informare scheda

Fujitsu assicurato il controllo e il monitoraggio di SAP

assicurato il controllo e monitoraggio delle attività di SAP che utilizzano l'autenticazione biometrica software Fujitsu PalmSecure ™ e Biolock ™ di AG in tempo reale.

Gestione di identificazione

Nella nostra società delle reti onnipresenti, in cui gli individui possono facilmente accedere alle loro informazioni in qualsiasi momento e ovunque, siamo anche di fronte al rischio che gli altri possono facilmente accedere alle stesse informazioni - sempre e ovunque. A causa di questo rischio, la tecnologia di identificazione personale in grado di distinguere tra gli utenti e, impostori legittimi registrati sta generando un crescente interesse. Tradizionale (password) di sicurezza basata sulla conoscenza, non si riunisce questa sfida, se un utente sta lavorando su un dispositivo dedicato o soprattutto quando più utenti accedono a SAP tramite un dispositivo condiviso come un chiosco o registratore di cassa.

Fujitsu ha sviluppato una tecnologia di autenticazione di palma vene senza contatto chiamato Fujitsu PalmSecure ™. La tecnologia PalmSecure di Fujitsu utilizza il modello della vena molto complesso nel palmo della vostra mano per garantire la sicurezza delle informazioni. Il tuo modello palma vena rimane lo stesso per tutta la vita ed è diversa per la mano sinistra e destra. Più di cinque milioni di punti di riferimento del modello della vena vengono catturati dal sensore PalmSecure estremamente preciso. Vena tecnologia di riconoscimento è una delle soluzioni più sicure perché i dati di autenticazione è all'interno del vostro corpo nel sistema circolatorio, che rende molto difficile da contraffare. Smart card, nomi utente e numeri di identificazione possono essere rubati, da copiare o dimenticato; caratteristiche biometriche sono unici e fissata ad una persona. Questo contatto, sistema igienico offre la massima sicurezza e la massima precisione.

Fujitsu PalmSecure ™ e in tempo reale Biolock ™

Investire in accesso biometrico, sicurezza a più livelli perimetrale e può meglio proteggere i dati SAP di un'organizzazione da frodi interne finanziaria, violazioni della privacy, spionaggio industriale, la perdita di dati o l'accesso non autorizzato ai proprietà intellettuale, mentre aumenta la conformità alle normative.

Protezione per SAP

SAP è la soluzione ERP leader di mercato utilizzato da grandi organizzazioni. L'unico programma di sicurezza biometrico disponibile che è perfettamente integrato e certificato per SAP® e Hana è un software Biolock ™ da SAP Gold Partner in tempo reale AG.

Combinato con Fujitsu PalmSecure l'approccio per la sicurezza è quello di controllare ciò che accade all'interno di SAP non solo al momento del log-on, ma soprattutto dopo che l'utente si trova nel sistema. SAP si basa normalmente sulle autorizzazioni basate su ruoli, i protocolli di processo Single Sign-On e GRC per impedire la separazione delle funzioni violazioni a seguito di un log-on a base di semplice password. Purtroppo, queste tecniche non offrono alcuna protezione dagli abusi di impostore di password che sono stati rubati, indovinate o volontariamente condivisi. Le password da solo non può legare una attività di SAP ad un utente specifico per creare la responsabilità o per far rispettare assolutamente una regola. Fortunatamente, i miglioramenti di sicurezza drammatici in SAP sono possibili mediante l'attuazione rigorosa biometrica ri-autenticazione a livello granulare, che diventano punti di controllo specifici per l'utente. Perché queste ri-autenticazione si basano sulla gestione dell'identità biometrica legata alle credenziali dell'utente ("Chi sei" sicurezza) al posto di password ("ciò che si sa" di sicurezza) o dispositivi ("quello che hai" sicurezza), i risultati sono di revisione indiscutibili sentieri e responsabilità.

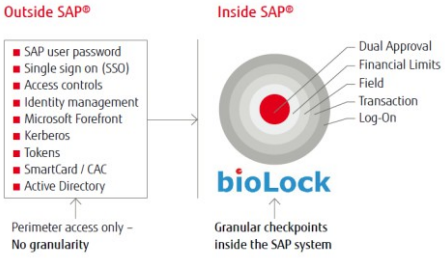
Oltre alla protezione contro le frodi fornito, questo aiut anche a garantire il rispetto delle varie normative governative, che di solito fanno molto affidamento su forte audit trail o la registrazione delle attività.

Come funziona

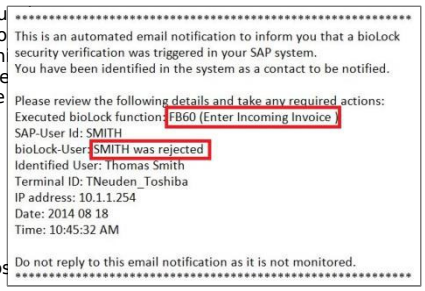
Con Biolock, sicurezza check-point personalizzabili possono essere stabiliti sulla base di politiche di gestione e regole di business su una base user-by-user. Questi punti di controllo autenticazione possono essere fissati a livelli molto granula se necessario, come le voci di menu, le tabelle, le operazion fior di informazioni, i campi, i valori dei campi, pulsanti o og volta che un'attività critica viene eseguita all'interno di SAP Azioni come l'esportazione dei dati, i dati di stampa, il salvataggio dei dati, i dati che cambiano e di dati di visualizzazione dei corsi possono essere tutti controllati. Questo potrebbe proteggere qualsiasi cosa che coinvolgonc dati sensibili o privati, grandi quantità di denaro, o qualsias informazioni mission-critical che sarebbe di valore a person non autorizzate in caso di furto. Su un utente per utente, si in grado di:

- Limitare l'accesso del tutto a una determinata voce di menu o schermo
- "Maschera" settori sensibili di dati in quello schermo in modo che tali campi non popoleranno per un utente con credenziali insufficienti
- Impostare i valori di campo di soglia che non possono essere superati
- Disattivare i pulsanti per salvare, stampare o esportare
- Richiede la presenza di un utente biometrico secondo credentialed

Ecco cosa intendiamo per granularità all'interno del sistema SAP:



Con Biolock, una data funzione granulare (es: ME54N, u
richiesta di acquisto) può essere al 100% "bloccato", co
l'eccezione del nome ("bianche quotate") gli utenti. Ch
altro tentativo la funzione sarà respinto, e non può acce
prescindere dal loro livello pre-Biolock di autorizzazione



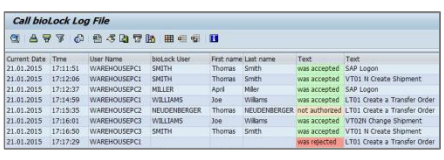
Come esempi, se un impiegato sta trasferendo una gros
somma di denaro, o la creazione di un nuovo account
venditore, o l'apertura di file di un cliente con tutte le loro
informazioni personali (PII) visibile, queste attività sono
abbastanza critica da richiedere biometrico ri-
autenticazione.

Questo può realizzare diversi obiettivi:

- Assolutamente impedire a un utente di accedere ad aree non autorizzate.
- Creare vera responsabilità per le azioni di ciascun utente.
- Applicare ogni separazione dei compiti, o di controlli ed equilibri ritenuti necessari dalle regole GRC dell'organizzazione, la gestione del rischio d'impresa o di disposizioni regolamentari.
- Generare un audit trail robusta con le notifiche di attività degli utenti, inclusi i tentativi di accesso non riusciti.
- Fornire i datori di lavoro munizioni legale per perseguire i dipendenti disonesti.

Esistenti SAP di sicurezza, i ruoli e le autorizzazioni sono invariati - complementi software Biolock ™ e rafforza la sicurezza SAP esistente e GRC.

Mentre, transazioni standard di log-on o info-tipi sono protetti da una semplice configurazione, i punti di controllo più avanzati possono essere impostati tramite il codice ABAP (Z-transazioni, uscite sul campo, miglioramenti o modifiche al codice di SAP). Posti di blocco sono perfettamente e in modo invisibile interposte nella logica di business SAP per innescare ri-autenticazione. Gli utenti finali non hanno accesso al codice checkpoint. A prova di manomissione informazioni del file di registro è a disposizione di strumenti di verifica e può silenziosamente avvisare un supervisore per tentativi di frode via e-mail:



Sindaci possono ora dimostrare che persona ha esaminato il bilancio, ha cambiato un ordine di acquisto, ha esportato la lista dei clienti, a cura di un numero di previdenza sociale o ha fatto un grande bonifico bancario in un paese straniero. Sicurezza non è più un insieme consigliato di protocolli, ma una procedura applicata rigorosamente che impedisce le frodi relative alle password e la rappresentazione dell'utente.

Amministrazione di sistema

I dipendenti possono essere iscritti in Biolock in pochi minuti, con entrambe i modelli di palma memorizzate e con l'aggiunta opzionale di una smart card. Questo stabilisce il modello Biolock di riferimento. Ulteriori informazioni possono essere raccolte e memorizzate con il record utente Biolock (separato dal record utente SAP), come ad esempio l'intervallo di date di validità del modello biometrico. accesso biometrico può essere pre-impostato per scadere in una determinata data, evitando così "lavoratori fantasma" (ex dipendenti, collaboratori, utenti temporanei). le credenziali biometriche sono assegnati a ogni utente che definisce l'ambito di attività consentiti o proibiti.

Altre opzioni includono restrizioni sulla nazionalità dell'utente e l'intervallo di indirizzi IP che dovrebbero essere l'accesso al sistema SAP da. Ecco un esempio nel file di log generato automaticamente i risultati di utenti che accedono a:

scansione biometrica

La biometria in forma di scansione palmo della vena viene utilizzato ai controlli di sicurezza. Il Fujitsu PalmSecure palm vena scanner sono utilizzati, sia attaccato come un disposit USB, integrato in un topo Fujitsu, collegato a un chiosco o registratore di cassa. PalmSecure utilizza algoritmi di estrazione e di corrispondenza proprietarie di Fujitsu.

Quando viene eseguita una scansione di palma vene, i dati biometrici dell'utente viene crittografata per la sicurezza. la privacy di un utente è quindi sempre protetto e le immagin biometriche attuali non sono mai memorizzati, in modo da alleviare problemi di privacy.

Una scansione iniziale di iscriversi a un utente consiste nel prendere diverse letture per stabilire una linea di base med Una volta iscritti, un utente esperienze solo un'interruzione momentanea quando gli viene chiesto di ri-autenticazione. processo di ri-autenticazione richiede al massimo alcuni secondi, a seconda della velocità di connessione al server. Indipendentemente dal profilo utente SAP che sembra esse arruolamento, Biolock sarà veramente identificare l'utente effettivo basato sulla biometria. A seconda che gli utenti hanno le credenziali appropriate, o come una determinata attività è limitato, possono essere accettate o rifiutate.

Come è concesso in licenza Biolock ™

Il prodotto è concesso in licenza a livelli utente che si laureano fino a una licenza a livello aziendale. Oltre agli utenti denominati, benefici si estendono agli utenti monitorati passivi, che di fatto non interagiscono con il software ancora sono protetti da esso. In Biolock ogni funzione protetta può essere bloccato a livello globale verso il basso, il che significa solo gli utenti specificamente accreditati possono accedere a tale funzione, anche se sono un amministratore o un altro tipo di utente di alimentazione

Esempio: se 500 dipendenti nominati su

3.500 hanno il potere di eseguire SAP funzioni finanziarie, g altri 3.000 utenti sono specificamente esclusi dalle funzioni finanziarie e non sarebbero in grado di fare qualsiasi attività di finanziamento, (anche con un amministratore, DDIC o la password "vigile del fuoco"), a meno che non abbiano una credenziale biometrica . Anche se i 3.000 utenti sono passiv Biolock protegge e

controlla l'intero sistema SAP contro

attività non autorizzate da qualsiasi utente passivo. Ciò si applica a qualsiasi funzione SAP che si sceglie di controllare. Gli ex dipendenti, revisori, consulenti e potenziali intrusi saranno tagliati fuori.

Pertanto, anche se la quota di licenza del software appare per coprire solo gli utenti di nome, in realtà il costo di proprietà dovrebbe essere vista come la diffusione su tutta la base di utenti SAP protetto se gli utenti di nome o passivi. In aggiunta al canone iniziale, una manutenzione annuale copre il supporto, correzioni di bug, nuove versioni e la documentazione.

Implementazione

Il software viene installato tramite trasporti nel suo proprio spazio dei nomi in SAP. le versioni di SAP HANA attuali, tra cui sono supportati, oltre a funzionalità limitata nelle versioni più vecchie di SAP. Il software Biolock risiede nel sistema SAP protetto dietro un "firewall biometrica", che significa dopo l'installazione si può accedere solo con la doppia verifica dei due utenti biometrici di fiducia ("doppia autenticazione").

Gli utenti possono essere iscritti in Biolock in pochi minuti, opzionalmente catturando alcune delle informazioni del profilo utente da SAP (SU01) o caricati Excel, se disponibile. è necessaria una scanner biometrico al posto di lavoro che prendono il nome di utente o dispositivo condiviso. Sicuro, l'iscrizione a distanza degli utenti e l'installazione di software client Biolock è supportato.

Stabilire un utente Biolock non ignorare o modificare le impostazioni di sicurezza di SAP esistenti o GRC. Invece, sovrapposizioni Biolock e rinforzi di sicurezza esistente. L'utilizzo è estremamente intuitivo quindi non c'è alcuna curva di formazione o di apprendimento, gli utenti devono semplicemente rispondere quando richiesto. La somministrazione di Biolock utilizza set di competenze che di solito sono già "in-house", come Amministrazione Basis, SAP Security, ABAP o HANA.

Caratteristiche e vantaggi

Caratteristiche principali	Benefici
massimo livello di sicurezza	
I dati sotto la pelle - nascosti all'interno del vostro corpo	Nessun furto di dati - nessuna immagine biometrici latenti lasciato alle spalle
Altamente complesso vena modello - più di 5 milioni di punti di riferimento	No copia del modello palma
	Facilmente possibile per gli utenti, igienico, alta utente accettazione
La crittografia dei modelli vena tramite EAS, la crittografia unica sola chiave per ogni progetto / cliente	La certificazione BSI permette l'uso di PalmSecure in alte aree sicure
	Accettato a certificazione ISO
Più basso tasso di accettazione falso (FAR): <0,00008 e falso tasso di rifiuto (FRR) = 0,01 rispetto ad altre tecnologie biometriche	La certificazione SAP di software Biolock dal 2002, sviluppato da SAP Gold Partner i tempo reale
	Facile integrazione in infrastrutture esistenti
	Flessibilità da usare con molti dispositivi come PC, tablet, chioschi, registratori di cassa e altro
	Somministrato con set di SAP di abilità in-house (Basis Administration, SAP Securit ABAP, HANA).
Controllo e monitoraggio	
La verifica eseguita utilizza palma vena biometria, anziché basarsi su password che sono facilmente compromesse. Anche se le password non continuino ad essere utilizzate in quanto sono necessarie da SAP, che sono solo il primo passo per verificare l'identità di un utente e vengono seguiti con il secondo fattore di autenticazione biometrica che è indiscutibile. La verifica biometrica viene eseguita dopo il log-on password (al contrario di prima log-on password di con la tipica Single Sign-On sistemi) proteggendo così questo processo internamente all'interno di SAP.	Utilizzo della stessa tecnologia per ogni tipo di Identity Management gestione / accesso all'interno di un'organizzazione. Ampia gamma di utilizzo:
	Applicare policy GRC attraverso la creazione di adeguate credenziali utente biomet posti di blocco per abbinare regole GRC. Impedire agli utenti fraudolenti di violare separazione delle funzioni tramite furto di password o la condivisione.
	Frodi finanziarie - Con Biolock il rischio di frode insider può essere mitigato, controllando Procure to Pay attività come richieste, ordini di acquisto, bonifici, voci diario e altro ancora. Questo viene fatto con i punti di controllo di controllo multi-livello tra cui i valori di campo massimo, doppia autenticazione o il blocco assoluto della funzionalità.
Il campione biometrico che viene rilevata al momento della firma su è paragonato a un "modello di riferimento" memorizzata, che è il modello inizialmente memorizzato da quel dall'utente al momento della loro iscrizione nel sistema. Questa iscrizione originale è stato fatto in condizioni molto controllate, e il modello di riferimento è quindi considerato autorevole. Ha senso quindi per memorizzare tale modello di riferimento molto sicuro. Nel caso della Biolock, il modello di riferimento è memorizzato all'interno di SAP, dietro un "firewall" biometricamente assicurata, e non in un'applicazione residente fuori SAP (come è consuetudine con Single Sign-On sistemi).	
	Inventario Ritiro - La capacità dei dipendenti di rilasciare l'inventario, merci della nave, creare clienti, scrivere fuori merci, emettere crediti e tale può essere prevenuta o controllata da richiedere l'autenticazione biometrica in ogni fase della catena di fornitura.
	Rilevazione Presenze - Il sistema Biolock può utilizzare la sua capacità di identificaz biometrica per stabilire indiscutibilmente l'identità di un dipendente clock dentro o al lavoro. Questo elimina le opportunità di frode libro paga come "compagno di timbratura" o l'abuso di password di clock-in, con conseguente importante rispar costo del libro paga. I dati è perfettamente integrato con SAP libro paga.
Alcuni sistemi di catturare immagini biometrici e li memorizzano, mentre Biolock non memorizza le immagini attuali. Invece, i punti di dati pertinenti vengono estratti dallo scanner palma vene, convertito in valori numerici utilizzando algoritmi Fujitsu e criptati prima di essere inviati al SAP per il confronto con i modelli di riferimento.	
	Point of Sale (POS) - In un ambiente di vendita, è possibile controllare ogni cassa transazione registro richiedendo autenticazione biometrica, riducendo così il restringimento di inventario. Nonostante la condivisione di dispositivi POS o di acce generico dei lavoratori, vera gestione delle identità è assicurato.
Non tutti i sistemi sono uguali in termini di algoritmi di matching e di identificazione. Nel caso di Biolock, potenti 1: corrispondenze identificazione N sono standard, combinato con 1: 1 di verifica nel caso in cui è previsto un campo informativo utente aggiuntivo, per velocità e precisione ottimale.	
	L'accesso alle informazioni - Richiedendo log-on e / o ri-autenticazione, l'accesso biometrico per la visualizzazione o la modifica delle informazioni sensibili può esse controllato e monitorato. I dati sensibili possono includere i record dei clienti o Informazioni di identificazione personale (PII), record di assistenza sanitaria, HR o d del personale, dati finanziari di alto livello, segreti aziendali, la proprietà intellettua (IP), disegni tecnici, ecc
La registrazione di attività, tra errori e violazioni, vengono registrati in modo sicuro in un modo a prova di manomissione che sia accessibile a strumenti di controllo di terze parti su una base di "sola lettura". Le violazioni possono essere trasmessi ai livelli di vigilanza attraverso silenziosi e-mail avvisi in tempo reale.	
In generale, (SSO) Sistemi di Single-Sign On aumentare notevolmente la convenienza, ma diminuiscono la sicurezza. credenziali di password vengono trasmessi automaticamente, dando un falso senso di sicurezza, perché	

Caratteristiche principali	Benefici
se la password è stata compromessa l'utente fraudolento può ancora rappresentare il vero utente, anche in più applicazioni.	■ Pure Logging - Se lo si desidera, Biolock può essere utilizzato per monitorare in mo semplice e registrare le attività previste all'interno di SAP, senza impedire le attivit allertare i dipendenti al monitoraggio. ■ Accesso fisico - Attualmente in fase di sviluppo, questa capacità legherà beni SAP I (Plant Maintenance) come la costruzione di ingressi ai controlli dati SAP HR e Biolo modo che l'accesso ai beni materiali può essere controllato e monitorato attraverso gestione dell'identità biometrica.

Maggiori informazioni

Fujitsu Optimization Services

Oltre a PalmSecure, Fujitsu offre una gamma di soluzioni di piattaforma. Essi combinano prodotti Fujitsu affidabili con i migliori servizi, know-how e partnership in tutto il mondo.

Dynamic Infrastructure

Con l'approccio di Fujitsu Dynamic Infrastructures, Fujitsu offre un portafoglio completo di prodotti IT, soluzioni e servizi, che vanno da clienti di soluzioni di data center, infrastruttura gestita e Infrastructure as a Service. Quanto si beneficiare di tecnologie e servizi Fujitsu dipende dal livello di cooperazione che si sceglie. Questo richiede IT flessibilità ed efficienza al livello successivo.

prodotti informatici

www.fujitsu.com/global/services/computing/

- PRIMERGY: server standard industriale
- SPARC Enterprise: server UNIX
- PRIMEQUEST: il server IA Mission-critical
- ETERNUS: Sistemi di magazzinaggio
- mainframe BS2000

Software

www.fujitsu.com/software/

- Interstadio: software di infrastruttura applicativa
- software di gestione del sistema: Systemwalker

Maggiori informazioni

Per ulteriori informazioni su Fujitsu assicurato il controllo e il monitoraggio di SAP si prega di contattare il proprio rappresentante di vendita Fujitsu, Fujitsu socio in affari o visitare il nostro sito web.

http://palmsecurebiolock.com/

Fujitsu innovazione politica verde

Fujitsu Verde politica dell'innovazione è il nostro progetto in tutto il mondo per la riduzione degli oneri per l'ambiente. Con il nostro know-how globale, ci proponiamo di risolvere i problemi di efficienza energetica ambientale attraverso di essa. Potete trovare maggiori informazioni su: www.fujitsu.com/global/about/environment/

A proposito di tempo reale

Fondata in Europa oltre 30 anni fa da ex dirigenti di alto livello SAP®, in tempo reale è un partner certificato SAP Software oro specializzata in sistemi di sicurezza e software di gestione delle identità biometrici. Il loro software Biolock ™ è l'unico sistema software biometrico nativamente integrato e certificato da SAP. Una vasta gamma di aziende globali in molti settori verticali, oltre a enti governativi sono serviti da un software in tempo reale.

Diritto d'autore

disconoscimento

Dati tecnici soggetti a modifica e la consegna in base alla disponibilità. Qualsiasi responsabilità che i dati e le illustrazioni sono completi, attuale o corretto è esclusa. Denominazioni possono essere marchi e / o copyright dei rispettivi produttori, il cui utilizzo da parte di terzi per prop scopi può violare i diritti di tale proprietario. La riproduzion di nomi di prodotto e commerciali

- Anche se non esplicitamente identificati come tali - in questa documentazione non autorizza a ritenere che che t nomi dovrebbero essere considerate esenti ai sensi del diritto dei marchi e protezione del marchio. Questa documentazione fornisce al lettore una descrizione delle prestazioni di un controllo di accesso e la tecnologia di monitoraggio di identità per lo scanner PalmSecure di Fuji Vena. In singoli casi, ci possono essere scostamenti tra i processi descritti nella documentazione e l'effettiva applicazione.

contatto

FUJITSU Mies-van-der-Rohe-Str. 8, 80807 Monaco di Baviera, Germania Tel: +49 89 62060 -1183 E-mail: thomas.bengs@ts.fujitsu.com Sito web: www.fujitsu.com/palmsecure