosec, protonix didn't work, lost weight
• Primary Hypercoagulable State
MUTATION FACTOR V LEIDEN
• Unspecified Glaucoma 1/06
• OPIOID PAIN MANAGEMENT 1/24/2007
Patient is on opioid contract - see letter 1/24/2007
• Chickenpox with Other Specified Complications 2002
```

Verifiëren

Uw resultaten zullen verschillen, gebaseerd op de berichtacties die u voor uw DLP-beleid hebt ingesteld. Configureer en bevestig uw acties voor uw wasmachine met een review vanuit de GUI: **Mail Policy > DLP-beleidsaanpassingen > Berichtacties**.

In dit voorbeeld wordt de **Standaardactie** ingesteld op DLP-quarantaine in de beleidsquarantaine en om ook de onderwerpregel met het voorlopen van "[DLP-inbreuk]" te wijzigen.

De **mail_logs** moeten hier net zo uitzien als wanneer u de vorige inhoud als teste-mail verstuurt:

```
Wed Jul 30 11:07:14 2014 Info: New SMTP ICID 656 interface Management (172.16.6.165)
address 172.16.6.1 reverse dns host unknown verified no
Wed Jul 30 11:07:14 2014 Info: ICID 656 RELAY SG RELAY_SG match 172.16.6.1 SBRS
not enabled
Wed Jul 30 11:07:14 2014 Info: Start MID 212 ICID 656
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 From: <my_user@gmail.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 RID 0 To: <test_person@cisco.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 Message-ID
'<A85EA7D1-D02B-468D-9819-692D552A7571@gmail.com>'
Wed Jul 30 11:07:14 2014 Info: MID 212 Subject 'My DLP test'
Wed Jul 30 11:07:14 2014 Info: MID 212 ready 2398 bytes from <my_user@gmail.com>
```

```
Wed Jul 30 11:07:14 2014 Info: MID 212 matched all recipients for per-recipient
policy DEFAULT in the outbound table
Wed Jul 30 11:07:16 2014 Info: MID 212 interim verdict using engine: CASE spam
negative
Wed Jul 30 11:07:16 2014 Info: MID 212 using engine: CASE spam negative
Wed Jul 30 11:07:16 2014 Info: MID 212 interim AV verdict using Sophos CLEAN
Wed Jul 30 11:07:16 2014 Info: MID 212 antivirus negative
Wed Jul 30 11:07:16 2014 Info: MID 212 Outbreak Filters: verdict negative
Wed Jul 30 11:07:16 2014 Info: MID 212 DLP violation
Wed Jul 30 11:07:16 2014 Info: MID 212 quarantined to "Policy" (DLP violation)
Wed Jul 30 11:08:16 2014 Info: ICID 656 close
```

Van het traceringstool ziet u resultaten die op deze afbeelding voorkomen, wanneer u vorige inhoud in de tekst van het bericht gebruikt:

Data Loss Prevention Processing	
Result:	Matches Policy: HIPAA and HITECH Violation Severity: LOW (Risk Factor: 22)
Actions:	replace-header("Subject", "[DLP VIOLATION] $subject") quarantine("Policy")

Problemen oplossen

Zorg ervoor dat u het gewenste DLP-beleid hebt geselecteerd via **Mail Policy > DLP Policy Manager > Add DLP Policy...** in de GUI.

Controleer het DLP Policy zoals toegevoegd en zorg ervoor dat u de Content matching Classifier hebt opgegeven en dat uw patroon van reguliere expressies geldig is. Zorg er ook voor dat u **de** sectie **EN** aansluit **bij verwante woorden of zinnen** ingesteld hebt. Classificatoren zijn de detectieonderdelen van de DLP-motor. Ze kunnen in combinatie of afzonderlijk worden gebruikt om gevoelige inhoud te identificeren.

> Opmerking: Vooraf gedefinieerde classificatoren kunnen niet worden bewerkt.

Als u de DLP-trigger niet op de inhoud ziet gebaseerd, controleert u ook **Mail-beleid > OutDoorgaande Mail-beleid > DLP** en garandeert u dat het gewenste DLP-beleid ingeschakeld is.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- ESA FAQ: Hoe kan ik debug in hoe een bericht door het ESA wordt verwerkt?
- leaving SSA.gov: Misbruik van socialezekerheidsnummers
- Online regex tester
- Technische ondersteuning en documentatie – Cisco Systems