Securitatea unei baze de date

Bouruc Petru-Liviu

15/01/2021

Contents

1 Introducere **2**
1.1 Importanța datelor 2
1.2 Tipuri de atacuri / probleme care pot apărea la o bază de date 2

2 Scurt istoric **3**

3 Atacurile software **4**
3.1 SQL Injection 4
3.2 Denial of Service 4
3.3 Cross-site scripting (XSS) attack 4
3.4 Malware attack 5
3.5 Factorul uman / Privilegiile 5

4 Cum ne protejăm? **5**
4.1 Encriptarea datelor 5
4.2 Firewalls 6
4.3 Backup & Updates 6
4.4 Accesul la baza de date 6

5 Concluzia **6**

1 Introducere

În zilele noastre, tehnologia din jurul nostru se dezvoltă la un ritm nemaivăzut până acum în istorie. Odată cu această dezvoltare rapidă a tehnologiei, apare și nevoia tot mai mare de a stoca datele. Bazele de date, prin definiție, conțin date de diferite tipuri, care pot varia de la numărul de la numărul de like-uri ale unei postări, la parolele de Facebook, Google, sau chiar date de la cardul personal. Astfel, bazele de date sunt printre țintele preferate ale hackerilor, securitatea ei fiind ceva de mare importanță pentru dezvoltatorii unei aplicații.

1.1 Importanța datelor

Securitatea datelor a fost mereu o problemă în rândul programatorilor, în momentul de față fiind mai cruciale decât niciodată. Cele 3 obiective principale ale Securității unei Baze de Date sunt *confidentialitatea*, *integritatea* și *disponibilitatea*. Pierderea datelor sau perturbarea lor nu afectează doar utilizatorul, cât și întreaga companie.

1.2 Tipuri de atacuri / probleme care pot apărea la o bază de date

Toate aceste "amenințări" însă pot apărea sub mai multe forme, ele putând fi împărțite în mod general în probleme de tip:

(a) Software - numite în engleză și *cyber − attacks*, și reprezintă acțiuni care au ca țintă sistemele informatice, rețelele de computere sau chiar computerele personale, folosind diferite metode de a fura, altera sau distruge date

(b) Hardware - pot varia de la defecțiuni fizice cum ar fi lovituri suferite de disk, calitatea proastă a fabricației componentelor, la probleme care pot apărea în urma închiderii neașteptate a sistemului (exemplu: pene de curent)

2 Scurt istoric

Problema securității bazelor de date a început să fie pusă începând cu anii '80 când au apărut primii viruși. Aceștia au fost la acel moment simple erori în cod. Odată ce s-a conștientizat existența lor, au apărut viruși sub forma unor "glume între programatori", cu scopul de a amuza sau a dovedi calitățile superioare ale creatorului.

Primul virus periculos care a apărut s-a numit *Brain* (1986) și avea ca scop atacul asupra așa-numitelor "floppy-disk-uri" (a fost folosit inițial de IBM PC pentru a urmări prgoramele piratate și distribuite ilegal). Acesta a fost dezvoltat de 2 frați, Amjad și Basit Farooq Alvi. *Brain* altera floppy-disk-urile, schimbându-le bootul, încetinindu-le și blocând 7kb de memorie.

În anul 1998, doi tineri de 16 ani din California împreuna cu mentorul lor de 18 ani din Israel au reușit să intre și să preia controlul sistemelor ce făceau parte din U.S. Department of Defence, sisteme care erau operate de guvern, armată și diferite companii din sectorul privat. Pentru a prinde hackerii (care inițial s-a crezut ca sunt din Iraq), au fost implicați oameni de la NASA, FBI, CIA și U.S. Department of Justice. Operațiunea s-a numit *Solar Sunrise*, iar după ce s-a terminat s-au luat măsuri drastice pentru a nu se mai repeta incidentul.

În anul 2013, toate cele 3 miliarde de conturi înregistrate la Yahoo au devenit victimele unui atac cibernetic care a fost descoperit abia în 2014. Andrew Komarov, investigatorul șef în această operațiune, a descoperit evidențe cum că pe *dark web* a apărut o listă cu peste un miliard de conturi pentru $300,000.

Malware	Year
40,000,000	2009
60,000,000	2010
75,000,000	2011
100,000,000	2012
190,000,000	2013
320,000,000	2014
475,000,000	2015
590,000,000	2016
720,000,000	2017
740,000,000	2018

Table 1: Numărul de atacuri malware pe ani

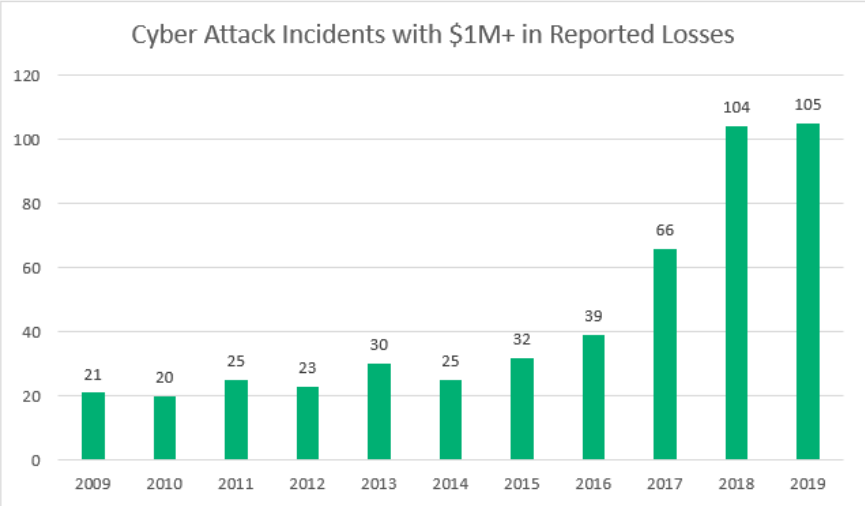


Figure 1: Numărul de incidente cu peste $1M+ pierderi

3 Atacurile software

Așa cum am menționat anterior, atacurile software, numite si *cyber − attacks* reprezintă acțiuni care au ca țintă sistemele informatice, rețelele de computere sau chiar computerele personale, folosind diferite metode de a fura, altera sau distruge date. În continuare, voi prezenta unele din cele mai întâlnite tipuri de *cyber − attacks*.

3.1 SQL Injection

Un SQL Injection se petrece atunci când cineva cu rele intenții executa o comandă SQL într-un input pe partea de client al unui website. Un exploit reușit poate citi date confidențiale din baza de date, modifica sau chiar executa operații destinate administratorului.

Spre exemplu, un formular dintr-o pagină web poate cere utilizatorului numele la logare, iar codul împreuna cu comanda SQL asociată este:

```
input = getRequestedString("UserName");
SQLcmd = "SELECT * FROM users WHERE user_name = " + input;
```

Astfel, dacă cineva introduce "$or'1' =' 1'$", ar rezulta un string de forma:

```
SQLcmd = "SELECT * FROM users WHERE user_name =" or '1'='1'";"
```

Deoarece 1=1 mereu, condiția va fi evaluata cu True și va returna toți userii din baza de date.

3.2 Denial of Service

Un DoS reprezintă un atac care poate copleși resursele serverului sistemului atacat, astfel încât acesta nu mai poate răspunde requesturilor. Acesta este lansat cu ajutorul unui număr mare de hosturi care sunt infectate cu diferiți viruși și controlate de atacator.

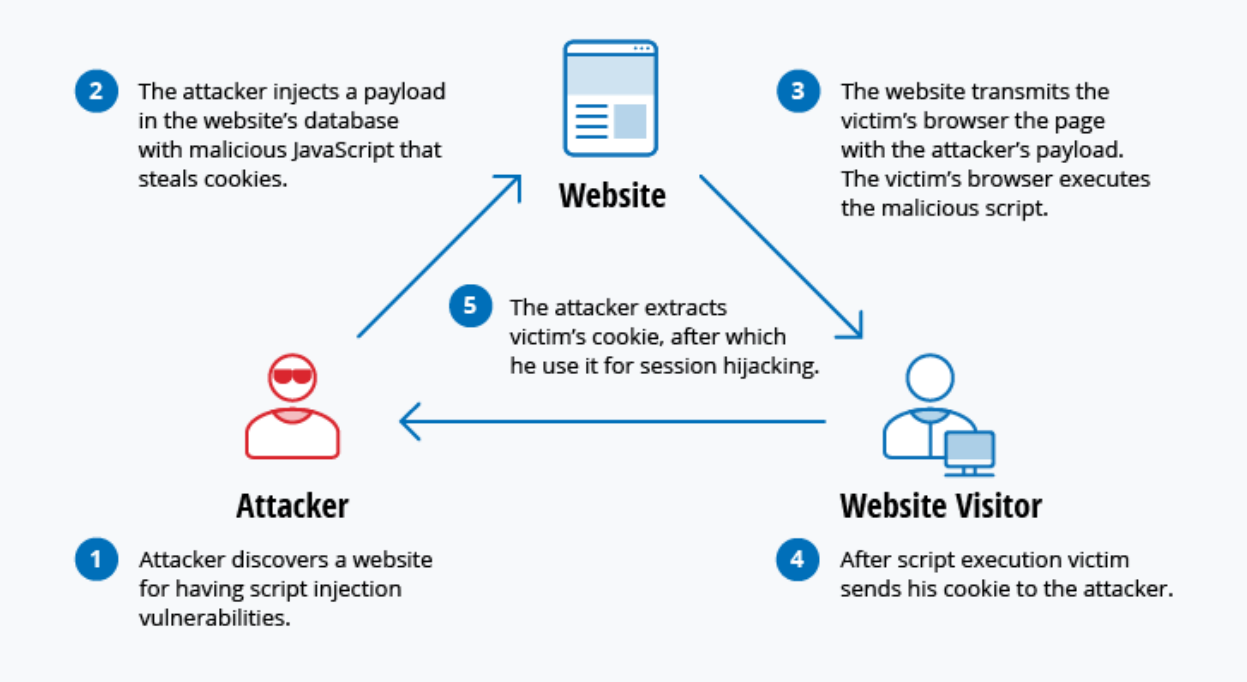
Spre deosebire de celelalte tipuri de atac, DoS-ul nu oferă beneficii directe atacatorilor. Pentru unii dintre ei, este suficient să aibă satisfacția atacului. Cu toate acestea, dacă resursa atacată aparține unui concurent de afaceri, atunci beneficiul pentru atacator poate fi suficient de real. Un alt scop al unui atac DoS poate fi acela de a scoate un sistem offline, astfel încât să poată fi lansat un alt tip de atac. Un exemplu obișnuit este deturnarea sesiunii.

Atacurile bazate pe consumul de resurse, cum ar fi trimiterea în mod repetat de interogări complexe de căutare pentru a epuiza resursele serverului reprezintă un exemplu bun de atac DoS.

3.3 Cross-site scripting (XSS) attack

Atacurile XSS folosesc resurse web third-party pentru a rula scripturi în browserul web sau în aplicația victimei. Mai exact, atacatorul injectează un playload (partea din datele trasmise care reprezintă mesajul propriu-zis) cu JavaScript rău intenționat în baza de date a unui site web. Când victima solicită o pagină de pe site, acesta îi transmite una cu playloadul atacatorului ca parte a corpului HTML, în browserul victimei, care execută scriptul rău intenționat.

De exemplu, pot fi trimise date de la victimă la atacator cum ar fi cookie-uri. Consecințele cele mai periculoase apar atunci când XSS este utilizat pentru a exploata vulnerabilități suplimentare. Aceste vulnerabilități pot permite unui atacator nu doar să fure cookie-uri, ci și să înregistreze lovituri cheie, să facă capturi de ecran, să descopere și să colecteze informații de rețea, să acceseze și să controleze de la distanță computerul victimei.



3.4 Malware attack

Software-ul rău intenționat poate fi descris ca software nedorit care este instalat în sistem fără consimțământ. Se poate atașa la cod legitim și se poate propaga; se poate ascunde în aplicații utile sau se poate replica pe internet. Câteva dintre cele mai frecvente tipuri de programe malware:

- Macro viruși - infecteaza aplicații și execută instrucțiuni înainte ca userul să preia controlul; se poate replica singur și atașa la alte bucăți de cod din sistem
- Torjane - este un program care la suprafață pare util, dar ascunde în spate program malițios. Acesta nu se poate replica, dar poate deschide o portiță hackerilor pentru a intra în sistem
- Worms - sunt programe malițioase de sine stătătoare; acestea se propagă pe internet, și mai ales prin intermediul atașamentelor pe email.

3.5 Factorul uman / Privilegiile

Cauza principală a 30 la sută din incidentele de încălcare a datelor este neglijența umană, potrivit studiului Ponemon Institute Cost of Data Breach Study: "De multe ori acest lucru se datorează lipsei de expertiză necesară pentru implementarea controalelor de securitate, aplicarea politicilor sau desfășurarea proceselor de răspuns la incidente".

Utilizatorii pot abuza de privilegii legitime de acces la date în scopuri neautorizate. De exemplu, un utilizator în vânzări cu privilegii de a vizualiza înregistrările individuale ale clienților poate abuza de acest privilegiu pentru a lua toate înregistrările clienților și a le transmite unui concurent.

Politicile bune de angajare vor reduce probabilitatea ca acest lucru să apară, dar ar trebui să fie pusă în aplicare prin măsuri tehnice și prin înregistrarea și monitorizarea eficientă pentru a detecta abuzul.

4 Cum ne protejăm?

4.1 Encriptarea datelor

Odată ce datele sensibile și confidențiale au fost identificate, este o bună practică să se folosească algoritmi robuști pentru a cripta aceste date.

Atunci când atacatorii exploatează o vulnerabilitate și au acces la un server sau sistem, primul lucru pe care vor încerca să-l fure este baza de date. Cel mai bun mod de a proteja o bază de date este de a o face ilizibilă pentru orice persoană care o accesează fără autorizație.

4.2 Firewalls

Firewall-urile îmbunătățesc securitatea bazei de date prin refuzarea traficului atunci când este necesar pentru a minimiza intrarea amenințărilor. Când sunt configurate corect, acestea ar trebui să permită traficul de la anumite aplicații și servere web care trebuie să acceseze datele și ar trebui, de asemenea, să împiedice baza de date să inițieze conexiuni de ieșire (în afară de cele necesare).

În plus, punerea unui firewall pentru aplicații web ajută în protejarea serverelor și crește securitatea bazei de date. Fără unul, atacurile aplicațiilor web ar putea fi utilizate pentru a șterge sau colecta date din baza de date.

4.3 Backup & Updates

Crearea unei copii de rezervă a fișierelor, de preferință bazată pe cloud, este o altă bună practică în securitatea și gestionarea bazelor de date. Indiferent dacă se păstrează datele brut sau versiunea criptată a bazei de date, o copie de rezervă în oglindă în cloud este o asigurare suplimentară.

De asemenea, trebuie să existe o persoană desemnată sau o echipă care să urmărească atent diferitele programe antivirus și anti-malware instalate pe serverul bazei de date și să le reînnoiască, atât cât să prevină expirarea acestora, cât și să fie la curent cu ultimele versiuni îmbunătățite ale programelor.

4.4 Accesul la baza de date

Ideal pentru o bază de date este ca un număr cât mai mic de persoane să aibă acces la ea. Administratorii ar trebui să aibă doar privilegiile minime de care au nevoie pentru a-și face treaba și numai în perioadele în care au nevoie de acces.

Pentru o organizație mai mare, o practică comună este automatizarea gestionării accesului utilizând un software de gestionare a accesului. Acesta poate oferi utilizatorilor autorizați o parolă temporară cu privilegiile de care au nevoie de fiecare dată când au nevoie să acceseze o bază de date. De asemenea, înregistrează activitățile desfășurate în acea perioadă și împiedică administratorii să partajeze parolele.

Totodată, este bine ca serverul de baze de date să se afle într-un mediu securizat, blocat, cu controale de acces pentru a menține persoanele neautorizate afară.

5 Concluzia

În concluzie, așa cum am prezentat anterior, există multe modalități prin care integritatea unei baze de date poate fi afectată, mai ales acum când lumea este interconectată mai mult decât niciodată, iar pericolele pot apărea din cele mai neașteptate locuri, dar măsurile de atenuare a acestor amenințări rămân aceleași: protejarea prin firewalls, menținerea acestora updatate, encriptarea datelor, cât și backup-urile frecvente și pregătirea bună a angajaților pentru a diminua factorul uman de eroare.