RELAZIONE TECNICO-INFORMATIVA INTERNA

Oggetto: Implementazione della verifica a doppia chiave (2FA) tramite codice VBA

Applicazione: Nephro&Clin 2000

Sviluppo e Controllo: A cura di **CNC Systems Srl**

Ambito di applicazione: Database Gestionale Emodialisi e Fatturazione (File Nrphro&2000_Accr.mde / Tabelle di backend)

Riferimento normativo: Adempimento misure di sicurezza GDPR (Art. 32 e Art. 9) per il trattamento di dati sanitari

1. Scenario e Obiettivo dell'intervento

L'applicazione **Nephro&Clin 2000** è lo strumento centrale per la gestione dei pazienti nefropatici sottoposti a trattamento di emodialisi e per la relativa fatturazione delle prestazioni eseguite dal Centro. Per la natura stessa della struttura, il software tratta dati ad altissimo rischio: informazioni cliniche sensibili (cartelle cliniche, schede dialitiche) e dati fiscali/amministrativi protetti.

Al fine di elevare i sistemi di protezione a tutela della privacy dei pazienti, **CNC Systems Srl** ha sviluppato e implementato una procedura di **Autenticazione a Due Fattori (2FA)** integrata direttamente nel codice VBA dell'applicazione. Questa misura si attiva in automatico all'avvio del software durante il caricamento della schermata iniziale, impedendo l'accesso ai dati clinici e di fatturazione in caso di postazioni lasciate incustodite nei reparti o furto di credenziali di rete.

2. Motivazioni Giuridiche (Conformità GDPR e Dati Sanitari)

Il Regolamento Europeo (GDPR 2016/679) impone restrizioni e tutele rigidissime (Art. 9) per il trattamento dei dati relativi alla salute. I centri medici sono i primi soggetti monitorati dalle autorità di controllo (Garante della Privacy).

- **Principio di Riservatezza dei Dati Sensibili:** La semplice identificazione del nome utente Windows non è più considerata una misura sufficiente per l'accesso a un database contenente cartelle cliniche di pazienti nefropatici e dati di fatturazione sanitaria.
- **Prevenzione del Data Breach e Accountability:** Con questa modifica, **CNC Systems Srl** assicura il rispetto del principio di responsabilità. In caso di ispezione o di incidente informatico (es. tentativo di copia non autorizzata del file di Access), la doppia chiave blocca l'applicativo prima che l'utente possa interagire con i dati dei pazienti o con i moduli di fatturazione, azzerando il rischio di sanzioni per la struttura.

3. Specifiche Tecniche della Procedura Sviluppata

La soluzione implementata da **CNC Systems Srl** applica il principio di sicurezza informatica del *"Qualcosa che conosci"* (l'account Windows del medico, infermiere o amministrativo) combinato con il *"Qualcosa che possiedi"* (l'accesso esclusivo alla casella email aziendale dell'operatore).

Il flusso logico eseguito all'avvio di Nephro&Clin 2000:

1. **Verifica strutturale dei Database:** Tramite la funzione `CheckTabella`, l'applicativo verifica istantaneamente l'integrità della tabella di controllo `p-ElencoPersonale` nel file `Personale.mdb`.
2. **Controllo dei Profili di Esecuzione:** Il codice intercetta l'utente corrente di **Nephro&Clin 2000**. Se l'utente è autorizzato al bypass (es. terminali di sola visualizzazione in sala dialisi o profili automatizzati), accede direttamente.
3. **Generazione del Token Univoco:** Se l'utente deve essere verificato (es. medici o personale amministrativo addetto alla fatturazione), il motore VBA genera un codice temporaneo (Token) univoco e *case-sensitive*.
4. **Spedizione tramite Protocollo CDO:** Il token viene inviato all'indirizzo email dell'operatore tramite la funzione `SendCDOMail` con mittente *NoReplay@Me.it* e oggetto specifico legato al Centro di Emodialisi.
5. **Verifica Binaria Stringente:** Una finestra di input (`InputBox`) richiede l'inserimento del codice. Il controllo avviene tramite un confronto binario puro (`StrComp(..., vbBinaryCompare)`), impedendo qualsiasi tentativo di accesso fraudolento o casuale.
6. **Chiusura Forzata di Sicurezza:** Se il codice viene inserito in modo errato per 3 volte o se la procedura viene annullata, il codice VBA comanda l'immediata chiusura della maschera iniziale `frmabout` e la terminazione totale di **Nephro&Clin 2000** tramite l'istruzione `DoCmd.Quit acQuitSaveNone`, sigillando i dati dei pazienti.

4. Gestione delle Eccezioni nell'Infrastruttura

- **Primo Accesso e Inserimento Email:** Qualora un operatore abilitato sia privo di indirizzo email nel database, l'applicazione lo reindirizza in modalità esclusiva sulla maschera `p-InserisciEmail` aperta come finestra di dialogo obbligatoria (`acDialog`). Finché l'anagrafica del personale non è completata, l'accesso ai dati clinici e di fatturazione rimane interdetto.
- **Tracciabilità dei Bypass:** L'attivazione del campo `bypassToken` è concessa e monitorata dai soli amministratori del sistema per specifiche esigenze tecniche di reparto, riducendo al minimo la superficie di attacco del software.

5. Conclusioni

L'integrazione di questa procedura nativa in VBA, curata da **CNC Systems Srl**, eleva drasticamente gli standard di sicurezza di **Nephro&Clin 2000**, trasformandolo in un applicativo protetto, moderno e pienamente conforme alle normative GDPR per le strutture sanitarie. L'impatto sull'operatività quotidiana del personale del Centro è di pochi secondi, a fronte di una protezione totale della privacy dei pazienti nefropatici e della sicurezza fiscale dei trattamenti eseguiti.

Bellizzi (Sa), 24/05/2026

Per CNC Systems Srl : l'Amministratore **Carmine CERRATO**