Misure tecniche di sicurezza per l'applicazione SenoNet

Versione 2.1 del 20/03/2023

Misure tecniche dell'applicazione SenoNet

SenoNet è un'applicazione web basata su LAMP (Linux, Apache/Nginx, MySQL, PHP). In SenoNet vengono registrati i dati clinici di pazienti con patologie mammarie. SenoNet è installato presso il cloud di Amazon AWS nella Regione di Milano (allegato *Infrastruttura cloud AWS*).

Protezione dei dati

SenoNet implementa diverse tecniche per aumentare il livello di protezione dei dati, principlamente: *pseudonimizzazione*, *crittografia e isolamento di rete*. Tali tecniche sono impiegate per ridurre sensibilmente la possibilità di identificazione di un soggetto a partire dai dati registrati.

Pseudonimizzazione

I dati nel database di SenoNet sono fortemente pseudonimizzati e resi *quasi-anonimi*, come illustrato di seguito:

- Il record completo di SenoNet ha una dimensione dell'ordine di 250 variabili. I dati clinici sono rappresentati da valori codificati, dove, ad esempio, la variabile B02 ha valori possibili: 1, 2, …, 11. B02 rappresenta una certa grandezza clinica (la sede della lesione) e i valori numerici indicano le sedi (supero-esterno, infero-interno, ecc.) —vedere esempio allegato
- Non esiste alcun tipo di ID paziente che riconduca il record a un individuo: i dati non sono riconducibili al paziente.
- Le date degli eventi clinici sono spostate di un valore casuale, entro un certo intervallo, in modo che non siano collegabili agli eventi clinici reali.
- Ogni centro è identificato da un ID alfanumerico. La mappa di decodifica è gestita in modo completamente separato dal database.
- Gli unici dati anagrafici del paziente sono l'anno di nascita e il genere.

Con tali misure si raggiunge un livello di anonimizzazione che rende pressoché impossibile la ricostruzione del collegamento di un record a un individuo. Persino per il centro stesso, titolare del trattamento, sarebbe un compito arduo.

Nonostante il considerevole grado di anonimizzazione, i dati vengono protetti con criteri di ulteriore sicurezza descritti di seguito.

Crittografia

Come misura addizionale di protezione dei dati, viene impiegata la cifratura “At Rest” del database fornita dal servizio RDS di AWS. L’algoritmo di cifratura è AES-256. La chiave master è gestita all’interno del servizio KMS (Key Management Service) di AWS e non lascia mai il KMS.

Isolamento di rete

SenoNet è inserito in un’infrastruttura di rete che consente l’accesso solo a una lista di indirizzi IP precedentemente autorizzati (whitelist). Il Web Application Firewall (WAF) davanti a SenoNet è configurato in modo tale che le connessioni provenienti dagli indirizzi IP presenti nella whitelist utilizzino esclusivamente la porta HTTPS. Tutti gli IP non contenuti nella whitelist e gli altri tipi di connessione sono rifiutati dal WAF e quindi non raggiungono l’applicazione. I centri che partecipano

a SenoNet devono comunicare preventivamente gli IP da cui accedono affinché siano inseriti nella whitelist.

Amministratori di Sistema (AdS)

Sono individuati tre tipi di AdS: Esperto applicativo, DevOps, Sistemista.

ESPERTO (O AMMINISTRATORE) APPLICATIVO

Tale figura possiede un elevato know-how sulle logiche e gli obiettivi di Senonet. È la figura che fornisce attività di supporto ed effettua le analisi dei dati. L'Esperto applicativo utilizza un ruolo che gli consente di:

- vedere tutti i dati
- verificare il corretto funzionamento dell'applicazione
- analizzare situazioni di errore
- effettuare test sugli aggiornamenti
- effettuare operazioni di esportazione, importazione e analisi utilizzando la console applicativa di gestione
- creare, modificare e cancellare gli account

L'esperto applicativo non ha accesso diretto al server e al database.

DEVOPS

Il DevOps (Development & Operations) è una figura con elevate competenze di sviluppo, di gestione dell'applicazione e di sicurezza, necessarie per effettuare le operazioni di:

- gestione del codice e delle versioni
- pubblicazione degli aggiornamenti
- gestione degli script di backup
- manutenzione del database
- test e verifiche

Il DevOps può accedere come amministratore a: applicazione, database, sistema operativo.

SISTEMISTA

Il sistemista si occupa della gestione del server, delle componenti di sistema e della sicurezza sistemistica, tra cui:

- sistema operativo
- database server
- software di sistema (web, posta, ecc.)
- trasferimento e archiviazione dei backup
- monitoraggio dei sistemi
- account di sistema

I sistemisti non hanno un account applicativo.

Utenti di Senonet

Utenti dei centri

Gli utenti di un centro accedono a SenoNet solo per effettuare l'upload dei dati.

Utenti Admin

Gli utenti di SenoNet con la capacità di accedere a qualsiasi dato dell'applicazione hanno il ruolo di Admin. Ad esempio, l'esperto applicativo sopra menzionato accede con il ruolo di Admin.

Controllo degli accessi

Protezione da tentativi di accesso non autorizzato

All'interno dell'applicazione sono attivi dei controlli per prevenire eventuali attacchi sul login (tentativi di accesso ripetuti). In seguito all'attivazione di tali controlli uno username o un indirizzo IP sono automaticamente bloccati al superamento di soglie predefinite di tentativi di login; in tal caso, lo sblocco può essere effettuato solo da un utente Admin.

Il tempo di inattività della sessione in SenoNet è di 60 minuti, trascorsi i quali un utente viene scollegato.

Il metodo di autenticazione è basato sull'autenticazione forte: l'utente deve fornire la password e un fattore TFA (Two Factor Authentication). Il secondo fattore è costituito da una OTP (One-Time Password) generata da un'app, come Google Authenticator o Authy, da installare sullo smartphone dell'utente e da accoppiare alle credenziali.

Regole per la password

La password è personale e deve essere mantenuta segreta, può essere modificata dall'utente in ogni momento e ha una validità di 90 giorni. Le password non sono memorizzate in SenoNet (viene memorizzato un hash), pertanto solo ed esclusivamente l'utente può conoscere la propria password.

L'utente ha l'obbligo di mantenere riservate le credenziali e adottare password composte da un minimo di 8 caratteri alfanumerici, contenenti:

- Almeno una lettera minuscola
- Almeno una lettera maiuscola
- Almeno un numero
- Almeno un carattere speciale scelto da questa lista + - * = ( ) [ ] < > / \ _ | ! % ? ^ . ; # € £ $

Modalità di accesso al server da parte dei DevOps e dei Sistemisti

L'accesso all'infrastruttura avviene esclusivamente tramite una connessione VPN con TFA.

Modalità di accesso all'applicazione da parte degli amministratori applicativi

Poiché un amministratore applicativo potrebbe avere l'esigenza di accedere anche in mobilità, si utilizza una funzionalità di filtro con autenticazione OIDC (OpenID Connect) gestita dall'Application Load Balancer (ALB) posto davanti a SenoNet, dopo il WAF. Il filtro richiede l'autenticazione

all’utente, ridirigendolo verso un Identity Provider esterno. Superata tale autenticazione, l’utente può arrivare a SenoNet ed effettuare il login con TFA sull’applicazione.

Backup e log

Backup

Il backup del database è effettuato direttamente dal servizio RDS e i backup sono cifrati con chiave gestita dal KMS. I backup vengono conservati per 30 giorni.

Log degli accessi all'applicazione

L’applicazione registra gli accessi da parte degli utenti. I dati vengono memorizzati nel servizio AWS CloudWatch e conservati per 12 mesi.

Log di sistema

I diversi moduli di sistema (sistema operativo, web server, ecc.) generano log che vengono conservati per 12 mesi in CloudWatch.