opentext™

Mascheramento dei dati sensibili con Reflection Desktop

La maggior parte delle violazioni della riservatezza dei dati è collegata a una persona di fiducia: il dipendente sanitario che vende i dettagli dei VIP ai tabloid. Un dipendente addetto alla contabilità fornitori che modifica in modo inappropriato le informazioni di fatturazione. Un cassiere di banca che comunica i codici fiscali o i numeri delle carte di credito rubati ai suoi complici. Oggi, può essere difficile distinguere tra un dipendente onesto e un impostore disonesto.

Panoramica di Reflection Desktop

- **Connettività:**
  Collegate gli utenti di computer desktop e mobili ai sistemi host.
- **Facilità di utilizzo:**
  Rendete le applicazioni host facili da usare quanto quelle Office.
- **Facilità di gestione:**
  Gestite facilmente le configurazioni utente.
- **Sicurezza:**
  Utilizzate i livelli di sicurezza per proteggere i dati in movimento e quelli inattivi.

Questo opuscolo sul prodotto descrive in che modo il software OpenText™ Reflection Desktop può aiutare a prevenire le violazioni della privacy dei dati, senza dover apportare modifiche alle applicazioni host.

Perché gli utenti interni malintenzionati la fanno franca

Le frodi interne sono difficili da individuare. I controlli tradizionali, incentrati sulla prevenzione degli attacchi dall'esterno, sono impotenti contro gli esperti utenti interni che dispongono dell'accesso legittimo a dati riservati.

Se un utente interno scontento o disonesto dispone dei necessari privilegi di accesso, il rischio di cattiva condotta aumenta notevolmente. Nell'ultimo anno documentato, le organizzazioni statunitensi hanno perso 40 miliardi di dollari per furti e frodi da parte di dipendenti. Secondo la società di ricerche di mercato Forrester, il 46% di quasi 200 responsabili decisionali del settore tecnologico ha indicato le violazioni interne come il tipo più comune di violazione riscontrato nell'ultimo anno e la metà degli intervistati ha dichiarato che tali violazioni sono state effettuate da utenti interni malintenzionati*.

Perché le organizzazioni non hanno fatto di più per proteggersi? La risposta è semplice: cambiare le applicazioni host consolidate per renderle più sicure è difficile, rischioso e costoso. Anche se siete abbastanza fortunati da trovare un esperto che conosca le piattaforme mainframe, è pericoloso modificare la logica aziendale, scritta e sviluppata nel tempo, su cui si basa la gestione dell'azienda. Le implicazioni in termini di costi e interruzioni sono proibitivamente elevate.

Un primo semplice passo

La domanda è: in che modo è possibile proteggere i clienti e l'azienda senza rinnovare sistemi host e processi aziendali consolidati nel corso di decenni? Come è possibile proiettare l'azienda nel nuovo mondo della sicurezza?

In generale, è necessario aggiungere ulteriori livelli di protezione. Si tratta di un approccio basato su best practice che è possibile effettuare a fasi. Nell'ambiente dei mainframe IBM e AS/400, c'è un primo semplice passo da compiere: si tratta del mascheramento dei dati.

Il mascheramento dei dati consente di impedire agli utenti di visualizzare i dati sensibili su una schermata host, copiarli su un pezzo di carta, fotografarli, stamparli o inviarli tramite posta elettronica. Tale funzione nasconde i dati sulla schermata in tempo reale, in modo che i dipendenti non possano mai visualizzare per intero un indirizzo, una data di nascita, un numero di carta di credito, un codice fiscale o eventuali altre informazioni private. Quello che i dipendenti vedono è solo ciò che serve per svolgere il loro lavoro. Tutto qui.

Tecnologia Reflection Information Privacy

Se siete clienti di Reflection Desktop, le funzionalità di mascheramento dei dati sono già nelle vostre mani. La tecnologia di mascheramento dei dati di OpenText™ Reflection Enterprise Suite vi consente di mascherare facilmente

*Keanini, TK. (2015) Perché le minacce interne sono ancora presenti. Information Age. Recuperato il 25 gennaio 2016 da: **www.information-age.com/technology/security/123459548/why-insider-threats-are-still-succeeding***

qualsiasi tipo di dati sugli schermi host, senza apportare modifiche sul lato host.

Il mascheramento dei dati di Reflection Enterprise Suite viene realizzato attraverso l'uso di filtri per la privacy e regole PAN (Primary Account Number) all'interno dello strumento Reflection Information Privacy:

- **Filtri per la privacy**: è possibile creare filtri per la privacy personalizzati che consentono di mascherare i dati sulle schermate host delle applicazioni mainframe IBM e AS/400. È anche possibile applicare diverse regole a questi filtri, per mascherare i dati non appena vengono visualizzati, digitati e spostati su un'altra schermata (stampa schermo, copia/incolla e screen scraping con API/macro).
- **Regole PAN**: con le regole PAN è possibile configurare Reflection in modo da mascherare per intero o in parte un numero di carta di credito su una schermata host selezionando le caselle appropriate. Reflection Enterprise Suite utilizza una tecnologia in attesa di brevetto per identificare e convalidare i PAN. Utilizza inoltre l'algoritmo Luhn per garantire che tutti i numeri di carta di credito siano nascosti dalla vista indipendentemente da dove o come vengano visualizzati. Gli utenti e gli amministratori possono scegliere una gamma di opzioni di controllo, dal riconoscimento base della carta di credito a personalizzazioni complesse, per soddisfare le proprie esigenze aziendali.

Di seguito, sono riportati alcuni esempi di ciò che sono stati in grado di fare i clienti OpenText™ utilizzando i filtri per la privacy di Reflection Enterprise Suite e le regole PAN:

- Mascherare un'intera colonna di dati.
- Mascherare i campi dei dati finanziari personali.
- Mascherare solo le ultime sei cifre di un campo a lunghezza variabile.
- Mascherare un campo di dati che viene visualizzato in più posizioni sulla stessa schermata.
- Mascherare i dati in base alle istanze condizionali di base (ad es., in base ai campi di dati o agli identificatori di schermata).
- Mascherare i dati in base a istanze condizionali complesse (ad es., utilizzando le condizioni di tipo if, then ed else).
- Mascherare diversi PAN, compresi quelli con lunghezze, prefissi e posizioni del trattino diversi.
- Mascherare dati visualizzati tra due valori separati.
- Fornire diversi livelli di visibilità in base al ruolo o alla funzione lavorativa dell'utente.

Le funzionalità di mascheramento dei dati di Reflection Enterprise Suite sono inarrivabili per qualsiasi altro client di emulazione terminale e forniscono inoltre una soluzione a basso rischio che è possibile implementare facilmente. Per saperne di più sulla configurazione della privacy delle informazioni con Reflection Desktop, consultate **https://docs.attachmate.com/reflection/16.0/info-privacy.pdf**.

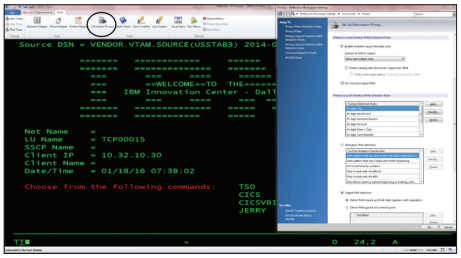

Figura 1. I filtri e le regole vengono memorizzati nei file, facilitando la gestione in base al ruolo o al gruppo di utenti.

Il cambiamento nel panorama delle minacce

Ogni organizzazione deve affrontare questa sconcertante verità: entro le sue mura ci sono persone che possono utilizzare i propri diritti di accesso privilegiati per commettere dannose violazioni della privacy. Ma gli approcci tradizionali alle nuove minacce perpetrate da utenti interni sempre più sofisticati non funzionano più. La strategia di gestione dei rischi deve evolvere per essere efficace.

Le funzionalità di mascheramento dei dati integrate di Reflection Enterprise Suite rappresentano un passo nella giusta direzione di facile implementazione e a basso rischio. Queste funzionalità consentono di proteggere i dati e, contemporaneamente, agevolano la conformità alle normative senza richiedere la riscrittura delle applicazioni host.

Scoprite di più su
www.opentext.com

Mettetevi in contatto con noi

Compatibilità con PCI DSS

Lo strumento per la privacy delle informazioni Reflection fa molto di più che mascherare i dati sulle schermate host. Solo selezionando le caselle appropriate, è possibile richiedere connessioni crittografate su tutte le reti, comprese le reti wireless. È possibile tenere traccia della visualizzazione dei numeri di carta di credito da parte di qualsiasi utente. Inoltre, è possibile generare rapporti dettagliati in base alle esigenze. In tali modi, lo strumento consente di agevolare la conformità allo standard PCI DSS. Per saperne di più, visitate il sito Web **www.attachmate.com/library/docs/advance-your-pci-compliance-with-reflection-desktop.html**.

opentext™