تصفية بريد ESA المنتحل

المحتويات

المقدمة

يصف هذا المستند مشكلة تتم مواجهتها على جهاز أمان البريد الإلكتروني من Cisco (ESA) عند دخول البريد العشوائي والبريد الإلكتروني الاحتيالي إلى الشبكة.

المشكلة

يحاول المحتالون انتحال صفة البريد الإلكتروني. عندما ينتحل البريد الإلكتروني صفة (من المفترض أنه من) أحد موظفي شركتك، فقد يكون خادعا بشكل خاص ويمكن أن يتسبب في حدوث إرباك. وفي محاولة لحل هذه المشكلة، قد يحاول مسؤولو البريد الإلكتروني حظر البريد الوارد الذي يبدو أنه ينشأ من داخل الشركة (البريد *المنتحل*).

قد يبدو من المنطقي أنه إذا قمت بحظر البريد الوارد من إنترنت الذي يحتوي على عنوان إرجاع الشركة في اسم المجال، فإنه يحل المشكلة. للأسف، عند حظر البريد بهذه الطريقة، يمكن أيضا حظر البريد الإلكتروني المشروع في الوقت نفسه. تأملوا في هذه الامثلة:

- يسافر الموظف ويستخدم موفر خدمة إنترنت فندقي (ISP) الذي يعيد توجيه كل حركة مرور بروتوكول نقل البريد البسيط (SMTP) بشفافية إلى خوادم بريد ISP. عند إرسال البريد، قد يبدو أنه يتدفق مباشرة من خلال خادم SMTP الخاص بالمؤسسة، ولكن يتم إرساله بالفعل من خلال خادم SMTP من جهة خارجية قبل تسليمه إلى المؤسسة.

- يشترك الموظف في قائمة مناقشة البريد الإلكتروني. عند إرسال الرسائل إلى قائمة البريد الإلكتروني، يتم إرجاعها إلى جميع المشتركين، من المنشئ على ما يبدو.

- يتم إستخدام نظام خارجي لمراقبة أداء الأجهزة المرئية خارجيا أو قابلية الوصول إليها. عند حدوث تنبيه، يحتوي البريد الإلكتروني على اسم مجال الشركة في عنوان الإرجاع. مزودو الخدمة من جهات خارجية، مثل WebEx، يفعلون ذلك بشكل متكرر إلى حد ما.

- بسبب خطأ في تكوين الشبكة المؤقت، يتم إرسال البريد من داخل الشركة عبر المصغي الوارد، بدلا من المصغي الصادر.

- يتلقى شخص ما خارج الشركة رسالة بأنه سيعيد إرسالها إلى الشركة مع وكيل مستخدم البريد (MUA) الذي يستخدم أسطر رأس جديدة بدلا من الرأس الأصلي.

- يستخدم تطبيق قائم على الإنترنت، مثل **صفحات الشحن** التابعة لشركة Federal Express أو **صفحة البريد الإلكتروني** لشركة Yahoo، لإنشاء بريد شرعي بعنوان إرجاع يشير إلى الشركة. البريد شرعي وله عنوان مصدر من داخل الشركة لكنه لا ينشأ من الداخل.

توضح هذه الأمثلة أنه إذا قمت بحظر البريد الوارد استنادا إلى معلومات المجال، فقد يؤدي ذلك إلى نتائج إيجابية خاطئة.

الحل

يصف هذا القسم الإجراءات الموصى بها التي يجب عليك تنفيذها لحل هذه المشكلة.

تطبيق عوامل التصفية

لتجنب فقدان رسائل البريد الإلكتروني الشرعية، لا تقم بحظر البريد الوارد استنادا إلى معلومات المجال. وبدلا من ذلك، يمكنك وضع علامة على سطر موضوع هذه الأنواع من الرسائل عند دخولها الشبكة، وهو ما يشير إلى المستلم أن الرسائل من المحتمل أن تكون مزورة. ويمكن تحقيق ذلك إما باستخدام عوامل تصفية الرسائل أو باستخدام عوامل تصفية المحتوى.

تتمثل الاستراتيجية الأساسية لهذه المرشحات في التحقق من خطوط رأس المتن ذات الخطوط الخلفية (البيانات **من** هي الأكثر أهمية)، بالإضافة إلى مرسل المغلف RFC 821. وتظهر خطوط الرأس هذه في أغلب الأحيان في MUAs وهي الخطوط التي يرجح أن يقوم شخص إحتيالي بتزييفها.

يوضح عامل تصفية الرسائل في المثال التالي كيفية وضع علامة على الرسائل التي يحتمل أن تكون منتحلة. يقوم هذا المرشح بتنفيذ عدة إجراءات:

- إذا كان سطر الموضوع يحتوي بالفعل **"{قد يكون** مزورا}"فيه، فلن تتم إضافة نسخة أخرى بواسطة عامل التصفية. وهذا مهم عند تضمين الردود في تدفق الرسائل، وقد ينتقل سطر موضوع عبر بوابة البريد عدة مرات قبل اكتمال مؤشر ترابط الرسالة.

- يبحث عامل التصفية هذا عن مرسل المظروف أو رأس **من** الذي يحتوي على عنوان ينتهي في اسم المجال **@yourdomain.com**. من المهم ملاحظة أن البريد من البحث غير حساس لحالة الأحرف تلقائيا، لكن البحث من رأس ليس كذلك. إذا تم العثور على اسم المجال في أي من الموقعين، يقوم عامل التصفية بإدراج **"{قد يكون مزيفا}"** في نهاية سطر الموضوع.
هنا مثال من المرشح:

```
:MarkPossiblySpoofedEmail

                if ( (recv-listener == "InboundMail")       AND
                   ( ("${\\subject != "\\{Possibly Forged)
                                                            }
                  if (mail-from == "@yourdomain\\.com$") OR
              ("header("From") == "(?i)@yourdomain\\.com)
                                                          }
                                  ;("strip-header("Subject
          ;("{insert-header("Subject", "$Subject {Possibly Forged
                                                          {
                                                             {
```

إجراءات إضافية

وبما انه لا توجد طريقة بسيطة للتعرف على البريد المنتحلة من البريد الشرعي، فلا توجد طريقة لإزالة المشكلة كليا. لذلك، توصي Cisco بتمكين المسح الضوئي المضاد للبريد العشوائي (IPAS) من IronPort، والذي يعرف بشكل فعال البريد الاحتيالي (الخداع) أو البريد العشوائي ويحظره بشكل إيجابي. يوفر إستخدام ماسح مكافحة البريد العشوائي هذا، عند اقترانه بالمرشحات الموصوفة في القسم السابق، أفضل النتائج دون فقدان البريد الإلكتروني المشروع.

إذا كان ينبغي عليك تحديد رسائل البريد الإلكتروني الاحتيالية التي تأتي إلى شبكتك، فعليك إذن مراعاة إستخدام تقنية البريد المعرف لمفاتيح المجال (DKIM)؛ فهي تتطلب المزيد من الإعداد، ولكنها تعد مقياس جيد ضد التصيد الاحتيالي ورسائل البريد الإلكتروني الاحتيالية.

ملاحظة: للحصول على مزيد من المعلومات حول عوامل تصفية الرسائل، ارجع إلى **دليل مستخدم AsyncOS** في صفحة دعم جهاز أمان البريد الإلكتروني من Cisco.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).