Produkt-Flyer

opentext™

Maskieren vertraulicher Daten mit Reflection Desktop

Die meisten Datenschutzverletzungen sind auf Menschen zurückzuführen, denen Sie vertrauen: Zum Beispiel der Mitarbeiter im Gesundheitswesen, der Informationen über Prominente an die Boulevardpresse verkauft. Oder der Beschäftigte in der Buchhaltung, der unangemessen Rechnungsinformationen ändert. Oder ein Bankangestellter, der gestohlene Sozialversicherungs- oder Kreditkartennummern an Mittäter weitergibt. Heutzutage kann es sich schwierig gestalten, einen integren Mitarbeiter von einem hinterlistigen Betrüger zu unterscheiden.

Reflection Desktop auf einen Blick

- **Konnektivität:**
  Verbinden Sie die Desktop- und mobilen Benutzer mit den Hostsystemen.
- **Benutzerfreundlichkeit:**
  Sorgen Sie dafür, dass sich Hostanwendungen so einfach wie Office-Anwendungen verwenden lassen.
- **Verwaltungsfreundlichkeit:**
  Verwalten Sie mit Leichtigkeit die Benutzerkonfigurationen.
- **Sicherheit:**
  Nutzen Sie mehrere Sicherheitsebenen, um Daten im Speicher und bei der Übertragung zu schützen.

In diesem Produktflyer erfahren Sie, wie die OpenText Reflection Desktop-Software Ihnen dabei helfen kann, Datenschutzverletzungen vorzubeugen – ohne dafür Änderungen an Ihren Hostanwendungen vornehmen zu müssen.

Warum böswillige Insider freie Hand haben

Betrug durch Insider ist schwer festzustellen. Die herkömmlichen Kontrollen, die sich auf die Abwehr von externen Attacken konzentrieren, sind gegen gerissene Insider mit rechtmäßigem Zugriff auf sensible Daten machtlos.

Wenn ein verärgerter oder betrügerischer Insider über die nötigen Zugriffsprivilegien verfügt, steigt das Risiko von Fehlverhalten. Im letzten Jahr erlitten Unternehmen in den USA aufgrund von Diebstahl oder Betrug durch Mitarbeiter Einnahmeverluste von 40 Milliarden US-Dollar. Gemäß dem Marktforschungsunternehmen Forrester gaben 46 Prozent der fast 200 zitierten Entscheidungsträger aus dem Technologiebereich an, dass interne Verstöße der häufigste Typ von Pflichtverletzungen seien, die sie im vergangenen Jahr erlebt hätten. Die Hälfte dieser Befragten sagte, dass böswillige Insider für diese Verstöße verantwortlich waren.*

Warum tun Organisationen nicht mehr, um sich zu schützen? Ganz einfach: Die Änderung etablierter Hostanwendungen zur Steigerung der Sicherheit ist schwierig, riskant und kostspielig. Selbst wenn Sie das Glück haben, einen Experten ausfindig zu machen, der sich mit den Mainframe-Plattformen auskennt, ist es gefährlich, die Geschäftslogik, auf das sich Ihr Unternehmen stützt und die im Laufe der Zeit aufgebaut und erweitert wurde, umzuschreiben. Die damit verbundenen Kosten und Ausfallzeiten sind unannehmbar hoch.

Ein einfacher erster Schritt

Die große Frage ist: Wie können Sie Ihre Kunden und Ihr Unternehmen schützen, ohne die Hostsysteme und Geschäftsprozesse, die auf jahrzehntelanger Entwicklung basieren, neu zu gestalten? Wie können Sie Ihr Unternehmen in die moderne Welt der Sicherheit befördern?

Allgemein ausgedrückt benötigen Sie weitere Sicherheitsebenen. Dies ist ein bewährtes Verfahren, das Sie schrittweise ausführen können. In der Welt von IBM Mainframe und AS/400 existiert ein einfacher erster Schritt, den Sie dazu unternehmen können. Dieser nennt sich Datenmaskierung.

Datenmaskierung gibt Ihnen die Möglichkeit, Benutzer davon abzuhalten, sensible Daten auf einem Hostbildschirm anzusehen, diese auf ein Blatt Papier zu kopieren, abzufotografieren, zu drucken oder per E-Mail zu versenden. Dabei werden die Daten in Echtzeit auf dem Bildschirm maskiert, sodass Mitarbeiter niemals eine vollständige Adresse, ein Geburtsdatum, eine Kreditkartennummer, Sozialversicherungsnummer oder jede andere persönliche Information zu Gesicht bekommen. Was ihnen angezeigt wird, ist gerade genug, damit sie ihre Arbeit erledigen können. Nicht mehr und nicht weniger.

Reflexion Information Datenschutztechnologie

Wenn Sie Reflection Desktop-Kunde sind, stehen Ihnen bereits Funktionen zur Datenmaskierung

---

* *Keanini, TK. (2015). Why insider threats are still succeeding. Information Age. Abgerufen am 25. Januar 2016 unter:* **www.information-age.com/technology/security/123459548/why-insider-threats-are-still-succeeding**

zur Verfügung, die nur einen Mausklick entfernt sind. Die Datenmaskierungstechnologie der OpenText Reflection Enterprise Suite befähigt Sie dazu, jeden Datentyp auf Hostbildschirmen auf einfache Weise zu maskieren – ohne Änderungen auf Seiten des Hosts durchführen zu müssen.

Die Datenmaskierung der Reflection Enter-prise Suite wird durch den Einsatz von Datenschutz-filtern und Primary Account Number (PAN)-Regeln innerhalb des Reflection Information Privacy Tools erreicht:

- **Datenschutzfilter** – Sie können benutzerdefinierte Datenschutzfilter erstellen, mit deren Hilfe Sie Daten auf IBM Mainframe- und AS/400-Anwendungs-Hostbildschirmen maskieren können. Sie können außerdem verschiedene Regeln auf diese Filter anwenden – und so Daten maskieren, während sie angezeigt, getippt und vom Bildschirm kopiert werden (Druckansicht, Kopieren/Einfügen und Screen Scraping mit API/Makros).
- **PAN-Regeln** – Mithilfe von PAN-Regeln können Sie Reflection so konfigurieren, dass es Kreditkartennummern oder Teile davon auf einem Hostbildschirm maskiert, indem Sie die entsprechenden Kontrollkästchen aktivieren. Reflection Enterprise Suite nutzt zum Patent angemeldete Technologie, um PANs zu identifizieren und bestätigen. Außerdem setzt es den Luhn-Algorithmus ein, um sicherzustellen, dass alle Kreditkartennummern verborgen bleiben, unabhängig davon, wo oder wie sie angezeigt werden. Benutzer und Administratoren können entsprechend ihren Geschäftsanforderungen aus einer Reihe von Kontrollmöglichkeiten auswählen – von grundlegender Kreditkartenerkennung bis zu komplexen Anpassungen.

Hier sind einige Beispiele dafür, für welche Zwecke OpenText Kunden die Datenschutzfilter und PAN-Regeln der Reflection Enterprise Suite einsetzen:

- Maskierung einer gesamten Datenspalte.
- Maskierung von Feldern mit persönlichen Finanzinformationen.
- Maskierung der letzten sechs Stellen eines Feldes von variabler Länge.
- Maskierung eines Datenfeldes, das an mehreren Stellen auf demselben Bildschirm erscheint.
- Maskierung von Daten auf Basis grundlegender Bedingungen (z. B. basierend auf Datenfeldern oder Bildschirmidentifikatoren).
- Maskierung von Daten auf Basis komplexer Bedingungen (z. B. vom Typ wenn, dann, sonst).
- Maskierung verschiedener PANs einschließlich solchen mit unterschiedlichen Längen, Präfixen und Bindestrichpositionen.
- Maskierung von Daten, die zwischen zwei separaten Werten angezeigt werden.
- Anzeige verschiedener Sichtbarkeitsebenen auf Basis der Rolle oder Stellenbezeichnung des Benutzers.

Reflection Enterprise Suite bietet unübertroffene Funktionen zur Datenmaskierung, die von keinem anderen Terminalemulation-Client erreicht werden. Dadurch wird Ihnen eine risikoarme Lösung geboten, die leicht implementiert werden kann. Weitere Informationen zur Einrichtung von Datenschutz mithilfe von Reflection Desktop erhalten Sie unter **http://docs.attachmate.com/reflection/16.0/info-privacy.pdf**.

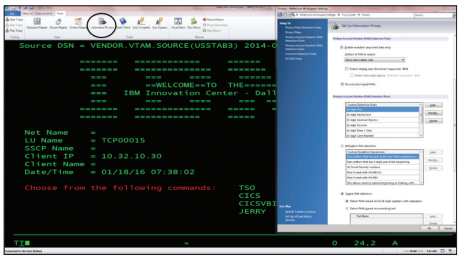

Abbildung 1. Filter und Regeln werden als Dateien abgespeichert, sodass eine einfache Verwaltung nach Rolle oder Benutzergruppe möglich ist.

Eine veränderte Bedrohungslandschaft

Die unbequeme Wahrheit ist: Jede Organisation hat unter ihrem Dach Menschen, die ihre privilegierten Zugriffsrechte dazu missbrauchen, böswillig Datenschutzverletzungen zu begehen. Gegen die neuen Bedrohungen, die von zunehmend raffinierteren Insidern ausgehen, haben herkömmliche Ansätze keine Chance mehr. Ihre Risikomanagementstrategie kann nur effektiv sein, wenn Sie sie weiterentwickeln.

Die in der Reflection Enterprise Suite integrierten Funktionen zur Datenmaskierung bieten Ihnen einen risikoarmen, einfach zu implementierenden Schritt in die richtige Richtung. Sie schützen Ihre Daten und erleichtern gleichzeitig die Einhaltung von Vorschriften, ohne die Hostanwendungen umprogrammieren zu müssen.

Erfahren Sie mehr unter **www.opentext.com**

Stets das Neueste erfahren

Einhaltung von PCI DSS-Bestimmungen

Das Reflection Information Privacy Tool kann noch mehr, als Daten auf Hostbildschirmen zu maskieren. Durch die Aktivierung der richtigen Kontrollkästchen können Sie verschlüsselte Verbindungen auf allen Netzwerken einschließlich drahtloser Netzwerke festlegen. Sie können nachverfolgen, wenn Kreditkartennummern von Benutzern angezeigt werden. Außerdem können Sie bedarfsgerecht detaillierte Berichte generieren. Auf diese Weise hilft Ihnen das Tool dabei, PCI DSS-Anforderungen einzuhalten. Weitere Informationen erhalten Sie unter: **www.attachmate.com/library/docs/advance-your-pci-compliance-with-reflection-desktop.html**.

opentext™