Filtro posta falsificata ESA

Sommario

Introduzione

In questo documento viene descritto un problema che si verifica in Cisco Email Security Appliance (ESA) quando nella rete vengono introdotti spam e posta elettronica fraudolenta.

Problema

I truffatori tentano di rappresentare la posta elettronica. Quando l'e-mail rappresenta (si presume provenga da) un membro dello staff aziendale, può essere particolarmente ingannevole e può causare confusione. Nel tentativo di risolvere questo problema, gli amministratori della posta elettronica potrebbero tentare di bloccare la posta in arrivo che sembra provenire dalla società (posta *falsificata*).

Potrebbe sembrare logico bloccare la posta in arrivo da Internet il cui nome di dominio contiene l'indirizzo del mittente della società per risolvere il problema. Sfortunatamente, quando si blocca la posta in questo modo, può anche bloccare la posta elettronica legittima allo stesso tempo. Considerate questi esempi:

- Un dipendente viaggia e utilizza un provider di servizi Internet (ISP) dell'hotel che reindirizza in modo trasparente tutto il traffico SMTP (Simple Mail Transfer Protocol) ai server di posta dell'ISP. Quando la posta viene inviata, è possibile che venga inoltrata direttamente attraverso il server SMTP dell'organizzazione, ma in realtà viene inviata tramite un server SMTP di terze parti prima di essere consegnata all'organizzazione.

- Un dipendente si iscrive a un elenco di discussione tramite e-mail. I messaggi inviati all'elenco e-mail vengono restituiti a tutti i sottoscrittori, apparentemente dal mittente.

- Un sistema esterno viene utilizzato per monitorare le prestazioni o la raggiungibilità dei dispositivi visibili esternamente. Quando si verifica un avviso, il messaggio di posta elettronica include il nome di dominio della società nell'indirizzo del mittente. I provider di servizi di terze parti, ad esempio WebEx, eseguono questa operazione con una certa frequenza.

- A causa di un errore temporaneo di configurazione della rete, la posta proveniente dall'interno della società viene inviata tramite il listener in entrata anziché tramite il listener in uscita.

- Un utente esterno all'azienda riceve un messaggio che inoltra all'azienda con un Mail User

Agent (MUA) che utilizza nuove righe di intestazione anziché l'intestazione originale.

- Un'applicazione basata su Internet, ad esempio le **pagine di spedizione di** Federal Express o l'indirizzo di **posta elettronica di** Yahoo per **questa** pagina di **articolo**, crea messaggi legittimi con un indirizzo di ritorno che rimanda all'azienda. La posta è legittima e ha un indirizzo di origine interno all'azienda, ma non ha origine all'interno.

Questi esempi mostrano che se si blocca la posta in arrivo in base alle informazioni di dominio, potrebbero verificarsi falsi positivi.

Soluzione

In questa sezione vengono descritte le azioni consigliate da eseguire per risolvere il problema.

Applicazione dei filtri

Per evitare la perdita di messaggi e-mail legittimi, non bloccare la posta in arrivo in base alle informazioni del dominio. È invece possibile contrassegnare la riga dell'oggetto di questi tipi di messaggi quando entrano nella rete, per indicare al destinatario che i messaggi potrebbero essere contraffatti. A tale scopo, è possibile utilizzare filtri messaggi o filtri contenuti.

La strategia di base per questi filtri è controllare le linee di intestazione del corpo appuntite all'indietro (i dati **From** sono i più importanti), così come il mittente della busta RFC 821. Queste linee di intestazione vengono comunemente visualizzate nei MUA e sono quelle che con maggiore probabilità vengono falsificate da una persona fraudolenta.

Il filtro messaggi illustrato nell'esempio seguente mostra come contrassegnare i messaggi potenzialmente rappresentati. Questo filtro esegue diverse azioni:

- Se la riga dell'oggetto contiene già **"{Possibly Forged}"**, il filtro non aggiungerà un'altra copia. Questo è importante quando le risposte sono incluse nel flusso di messaggi e una riga dell'oggetto potrebbe spostarsi nel gateway di posta diverse volte prima del completamento di un thread di messaggi.

- Questo filtro cerca l'intestazione Busta mittente o **Da** con un indirizzo che termina con il nome di dominio **@dominio.com**. È importante notare che la ricerca da-posta non fa automaticamente distinzione tra maiuscole e minuscole, mentre la ricerca da-intestazione non fa distinzione. Se il nome di dominio viene trovato in una delle due posizioni, il filtro inserisce **"{Possibly Forged}"** alla fine della riga dell'oggetto.

Di seguito è riportato un esempio del filtro:

```
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}");
```

```
    }
}
```

Misure aggiuntive

Poiché non esiste un modo semplice per identificare la posta falsificata dalla posta legale, non esiste un modo per eliminare del tutto il problema. Pertanto, Cisco consiglia di abilitare IronPort Anti-Spam Scanning (IPAS), che identifica efficacemente la posta fraudolenta (phishing) o lo spam e lo blocca in modo positivo. L'uso di questo scanner antispam, se abbinato ai filtri descritti nella sezione precedente, fornisce i migliori risultati senza la perdita di e-mail legittime.

Se devi identificare e-mail fraudolente che entrano nella tua rete, prendi in considerazione l'uso della tecnologia DKIM (Domain Keys Identified Mail); richiede una maggiore configurazione, ma è una buona misura contro il phishing e le e-mail fraudolente.

> **Nota:** Per ulteriori informazioni sui filtri messaggi, consultare la **Guida dell'utente di AsyncOS** nella pagina di supporto di Cisco Email Security Appliance.