PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4105 di venerdì 20 ottobre 2017

I rischi principali dei dati personali archiviati in database

La maggior parte dei dati personali sono custoditi in data base interni alle aziende o affidati a soggetti terzi (cloud). Quali sono i rischi principali che i responsabili del trattamento e il responsabile della protezione dei dati debbono esaminare?

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

Un recente studio di un'azienda specializzata ha messo in evidenza che il 95% delle violazioni di dati personali avvengono presso basi dei dati. Il numero di dati personali coinvolti in questa violazione ha superato abbondantemente il quarto di milione, nell'ultima ricerca effettuata.

Le ragioni per cui i database sono presi di mira dagli attaccanti è molto semplice: questi database sono alla base di ogni organizzazione, perché custodiscono dati personali di clienti ed altre informazioni riservate. Purtroppo a questa grande importanza dei dati custoditi nei database non corrisponde una sufficiente professionalità ed un adeguato investimento nella protezione dei dati stessi.

Questo è il motivo perché in cui, secondo un altro recente studio, il 97% delle violazioni avrebbe potuto essere prevenuto con relativa facilità, adottando semplici misure di protezione e di controllo.

Offriamo di seguito un elenco delle 10 principali minacce che sono state evidenziate in questo studio:

privilegi di accesso eccessivi o non utilizzati

abuso di privilegi di accesso

iniezione di SQL

malware

debolezza dell'audit trail

mancata protezione dei supporti fisici di archiviazione

sfruttamento di vulnerabilità o inadeguate configurazioni dei database

insufficiente gestione di dati sensibili

negazione di servizio

insufficiente preparazione ed educazione del personale addetto alla protezione.

Privilegi di accesso eccessivi o non utilizzati

Quando ad un incaricato del trattamento viene concesso l'utilizzo di un profilo di accesso che eccede le esigenze minime, connesse alla sua funzione aziendale, si apre la porta a possibili abusi. Ad esempio, un dipendente bancario che sia incaricato di cambiare solo le informazioni di contatto con un cliente, se ha a disposizione un privilegio di accesso eccessivo, potrebbe intervenire anche sulla disponibilità del conto ed effettuare trasferimenti non autorizzati.

Inoltre, l'esperienza insegna che spesso, quando un dipendente abbandona l'azienda, l'azienda non provvede all'immediata cancellazione dei suoi privilegi di accesso.

Questa situazione è dovuta, per solito, alla mancata effettuazione, almeno a scadenze periodiche di alcuni mesi, della validità e legittimità dei profili di accesso, nonché di verifica critica dei privilegi di accesso stessi.

Abuso di privilegio

Si tratta di un'altra forma di abuso, che è diretta conseguenza del caso precedente.

Supponiamo ad esempio che un applicativo possa permettere di esaminare la cartella clinica di un paziente, attraverso un collegamento Web. L'applicazione Web normalmente limita gli utenti ad esaminare soltanto la storia sanitaria di uno specifico paziente e non possono essere esaminate contemporaneamente le cartelle sanitarie di più pazienti. Tuttavia un hacker, anche non particolarmente esperto, può aggirare questi vincoli collegandosi al database sotto forma di cliente alternativo. È così possibile scaricare e salvare tutte le cartelle sanitarie dei pazienti, per i quali si è ottenuto l'accesso.

Iniezione di codici SQL

Un attacco con iniezione di codici SQL può consentire ad un soggetto terzo di avere un accesso illimitato all'intero database. Questo attacco può essere perpetrato utilizzando applicazioni Web, in grado di penetrare il data base, non sufficientemente protetto. Con questa violazione, i dati personali critici possono essere esaminati, copiati e perfino modificati.

Malware

I criminali informatici usano tecniche di attacco che utilizzano modalità multiple, che possono consentire di penetrare all'interno dei database e sottrarre informazioni riservate. Gli utenti legittimi, che non si rendono conto che il malware ha infettato i loro dispositivi di accesso, diventano un canale di collegamento, che facilmente permette di estrarre dati sensibili.

Audit trail insoddisfacenti

La registrazione automatica di tutte le transazioni che coinvolgono i database dovrebbe far parte di qualsiasi architettura di sicurezza di un database. Se non si è a disposizione una dettagliata registrazione delle attività di collegamento al database ci si trova in una situazione di rischio estremamente elevata.

Le organizzazioni che non dispongono di questi meccanismi di audit dell'accesso al database potrebbero anche trovarsi in difficoltà nel rispettare indicazioni specifiche, che vengono poste dalle aziende pubbliche e delle autorità di governo. Ad esempio, negli Stati Uniti esiste una legge che specificamente impone che questi meccanismi di protezione siano attivi, a pena di severe sanzioni. È ben vero che molti fornitori di database mettono a disposizione dei sistemi di tracciamento degli accessi, ma occorre vedere se questi dispositivi sono sufficientemente efficaci e se hanno, in caso di violazione, un soddisfacente valore probatorio, a fronte di una indagine criminologica. Quando poi gli utenti si collegano al database attraverso delle applicazioni Web potrebbe essere ancora più difficile capire se e come l'accesso sia legittimo, almeno nei confronti di uno specifico utente. Molti meccanismi di audit non sono in grado di individuare chi è l'utente finale, perché tutta l'attività è associata con il nome, cui il profilo di accesso si riferisce.

Infine non dimentichiamo che anche un utente, con accesso a livello di amministratore, potrebbe accidentalmente o dolosamente

neutralizzare i sistemi di protezione esistenti per nascondere attività fraudolente. Il compito di effettuare attività di audit dovrebbe essere sempre separato da quello degli amministratori del database, per garantire un controllo incrociato soddisfacente.

Mancata protezione dei supporti fisici di archiviazione

Spesso i supporti di backup non sono sufficientemente protetti da attacchi ed ecco la ragione per cui numerose violazioni di sicurezza sono state collegate al furto di dischi e nastri di backup. A questo fatto si aggiunge anche l'insoddisfacente controllo e monitoraggio delle attività degli amministratori, che hanno accesso a informazioni sensibili. Occorre ricordarsi sempre che le misure appropriate per proteggere le copie di backup di dati sensibili devono essere di alto livello, non solo per garantire la protezione, ma anche per garantire il rispetto di specifiche disposizioni di legge.

Sfruttamento di vulnerabilità o inadeguate configurazioni del data base

È purtroppo frequente il fatto che ci si trovi davanti a database e che hanno dei conti di accesso di default e dei parametri di configurazione, che non sono stati personalizzati, per soddisfare esigenze specifiche dell'utente. Gli attaccanti sanno bene come sfruttare queste debolezze per lanciare attacchi contro i dati ivi custoditi. A loro vantaggio gioca anche una possibile pigrizia da parte del responsabile della protezione del data base, che non applica gli interventi correttivi, messi a disposizione, ad esempio, dal fornitore del database. L'esperienza ha dimostrato che, una volta che un intervento correttivo è disponibile, alcune aziende ci mettono dei mesi per attivare queste attività protettive.

Insufficiente gestione dei dati sensibili

Se l'azienda non sa esattamente dove si trovano i dati sensibili, che devono avere un maggior livello di protezione, nell'ambito del database, diventa difficile adottare misure specifiche di protezione. Al proposito, si ricorda che tutte le disposizioni di legge in materia di dati personali fanno obbligo di adattare il livello di protezione alle criticità e sensibilità del dato in questione.

Negazione del servizio

La negazione di servizio è una categoria generale di attacco informatico, che impedisce agli utenti di collegarsi alle applicazioni ed ai dati. Queste tecniche di attacco possono essere attuate in vari modi. La tecnica più corrente, almeno con riferimento ai database, è quella di sovraccaricare le risorse del server inviando numerose richieste di accesso al database, che alla fine portano al blocco del server. I motivi legati a questa tipologia di attacco sono spesso collegati a tentativi di estorsione, in cui un attaccante remoto blocca ripetutamente il server, finché non ottiene la somma richiesta. È bene ricordare che questo tipo di attacco rappresenta uno dei rischi maggiori per qualsiasi organizzazione.

Insufficiente esperienza e preparazione del personale addetto alla protezione dei dati

Purtroppo non sempre i soggetti, cui è affidata la responsabilità di tenere sotto controllo ed aggiornare la sicurezza di database, hanno ricevuto una sufficiente preparazione e hanno partecipato a periodici corsi di aggiornamento, che permettano di tenere la loro formazione sempre allineata con l'evoluzione delle tecniche di attacco.

Una recente indagine ha messo in evidenza che il 75% delle aziende interpellate ha sofferto delle perdite dovute al fatto che le politiche di sicurezza non erano state comprese a fondo, mentre addirittura la metà delle piccole aziende interpellate ha confessato di non avere in atto un programma per educare il proprio personale su questi rischi, afferenti alla sicurezza e protezione dei dati.

Conclusioni

Alla luce di queste informazioni, sollecitiamo i responsabili del trattamento ed i responsabili della protezione dei dati ad effettuare una verifica dei database affidati alle loro cure per esaminare, grazie ad un'appropriata analisi di rischio informatico, se il livello di protezione assicurato è compatibile con quanto il regolamento generale europeo impone e il buon senso raccomanda.

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it