Brain-Computer Interfaces (BCI) e Sicurezza Informatica: una sfida emergente



L’evoluzione tecnologica nel campo delle interfacce cervello-computer (Brain-Computer Interfaces, BCI) sta aprendo nuove frontiere nella medicina personalizzata, offrendo possibilità terapeutiche prima inimmaginabili. Come sottolineano Schroder e colleghi nel documento “*Cyber Risks to Next-Gen Brain-Computer Interfaces: Analysis and Recommendations*” questi dispositivi *“consentono la comunicazione diretta tra il cervello e computer esterni, rappresentando una rivoluzione per il trattamento di patologie neurologiche come il morbo di Parkinson, l’epilessia e diverse malattie mentali resistenti alle terapie convenzionali”*. Tuttavia, con l’avanzamento tecnologico emergono nuove vulnerabilità in ambito di sicurezza informatica che non possono essere ignorate.

L’era delle Brain-Computer Interfaces: tra potenziale e rischi

Le Brain-Computer Interfaces moderne si differenziano notevolmente dai loro predecessori. *“In passato, questi dispositivi erano circuiti integrati per applicazioni specifiche (ASIC) che potevano eseguire solo una singola funzione sanitaria in un ciclo*” (Schroder). Oggi, invece, si avvicinano sempre più a veri e propri computer personali impiantabili. Caratterizzati da capacità di aggiornamento software, memorizzazione di dati locale e trasmissione in tempo reale, questi dispositivi offrono possibilità terapeutiche senza precedenti, ma introducono al contempo

superfici di attacco inedite.

La FDA (Food and Drug Administration) classifica le Brain-Computer Interfaces come dispositivi medici impiantabili di Classe III, la categoria a più alto rischio, soggetta alle normative più rigorose. Ciononostante, il quadro normativo fatica a tenere il passo con l'innovazione tecnologica. Se l'hardware è sottoposto a severe restrizioni, il software integrato gode ancora di regolamentazioni relativamente permissive, creando uno spazio liminale in cui i rischi informatici possono proliferare.

Classificazione FDA dei dispositivi BCI

La FDA classifica i dispositivi medici in tre categorie in base al loro rischio:

- Classe I: dispositivi a basso rischio;
- Classe II: dispositivi a rischio moderato;
- Classe III: dispositivi ad alto rischio

Le BCI sono classificate come dispositivi medici impiantabili di Classe III, che rappresenta la categoria a più alto rischio. Questa classificazione è giustificata dal fatto che le BCI sono dispositivi che supportano o sostengono la vita del paziente e vengono impiantati direttamente nel cervello.

Regolamentazione e lacune normative

Un punto cruciale evidenziato nello studio è che, sebbene le Brain-Computer Interfaces siano regolamentate come dispositivi impiantabili di Classe III con rigorose restrizioni sull'hardware, esiste una discrepanza significativa nella regolamentazione del software a bordo di questi dispositivi. Come spiega il documento:

> *"I dispositivi di Classe III sono soggetti alle normative più rigorose, ma faticano a tenere il passo con il cambiamento tecnologico, specialmente con le moderne BCI che sono dispositivi in rete con capacità di aggiornamento e accesso*

remoto.”

In pratica, questo significa che mentre l’hardware dei dispositivi neurali è sottoposto a controlli rigorosi, il software che gestisce questi dispositivi è regolamentato in modo più permissivo. Questa disparità crea quella che gli autori chiamano uno “spazio liminale”: le Brain-Computer Interfaces sono trattate come impianti con rigide restrizioni hardware, ma con componenti software più avanzati comparativamente meno regolamentati.

Evoluzione delle normative FDA

Il documento menziona anche l’evoluzione delle normative FDA riguardanti la cybersecurity. Fino a poco tempo fa, la sicurezza informatica era raramente considerata per qualsiasi classe di dispositivi medici. I dispositivi più vecchi (definiti “*legacy devices*“) spesso non hanno alcun metodo per aggiornare il software o correggere bug.

La situazione è cambiata nell’ottobre 2014, quando la FDA ha introdotto un requisito di pianificazione della cybersecurity: “*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*“. Tuttavia, fino al 2022, queste linee guida erano solo raccomandazioni non vincolanti. Con il *Food and Drug Omnibus Reform Ac*t del 2022 (FDORA) e il *Protecting and Transforming Cyber Health Care Act* del 2022 (PATCH), è stata introdotta l’applicazione obbligatoria, richiedendo che le informazioni sulla cybersecurity vengano presentate insieme alle domande di commercializzazione di nuovi dispositivi.

Implicazioni per le Brain-Computer Interfaces

Questa evoluzione normativa è particolarmente rilevante per le Brain-Computer Interfaces poiché rappresentano una tecnologia emergente che non ha ancora raggiunto la disponibilità generale sul mercato. Gli autori sottolineano che questo è “un

momento opportuno per suggerire modifiche alla regolamentazione della sicurezza informatica dei dispositivi medici", prima che i dispositivi neurali diventino ampiamente disponibili.

Un modello di minaccia per le Brain-Computer Interfaces

Utilizzando il *Common Vulnerability Scoring System* (CVSS), gli esperti hanno identificato quattro vettori di attacco principali per le Brain-Computer Interfaces: fisico, locale, locale adiacente e di rete. Mentre l'accesso fisico rappresenta un rischio contenuto per dispositivi impiantati, le connessioni locali e remote costituiscono vulnerabilità significative.

Le BCI generano enormi quantità di dati clinici e personali che devono essere memorizzati e protetti. Che si opti per la memorizzazione locale sul dispositivo o remota su computer esterni, questi dati rappresentano un tesoro di informazioni sensibili che richiedono adeguata protezione. Lo studio HALO di Karageorgos et al., citato nella ricerca di Schroder, ha rivelato una preoccupante realtà: "*sette dei principali prodotti BCI sul mercato non supportavano la crittografia dei dati*", esponendo potenzialmente informazioni sanitarie personali a accessi non autorizzati.

Le minacce non si limitano al furto di dati. Un attacco informatico riuscito potrebbe comportare conseguenze drammatiche come la disabilitazione del dispositivo (che richiederebbe intervento chirurgico per il ripristino), la stimolazione cerebrale indesiderata, l'induzione di movimenti involontari, o l'alterazione dell'elaborazione della visione e della sintesi vocale. Sebbene alcuni di questi rischi non siano esclusivi delle BCI, la particolare invasività di questi dispositivi e la loro connessione diretta con il cervello amplificano le potenziali conseguenze.

Raccomandazioni per rafforzare la sicurezza

Per affrontare queste vulnerabilità, è essenziale implementare misure di sicurezza adeguate prima che le BCI raggiungano la disponibilità generale. Come affermano Schroder e colleghi:

> *“Ora è il momento opportuno per suggerire modifiche alla regolamentazione della sicurezza informatica dei dispositivi medici, poiché le BCI non hanno ancora raggiunto la disponibilità generale”.*

Quattro aree principali richiedono interventi immediati:

Aggiornamenti Software

Gli aggiornamenti software rappresentano un elemento critico per la sicurezza, ma anche un potenziale vettore di attacco. I produttori dovrebbero fornire metodi di aggiornamento wireless o comunque non chirurgici, implementando controlli di integrità nelle fasi di download, trasferimento e installazione. Dal canto loro, i regolatori dovrebbero imporre che ogni dispositivo BCI abbia almeno un’opzione di aggiornamento non chirurgica e che verifichi l’integrità degli aggiornamenti prima dell’installazione.

Autenticazione e Autorizzazione

Le BCI necessitano di connettività wireless per funzionare efficacemente, ma questa comunicazione deve essere adeguatamente protetta. I produttori dovrebbero implementare controlli tecnici per l’autenticazione e l’autorizzazione nell’accesso ai dati e alle impostazioni del dispositivo, consentendo ai pazienti di gestire i permessi e ripristinare gli accessi. I regolatori dovrebbero richiedere questi sistemi e promuovere l’adozione di pratiche di sicurezza avanzate come l’autenticazione a due fattori.

Minimizzazione della Superficie di Attacco

Sebbene la connettività offra vantaggi significativi, espone anche i dispositivi a potenziali attacchi. Poiché le BCI necessitano di connessione solo durante il trasferimento di dati o l'aggiornamento delle impostazioni, i produttori dovrebbero implementare funzionalità che consentano ai pazienti di abilitare o disabilitare la connessione wireless. I regolatori, parallelamente, dovrebbero rendere obbligatorie queste funzionalità per ridurre la superficie di attacco.

Crittografia

La maggior parte delle BCI all'avanguardia non implementa la crittografia a causa delle limitazioni energetiche. Tuttavia, architetture hardware innovative hanno dimostrato che è possibile integrare routine di crittografia senza esaurire il budget energetico. La priorità dovrebbe essere data alla crittografia dei dati in transito, con i produttori che implementano routine crittografiche per i dati che lasciano il cervello e i regolatori che ne impongono l'adozione.

Verso un futuro più sicuro

Le Brain-Computer Interfaces rappresentano una frontiera terapeutica straordinaria, ma la loro adozione sicura richiede un approccio proattivo alla cybersecurity. Il momento per implementare misure di protezione adeguate è ora, prima che questi dispositivi raggiungano ampia diffusione. Come avvertono gli autori dello studio, "*se queste raccomandazioni vengono ignorate, la sicurezza e la privacy dei pazienti sono a rischio*". Le conseguenze potrebbero spaziare dalla compromissione della privacy fino alla possibilità di interferenze dirette con le funzioni cerebrali.

La tecnologia BCI ha il potenziale per migliorare radicalmente la qualità della vita di molti pazienti, ma questo potenziale può realizzarsi pienamente solo se accompagnato da solide

pratiche di sicurezza informatica. Schroder et al. concludono che “*i dispositivi ad alto rischio non dovrebbero essere introdotti al pubblico finché i problemi di sicurezza essenziali non sono risolti*“. Produttori, regolatori e ricercatori hanno la responsabilità condivisa di garantire che l’innovazione proceda di pari passo con la protezione della privacy e della sicurezza dei pazienti.

Riferimenti:

Schroder, T., Sirbu, R., Park, S., Morley, J., Street, S., & Floridi, L. (2025). *Cyber Risks to Next-Gen Brain-Computer Interfaces: Analysis and Recommendations*. Yale University Digital Ethics Center.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/brain-computer-interfaces-bci/