МЕЃУНАРОДЕН СЛАВЈАНСКИ УНИВЕРЗИТЕТ
„ГАВРИЛО РОМАНОВИЧ ДЕРЖАВИН“
СВЕТИ НИКОЛЕ – БИТОЛА
РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА



ФАКУЛТЕТ ЗА ИНФОРМАТИКА
СТУДИСКА ПРОГРАМА: СОФТВЕРСКИ ТЕХНОЛОГИИ

МАГИСТЕРСКИ ТРУД

ЗАШТИТА НА ПОДАТОЦИТЕ ВО БАЗА СО ПОДАТОЦИ

СТУДЕНТ: **НАУМ ПАВЛОВ**
БРОЈ НА ИНДЕКС: **M189003**
МЕНТОР: **ПРОФ. Д-Р АЛЕКСАНДАР ПЕТРОВСКИ**

Свети Николе, 2021

Апстракт:

Во денешниот свет, податоците се генерираат со голема брзина и крајната дестинација на таквите податоци е базата на податоци. На компаниите им се потребни бази на податоци за складирање на секаков вид на податоци, а брзината и достапноста на базата на податоци ги намалуваат трошоците и ја зголемуваат популарноста. Предност на користење на база со податоци е тоа што автоматизира различни процедури, заштедува ресурси и човечки часови работа. На пример, наместо рачно да се проверуваат трансакциите, корисниците можат да ги искористат компјутерските извештаи зачувани во базата на податоци. Наместо рачно да се внесуваат информации за стоки или залихи, може да се користат рачни скенери за зачувување на информации во базата на податоци. Базата на податоци може да обезбеди ефикасност и брзина на секое современо работно место.

Следното прашање за секоја компанија е:

- „**Дали податоците се безбедни со користење на база на податоци**? “

Безбедноста во денешниот свет е една од најважните и предизвикувачки задачи со кои се соочуваат луѓето низ целиот свет во секој аспект од нивниот живот. Базите на податоци се комплексни и многу професионалци за безбедност на базите со податоци немаат целосно разбирање за ризиците и безбедносните прашања поврзани со различни бази на податоци.

Податоците се чуваат во базата на податоци заради лесен и ефикасен начин за управување со овие податоци. Сите операции со податоците, манипулацијата и одржувањето се вршат со користење на системи за управување со базите на податоци. Имајќи ја предвид важноста на податоците во организацијата, апсолутно од суштинско значење е да се обезбедат податоците присутни во базата на податоци[1]. Сигурна база на податоци е онаа база со податоци што е заштитена од различни можни напади. Безбедносните модели се потребни за развој на бази на податоци. Овие модели се различни во многу аспекти со кои се занимаваат со различни прашања за безбедноста на базата на податоци. Тие можат да бидат различни, затоа што земаат различни претпоставки за тоа што претставува безбедна база на податоци.[2] Значи, станува многу

[1] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

[2] Sohail IMRAN, Dr Irfan Hyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009

тешко за администраторите да изберат соодветен модел за обезбедување на нивната база на податоци. Обезбедувањето база на податоци е важен пристап за планирање на експлицитна и директна база на безбедност на базата на податоци. Обезбедувањето безбедност за базата на податоци е многу критично прашање за компаниите. Како сложеноста и големината на базата на податоци се зголемуваат, така постои тенденција да имаме покомплексни безбедносни проблеми на базата со податоци.

Клучни зборови:

заштита на податоците, заштита на информациските системи, заштитни објекти, мерки на заштита, ризик

Abstract:

In today's world, data is generated at high speed and the final destination of such data is database. Companies need databases to store all kinds of data, but the speed and availability of the database reduces costs and increases popularity. The advantage of using the database is that it automates various procedures, saves resources and man-hours of work. For example, instead of manually checking transactions, users can use computer reports stored in a database. Instead of manually entering information about goods or stocks, handheld scanners can be used to store information in the database. The database can provide efficiency and speed to any modern workplace.

The next question for any company is:

- "Is the data secure using a database?"

Security in today's world is one of the most important and challenging tasks that people all over the world face in every aspect of their lives. Databases are complex and many database security professionals do not fully understand the risks and security issues associated with different databases.

The data is stored in the database for an easy and efficient way to manage this data. All data operations, manipulation and maintenance are performed using database management systems. Given the importance of data in the organization, it is absolutely essential to secure the data present in the database. A secure database is one that is protected from various possible attacks. Security models are needed for database development. These models are different in many respects dealing with different database security issues. They can be different, because they take different assumptions about what a secure database is. So, it becomes very difficult for administrators to choose the appropriate model for securing their database. Database security is an important approach to planning explicit and direct database security. Ensuring database security is a very critical issue for companies. As the complexity and size of the database increases, we tend to have more complex database security issues.

Keywords:

data protection, information systems protection, security objects, protection measures, risk

Содржина

АПСТРАКТ.....
ВОВЕД.....06
1. "Златни прашања" на информатичката заштита …….....11
1.1.Основни поими за бази со податоци 12
1.2.База на податоци – модели на податоци…….....……12
1.3.Цели за воведување на бази со податоци…….....…13
1.4.Архитектура на бази со податоци…….....…….15
1.5.Јазици за работа со бази на податоци…….....……...…16
1.6."SQL Server Management Studio"…….....……..17
2. Главни ентитети (субјекти) на проблемот за заштита……..…….……...18
2.1.Објекти……....…..……..18
2.2.Закани……....……..……..…19
2.2.1. Пресек……..…….....19
2.2.2. Пресретнување……..……19
2.2.3. Измена – Промена……..……20
2.2.4. Фабрикување……..…..20
2.3.Последици……....……..……21
2.4.Мерки……....……..….21
2.5.Политика……....…….....22
3. Анализа и процена на ризик……..……..……22
4. Закани за базата на податоци……..……..24
4.1.Прекумерни привилегии……....……..….24
4.2."SQL" Вбризгување (SQL Injections)…….....……25
4.3.Малициозен софтвер……..……....……26
4.4.Слаба ревизорска трага……..……....……26
4.5.Изложеност на резервна копија…….....……27
4.6.Слаба автентикација…….....……28
4.7.Ранливост на ДБ и погрешна конфигурација…….....……..28
4.8.Неменаџирани чувствителни податоци…….....……29
4.9.Одбивање на услугата……...……....……29
4.10. Ограничена безбедносна експертиза и едукација……....……29
5. Стратегии за заштита на информациските системи……..…..……..29
6. Методи за контрола на закани кон бази со податоци…….....……32
6.1.Контрола на пристап……..…....……33
6.2.Полиси за заклучување……....……33
6.3.Идентификација / автентикација на корисник……..……....……34
6.4.Отчетност и ревизија……..……....……34
6.5.Шифрирање (енкрипција)……..……35
6.6.Правила за лозинки……..……....…..35
6.7.Автентикациски протоколи……..……....……36
7. Напади и ризици……..……36
7.1.Надворешни и внатрешни напади……..……....……36
7.2.Ризици од губење на податоци…….....……38
7.3.Ризик на рејтинг…….....……38
7.4.Ризик на спроводливост……..……....…..39
7.5.Ризик од судски спор…….....……40
8. Заштита на податоците со шифрирање……..……..……40
8.1.Социјален инженеринг како битен фактор при развој на стратегија….....41
8.2.Планирање на стратегија на шифрирање во база со податоци…….....41

8.3.Криптографија и криптографски алгоритми…….....……...42
8.4.Влијание на шифрираните податоци на базата со податоци…….....….43
8.5.Текови на податоците на апликативно ниво…….....……..44
8.6.Стратегија за управување со криптографските клучеви…….....…..45
8.7.Потребен број на клучеви и начин на управување…….....….46
8.8.Сигурно место за чување на клучеви…….....……...46
8.9.Заштита на пристапот до клучевите…….....…..46
9. Репликација на податоци и типови на репликација…….……..47
9.1.Репликација Слика - “Snapshot”…….....…48
9.2.Репликација Трансакциска -“Transactional”…….....……49
9.3.Репликација Спојување - “Merge”……..…....…….50
9.4.Хетерогени репликации на бази на податоци…….....…..53
10. Статистика која загрижува…….…….53
11. Загуба на податоци……..……55
12. Со броеви: Цена на чинење на губење на податоци на помала скала…….....56
13. Реален пример на добра заштита на база со податоци.....59
Заклучок.....63
Користена литература.....65

ВОВЕД

Базата на податоци може да се дефинира како збирка на податоци што се зачувува во компјутерските системи. Базите на податоци му овозможуваат на секој овластен корисник да пристапува, внесува, анализира и обработува податоци, брзо и лесно. Тоа е колекција на табели и прегледи. Податоците зачувани во базите на податоци обично се организираат на моделирање на аспекти кои ги поддржуваат процесите за кои е потребно складирање и враќање на информациите. Податоците се чуваат во складиштето наречено база на податоци. Корисничкиот интерфејс за базите на податоци се нарекува систем за управување со базата на податоци. DBMS е софтверска апликација која комуницира со овластените корисници, со други апликации и со самата база на податоци за преглед и анализа на податоци. Тоа помага да се организираат податоци за подобри перформанси и побрза обработка.

Заштитата на базите со податоци има многу важна улога во информационите системи. Цел на секоја организација е да ги заштити осетливите податоци во базите со податоци. Мрежните бази со податоци претставуваат срце на секоја организација. Сите субјекти коишто имаат бази со податоци, особено таму каде што има осетливи податоци, мораат да ги заштитат своите податоци. Базите со податоци содржат деловни информации, информации за трансакции, финансиски податоци, лични податоци за вработени или за деловни соработници.

Сложените процеси кои се извршуваат во рамки на компјутерските системи, ниту во еден момент и во ниедна точка не смеат да се потценат, затоа што опасностите, коишто посредно или непосредно, постојано или повремено, ги загрозуваат тие процеси, во некој облик претставуваат закана за системот или неговите сегменти.

Базите на податоци се омилена цел за напаѓачите поради нивните доверливи и важни податоци. Постојат многу начини на кои може да се загрози нивната безбедност. Развиени се многу различни видови напади и закани од кои треба да се заштити базата на податоци. Тие му откриваат клучни или важни податоци на напаѓачот.

Според многу ИТ експерти, многу компании не се свесни за тоа кои бази на податоци, табели и колони содржат чувствителни податоци. Тоа е затоа што тие користат најразлични неповрзани апликации или немаат записи или документација за моделите на податоци. Дури и со целосно познавање на базите со податоци многу е тешко да се обезбедат бидејќи тие се уникатни имплементации и процедури за базите на податоци. Можеме да кажеме дека безбедноста на базите со податоци содржи широк спектар на

контроли на безбедност на базите за заштита на податоци од какви било напади (внатрешни или надворешни), наспроти компромисот за доверливост, интегритет и достапност на базите со податоци. Безбедноста вклучува различни видови на контроли, како што се: техничките, административните и физичките контроли. Слично на тоа и безбедноста во електронскиот свет има големо значење. Заштита на доверливите - чувствителните податоци зачувани во складиштето е всушност безбедност на базата со податоци. Постојат различни безбедносни слоеви во базите со податоци. Овие слоеви се: администратор на база, систем администратор, администратор за безбедност, програмери и вработени. Безбедноста може да се наруши во кој било од овие слоеви од страна на напаѓачот.

Заштитата на информационите системи, а со тоа и заштитата на базите со податоци подразбира преземање на одредени мерки и чекори за да се заштитат податоците и документите со кои се располага од непредвидени настани и несакани последици.

Заканите се толку многубројни, меѓусебно поврзани и испреплетени, така што формираат комплексна мрежа на опасности во целиот информациски систем. Затоа, постои зголемена потреба за оневозможување на какви било случајни или намерни, „од какви било непланирани и неочекувани причини“, нарушување, стеснување или спречување на функциите на компјутерските системи или отуѓување, уништување, оштетување, модификација или неовластено користење на информативни ресурси (хардвер, софтвер, програми, податоци, ...), туку да се создадат сите потребни услови за да се одвиваат функциите и податоците и информациите да бидат обработени и користени на очекуваниот и однапред дефиниран начин.

Споменатите видови на податоци и информации често претставуваат мета на напаѓачите. Успешен напад може да предизвика огромни финансиски штети на компанијата и да го наруши нејзиниот корпоративен углед. Често мета на напади се трансакциите кои се одвиваат на нет-опкружувањето, коишто на компаниите им го загрозуваат кредибилитетот и односите со клиентите. Единствен начин за да се заштитат базите со податоци е да се преземат одредени мерки и регулативи за заштита. Мерките за заштита вклучуваат шифрирање на податоците кои се разменуваат низ мрежата и податоците кои се наоѓаат на уредите за складирање на податоци. Друг проверен метод на заштита е контрола на пристапот на базите со податоци. Овој метод заштитува од

неовластен пристап на напаѓачи. Да се изгради стратегија за заштита на базите со податоци е многу важен и сложен сегмент.[3]

Стратегијата за заштита на податоците е важна и комплексна. Еден од посредните услови за успешност на решенијата за заштита претставува и неговата едноставност за употреба. Идеално, во конкретните решенија, е корисниците што помалку да чувствуваат присуство на криптографски решенија, т.е. да не им се усложнува работата и значајно да не се менуваат временските ресурси при извршувањето на работните процеси. Реализацијата на заштитата над самата база со податоци обезбедува одличен метод на заштита на осетливите податоци, но од друга страна, доведува до намалување на перформансите и ја усложнува употребата. Тоа значи дека може да се шифрираат само одредени важни податоци, како што се: броеви на кредитни картички, податоци за клиентите и сл. Ќе прикажеме постапки за шифрирање внатре во базата со податоци, како и реализација на процес на шифрирање на страна на апликативниот сервер. Низ анализа на перформансите на наведените решенија детално се анализираат сложеноста на реализацијата и оптовареноста на серверот.

Исто така, ќе претставиме некои од нападите што можат да бидат кон базите со податоци и можните и контрамерки и нивните контролни методи што можат да се применат. Ќе се споменат повеќе решенија за повеќето од заканите, иако некои решенија се добри, додека некои се само привремени.

Може слободно да констатираме дека сè се врти околу информациите и затоа мора да се посвети поголемо внимание на нивната заштита. Работата со бази на податоци, т.е. складирањето на податоците се токму тој сегмент.

Информатиката како наука е доста млада, но во исто време таа е наука којашто е многу брзорастечка и променлива. И покрај големата достапност на литература во најразлични облици, пред да ја изберам темата за мојата магистерска работа, сметав дека литературата достапна за овој сегмент на нашиот мајчин македонски јазик е доста оскудна. Сето тоа придонесе да се зафатам со обработка на еден сегмент од оваа област.

Во мојот магистерскиот труд на тема **“Заштита на податоците во базата со податоци“** предмет на истражување ќе биде да се прикаже важноста на податоците во базите со податоци и нивната заштита, можните злоупотреби на податоците и

[3] McDonald D., C. Metz, B. Phan, "PF_KEY Key Management API, Version 2" IETF RFC 2367, 1998.

влијанието на губењето на податоците од базите со податоци врз развојот на компаниите.

Цел на истражувањето би била како и колку влијае заштитата на податоците во работата на компаниите. Со истражувањето ќе се добие претстава колку позитивно или негативно можат да влијаат податоците во базите со податоци при нивно губење, оштетување или злоупотреба. Добиените научни сознанија би биле од полза за сите корисници на бази со податоци: компании, институции, невладини организации и други.

При истражувањето ќе се користи дескрипција или опишување на конкретните појави, а процесот на истражување ќе биде комбиниран, т.е. квантитативен и квалитативен метод на истражување.

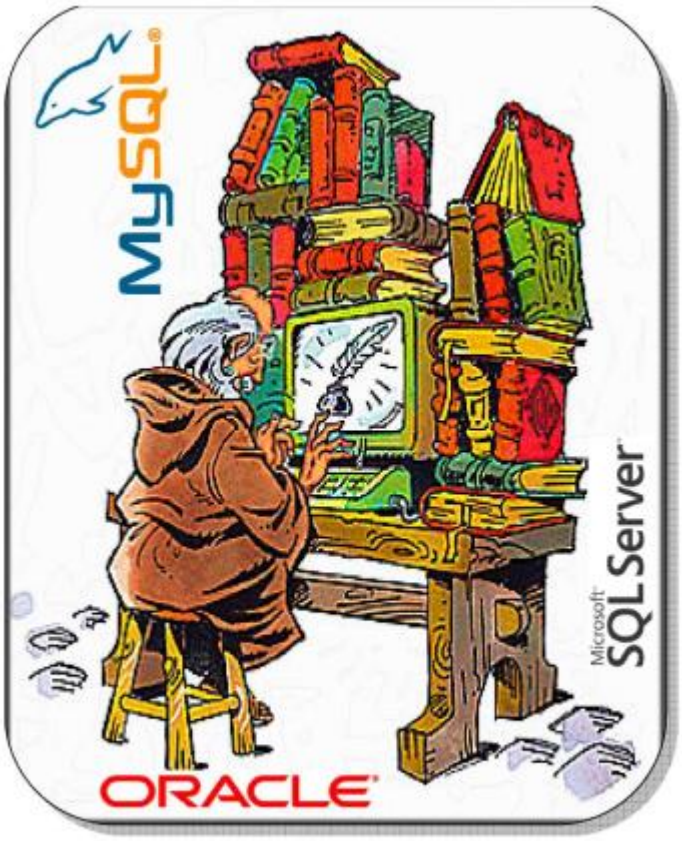
Како испитаници ќе се земат компании чиешто работење во голем дел зависи од нивните податоци складирани во бази со податоци.

Од самиот предмет и цел на истражувањето произлегува генералната хипотеза, според која се претпоставува дека заштитата на податоците во базите со податоци е важен или еден од најважните сегменти во работењето на компаниите, институциите.

Од формулираната општа хипотеза, произлегуваат следните потхипотези:

H1: Се претпоставува дека компаниите кои имаат висока заштита на податоците во базите со податоци, се сигурни и успешни во своето работење;

H2: Се претпоставува дека кај компаниите кои имаат минимална или никаква заштита на податоците во базите со податоци, има голема веројатност за неуспех, дури и комплетно затворање на бизнисот;



Бази со податоци

“Книгата е збир на податоци, но за слеп и за неписмен тоа не се информации”

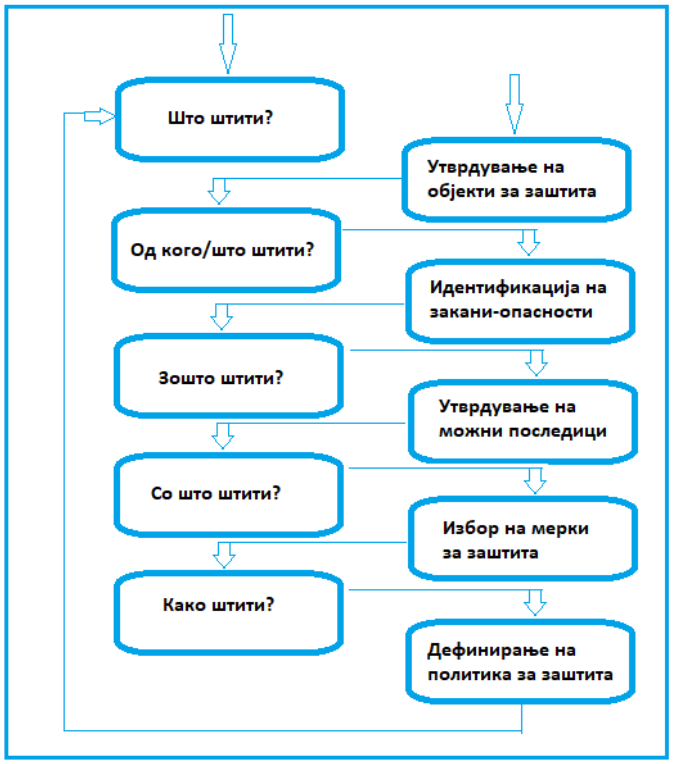
1. “Златни прашања” на информатичката заштита

Заштита на информациските системи (ИС) подразбира преземање на соодветни мерки и активности со цел да се заштитат нечии податоци со кои располагаат од можни непредвидливи настани со непожелни последици. Затоа, постои растечка потреба да се спречи какво било случајно или намерно нарушување, стеснување или спречување на функциите на компјутерскиот систем, или отуѓување, уништување, оштетување, измена или неовластено користење на информациските ресурси (хардвер, софтвер, програми, податоци и сл.). Треба да се создадат сите потребни услови со цел сите функции, податоци и информации да бидат обработени и користени на очекуван и однапред дефиниран начин. Појдовна точка за наоѓање на задоволителен глобален одговор на ова прашање е класификацијата на заканите што можат да ги загрозат информациските системи од несреќи, грешки и криминал. Врз основа на тоа, дадени се четири причини, чија анализа обезбедува делумен, а нивната синтеза целосен одговор на прашањето.

Овие причини се:

- вредност на хардверот и софтверот;
- разновидност на функциите на компјутерскиот систем;
- различноста, природата и важноста на податоците и информациите што се собираат, уредуваат, чуваат, обработуваат, дистрибуираат и архивираат во рамките на компјутерските системи;
- Карактеристики на компјутерскиот систем. Со цел да најдеме и развиеме сеопфатен пристап, кој треба да обезбеди сигурна основа за дизајнирана, организирана, професионална и рационална студија за решавање на проблеми со компјутерскиот систем, поминуваме низ изградба на соодветен систем на заштита. Се тргнува од фактот дека секој систем на заштита има смисла ако и само ако заштитува нешто, а за да ја постигне целта, мора да ја изврши својата функција со нешто и на некој начин. Од оваа општа изјава не е тешко да се забележат логичките целини, и што е многу важно, нивниот редослед, според кој е можно да се изврши потребната студија и очекуваното решавање на разгледуваниот проблем.

Овие логички целини, според принципот на „златни прашања“ од криминологијата, можат да бидат изразени со соодветни „златни прашања“ за заштита на информациите, прикажани на слика 1, за кои се потребни целосни одговори по горниот распоред.



Слика 1. “Златни прашања” на информатичка заштита

1.1. Основни поими за бази со податоци

Базите со податоци претставуваат повисоко ниво на работа со податоците во однос на класичните програмски јазици. Станува збор за технологија која настанала со цел да се средат аномалиите и слабостите на традиционалните автоматски обработки. Таа технологија овозможила поголема продуктивност, квалитет, доверливост во развојот на апликациите, кои се сведуваат на потхранување и претражување на податоците во системите.

1.2. База на податоци – модели на податоци

Базата со податоци е збир на меѓусебно поврзани податоци, зачувани во надворешната меморија на компјутерот. Податоците се достапни истовремено на различни корисници и апликативни програми. Внесувањето, промената, бришењето и читањето на податоците се одвива преку користење на заеднички софтвер. Корисниците и апликациите притоа не мора детално да ги познаваат деталите од физичкиот приказ на податоците, наместо тоа ја користат логичката структура на базата. Системот за

управување со базата со податоци "DBMS[4]" е сервер за базите со податоци. Тој го обликува физичкиот приказ на базата во согласност со бараната логичка структура. Исто така, тој ги извршува сите операции со податоците во името на клиентот. Понатаму, тој е во состојба да поддржи различни бази, од кои секоја може да има своја логичка структура, но во склад со истиот модел. Исто така, се грижи за сигурноста на податоците, т.е. ги автоматизира административните работи со базата. Податоците во базата се логички организирани во согласност со некој модел на податоци. Модел на податоци е збир на правила коишто определуваат како може да изгледа логичката структура на базата. Моделот ја прави основата за концепирање, проектирање и имплементација на базата. Досегашните DBMS обично ги поддржуваат некои од следните модели:

Релационен модел – заснован на математичкиот поим релација. И податоците и врските помеѓу податоците се прикажуваат со "правоаголни" табели.

Мрежен модел – базата е претставена со насочен граф. Јазлите се типовите на записите, а лаковите ги дефинираат врските помеѓу типовите на записите.

Хиерархиски модел – специјален случај на мрежниот модел. Базата е претставена со едно стебло или од збир на стебла. Јазлите се типовите на записите, а хиерархискиот однос "надреден - подреден" ја покажува врската помеѓу типовите на записи.

Објектен модел – инспириран е од објектно-ориентираните програмски јазици. Базата е збир на трајно зачувани објекти кои се состојат од своите интерни податоци и "методи" (операции) за ракување со тие податоци. Секој објект припаѓа на некоја класа. Помеѓу класите се воспоставуваат врски на наследување, агрегација, односно мегусебно користење на операции. Од 1980-тите години, па сè до денес, преовладува релациониот модел.[5]

1.3. Цели за воведување на бази со податоци

Спомнато е дека базите со податоци претставуваат повисоко ниво на работа со податоци во однос на класичните програмски јазици. Тоа повисоко ниво на работа се гледа во тоа што технологијата на базите со податоци настојува да ги исполни следните цели:

Физичка независност на податоците. Се раздвојува логичката дефиниција на базата од нејзината вистинска физичка градба. Значи, ако се промени физичката градба

[4] Data Base Management System – DBMS

[5] Robert Vierira: SQL Server 2005 Programiranje - 1/2006

(пример, податоците се препишуваат во други датотеки на други дискови), тоа нема да бара промена во постоечките апликации.

Логичка независност на податоците. Се раздвојува глобалната логичка дефиниција на целата база со податоци од локалните логички дефиниции за една апликација. Значи, доколку се промени логичката дефиниција (пример, се воведе нов запис или врска), тоа нема да бара промени во постоечките апликации. Локалната логичка дефиниција се сведува на издвојување само на некои елементи од глобалната дефиниција со помош на некои едноставни трансформации на тие елементи.

Флексибилност на пристапот на податоците. Во постарите мрежни и хиерархиски бази, патеките за пристап до податоците биле однапред дефинирани. Значи, корисникот можел да пребарува податоци само по оној редослед којшто бил предвиден во времето на проектирање и имплементацијата на базата со податоци. Денес се бара корисниците да можат слободно да пребаруваат по податоците, т.е. по своја желба да воспостават врска помеѓу податоците. Ова барање го задоволуваат само релационите бази со податоци.

Истовремен пристап до податоците. Базата со податоци мора да овозможи поголем број на корисници истовремено да користат исти податоци. Притоа тие корисници не смеат да си пречат еден на друг, т.е. секој од нив треба да има впечаток дека сам работи со базата со податоци.

Чување на интегритет. Се настојува автоматски да се сочува коректноста и конзистентноста на податоците, и тоа во ситуации кога постојат грешки во апликациите, т.е. конфликти од истовремени активности на корисниците.

Заштита од недозволено користење. Мора да постои можност на корисниците да им се ограничат правата за користење на базите. Треба на секој корисник да му се регулираат овластувањата и привилегиите, т.е. што тој корисник може, а што не може да прави со податоците.

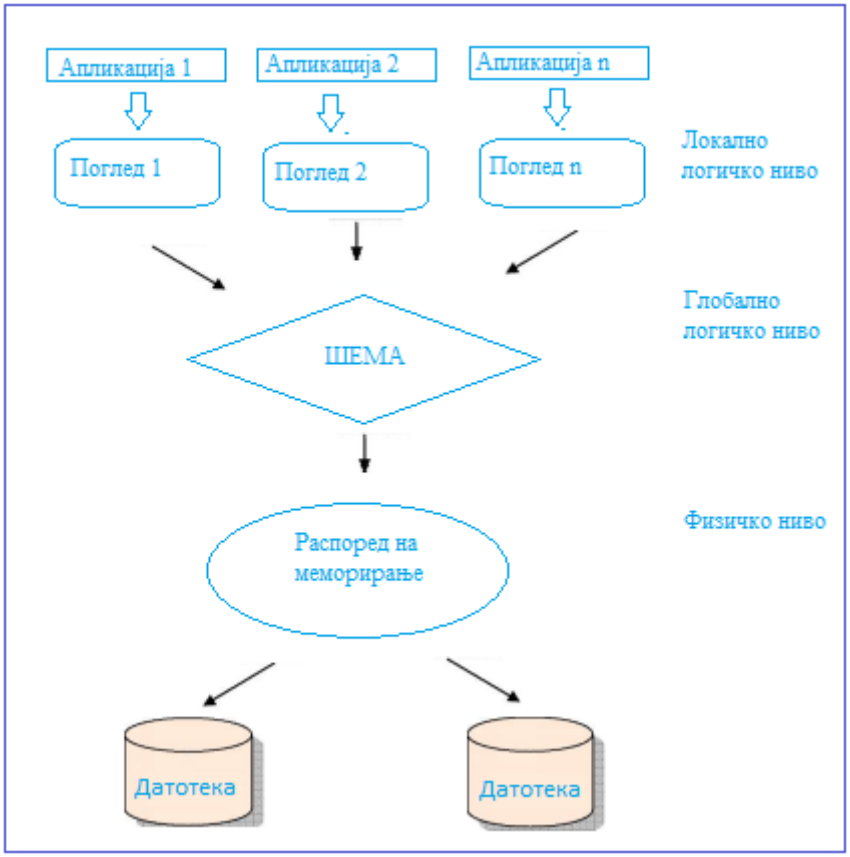
Задоволувачка брзина на пристап. Операциите со податоците мора да се одвиваат доволно брзо во согласност со потребите на одредени апликации. На брзината на пристап може да се влијае со избор на погодна физичка структура на податоците, т.е. со избор на погодни алгоритми за пребарување.

Можност за подесување и контрола. Голема база со податоци побарува голема грижа: следење на перформансите, менување на параметрите во физичката градба, рутинско следење и правење на резервни копии со податоци, регулирање на овластувањата на корисниците. Исто така, целта на базите со текот на времето се менува,

па повремено треба да се подесува и логичката структура. Сите овие операции мора да се извршуваат централизирано. Одговорното лице се вика администратор на база со податоци. На администраторот на базите со податоци мора да му се достапни на располагање разни алатки и помагала.

1.4. Архитектура на бази со податоци

Архитектурата на базата со податоци се состои од три "слоја" и интерфејси помеѓу слоевите. Како што е прикажано на слика 2, станува збор за три нивоа на апстракција.



Слика 2. Архитектура на база со податоци

Физичкото ниво се однесува на физичкиот приказ и распоред на податоците на единиците на надворешната меморија. Тоа е аспект којшто го гледаат само системските програмери (оние што го развиле DBMS). Самото физичко ниво може да се подели на повеќе поднивоа на апстракција, од сосема конкретни патеки и цилиндри на дискот, до некаде апстрактни поими на датотеките и записите какви што среќаваме во класичните програмерски јазици.

Распоредот на меморирање опишува како елементите од логичките дефиниции на базата се пресликуваат на физичките уреди.

Глобалното логичко ниво се однесува на логичката структура на целата база. Тоа е аспект којшто го гледа проектантот на базата, односно нејзиниот администратор. Записот на логичката дефиниција се нарекува "шема". Шема е текст или дијаграм кој ја дефинира логичката структура на базата, а е во согласност со зададениот модел. Значи, се дефинираат и се именуваат сите типови на податоци и врски помеѓу тие типови во согласност со правилата на моделот што се користи. Исто така, шемата воведува и ограничувања со коишто се чува интегритетот на податоците.

Локално логичко ниво се однесува на логичкиот дел којшто го користи некоја единечна апликација. Тоа е аспект којшто го гледа корисникот или програмерот на апликацијата. Записот на една локална логичка дефиниција се вика "поглед" или потшема. Тоа е текст или дијаграм со кој се именуваат и се дефинираат сите локални типови на податоци и врските помеѓу тие типови во согласност со правилата на моделот којшто се користи. Истотака, погледот дава пресликување со кое од глобалните податоци и врски се изведуваат локални. За креирање на база со податоци потребно е да се зададат само шема и погледи. DBMS тогаш автоматски генерира потребен распоред на меморирање и физичка база. Администраторот може само до некаде да влијае на физичката градба на базата преку подесување на параметри кои му се достапни. Апликациите и корисниците не пристапуваат директно на физичката база, туку добиваат податоци со посредство на DBMS. Комуникацијата на апликациите, т.е. корисниците со DBMS, се одвива на локално логичко ниво.[6]

1.5. Јазици за работа со бази на податоци

Комуникацијата на корисниците, т.е. на апликациите и DBMS се одвива со помош на посебни јазици. Тие јазици традиционално се делат на следните категории:

Јазик за опис на податоци (Data definition Language - DDL). Му служи на проектантот на базата или на администраторот со цел за запишување на шемите или погледите. Значи, со тој јазик се дефинираат податоците и врските помеѓу податоците и тоа на логичко ниво. Понекогаш постои посебна варијанта на јазикот за шемата, а посебна варијанта за погледите. Наредбите "DDL" обично потсетуваат на наредби кои

[6] Gordana Pavlovic-Lazetic: Uvod u relacione baze podataka

се за дефинирање на сложени типови на податоци во јазиците, како што се: Cobol, C, Pascal.

Јазик за манипулација на податоци (Data Manipulation Language – DML). Го користат програмерите за воспоставување на врски помеѓу апликациските програми и базите со податоци. Наредбите DML овозможуваат "маневрирање" по базата, т.е. едноставни операции, како што се: запис, промена, бришење или читање на податоци. Во некои софтверски пакети, DML е библиотека од потпрограми. Наредба во DML се сведува на повик на потпрограми. Во други пакети навистина станува збор за посебни јазици: програмерот тогаш пишува програма во која се измешани наредби од двата јазика, па таквата програма треба да се преведува со два преведувачи (DML- precompiler, обичен compiler).

Јазик за поставување на прашања (Query Language – QL). Го користи непосредниот корисник за интерактивно пребарување на базата. Тоа е јазик кој потсетува на говорниот (англиски) јазик. Наредбите се непроцедурални, така што го специфицираат резултатот којшто сакаме да го добиеме, а не и постапката за добивање на резултатот.

Оваа поделба на три јазици денес е веќе поприлично застарена. Имено, кај релационите бази со податоци постои тенденција сите три јазици да се обединат во еден заеднички. Пример за таков интегриран јазик за релациони бази со податоци е SQL: тој служи за дефинирање на податоци, обработка и пребарување. Интегрираниот јазик може да се користи интерактивно (преку online интерпретер) или тој може да се појави вклопен во апликациските програми. Треба да се нагласи дека горе споменатите видови на јазици не се програмски јазици. Значи, тие јазици ни се потребни за да се поврземе со базата, но тие не се доволни за развој на апликација којашто ќе работи со податоците од базата.

1.6. "SQL Server Management Studio"

"SQL Server Management Studio" е основна алатка која се користи за управување со база на податоци и објекти на таа база. Менаџмент-Студио е алатка која го опфаќа "Enterprise Manager" и "Analyzer". "SQL Server Management Studio" за многумина е основен алат за администрација на "SQL Server". Со помош на алатките на Сервер Менаџмент-Студио може да се извршуваат следните операции:

- Креирање, менување и бришење бази на податоци и објекти во бази на податоци;
- Да се дознае кои системски бази на податоци се добиваат со "SQL Server";

- Да се управува со распоредот на задачи, како што се правење на заштитни копии и придвижување на извршување на пакетот “SSIS”;
- Да се покажува моменталната активност, како на пример, информации за тоа кој е пријавен, кои објекти се заклучени и кој клиент ги користи;
- Управување со безбедноста, вклучувајќи работи како што се: правила, налози и оддалечени и поврзани сервери;
- Да се иницира Дата база Меил Сервис и да се управува со него;
- Правење каталози на сервисот “Full-taxt search” и да се управува со него;
- Управување со параметрите за конфигурација на сервер;
- Да се објавува и пријавува база на податоци за реплицирање и да се управува со тие процеси;

Кога ќе се воспостави врска со серверот која е зададена, ќе се појави екран од “SQL Server Management Studio” кој се користи.

2. Главни ентитети (субјекти) на проблемот за заштита

Главните субјекти на проблемите за заштитата од областа на информациските системи се: објекти, закани, последици, мерки и политики на политики. Овој пристап овозможува проблемот на заштита, за јасно и полесно набљудување на постојните меѓузависности, да се претстави во форма на тридимензионална матрица. Во тридимензионалната матрица секој елемент претставува збир на мерки што треба да се применат за да се спречат последиците, коишто може да се случат ако заканите се реализираат.

2.1. Објекти

Прашање: - **Што треба да се заштити**?

Тоа е првиот клучен чекор во проучувањето и решавањето на безбедносните проблеми во информациските системи. Доколку множеството одговори на прашањето е празно множество, нема потреба да се преземаат активности во оваа област. Сепак, како еден од основните критериуми при утврдување на предметите на заштита е нивната вредност за лицето на кое припаѓаат.

Јасно е дека овој сет на мерки сигурно нема да биде празен. Напротив, во секој информативен систем има цела низа предмети, чии вредности недвосмислено ја наметнуваат потребата за нивна заштита. Значи, заштита треба да се прави на следните

објекти: податоци, датотеки, бази на податоци, документи, програми, опрема за комуникација, компјутерски хардвер итн.

2.2. Закани

Прашање: - **Од кого или од што треба да се заштити базата со податоци**?

Ќе се добијат одговори што ги содржат сите класични ризици, како што се: пожар, вода, експлозија, хардверски грешки и друго. Но, исто така, ќе се добијат и одговори кои содржат и специфични закани, како што се: компромитирање, компјутерски криминал и други. Овие специфични ризици обично имаат нематеријално потекло или манифестација што го докажува нивното постоење, како и проценката за можни загуби и истото го прави многу тешко. Одредена тешкотија е претставена со неограничен број закани што можат да го загрозат информативниот систем, па затоа е невозможно сите да се предвидат. Меѓу одредени закани, постои одредена меѓузависност што го комплицира влијанието врз информацискиот систем. Заканите насочени кон нарушување на безбедноста на протокот на информации во компјутерските системи и мрежи генерално може да се класифицираат во четири основни категории.

2.2.1 Пресек

Пресек, т.е. прекин е напад врз достапноста. Пресекот го прекинува протокот на информации, т.е. обезбедувањето услуга или функционирањето на системот е оневозможено. Овој вид напад е активен (слика 3).

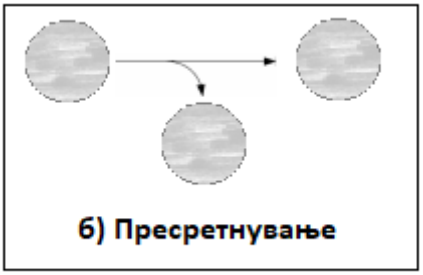


Слика 3. Пресекување

2.2.2. Пресретнување

Пресретнување е напад врз доверливост. Во пракса пресретнувањето може да биде прислушување на сообраќајот, следење на неговиот интензитет, увид во чувствителни информации и друго. Како пасивен напад, тешко е да се открие бидејќи не ги менува

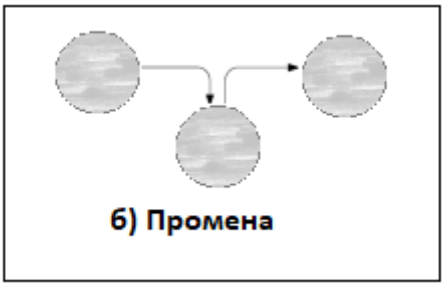
податоците, т.е. не влијае на внатрешното функционирање на системот. Овој вид напад понекогаш е подготвителна фаза за друг вид напад (слика 4).



Слика 4. Пресретнување

2.2.3. Измена-Промена

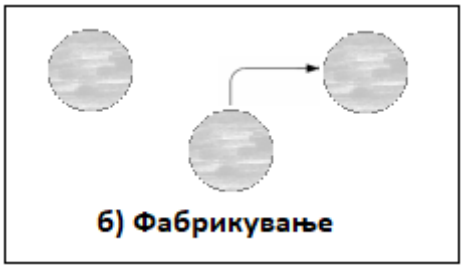
Измена - промена е напад врз интегритетот. По својата природа тоа е активен напад. Тоа се случува на патека за пренос или во рамките на компјутерскиот систем кога станува збор за промена на податоци, права за пристап, како работат програмите или системите и слично. Иако ги менува податоците или системот, нападот честопати останува незабележан некое време или поради невнимание или поради сложените техники што се користат при овој напад (слика 5).



Слика 5. Промена

2.2.4. Фабрикување

Фабрикување е напад врз автентичност. Напаѓачот го извршува овој активен напад преку генерирање лажни податоци, лажен сообраќај или издавање на неовластени команди. Исто така, многу често се користи лажна репрезентација на корисник, услуга, сервер, веб-страница или друг дел од системот (слика 6).



Слика 6. Фабрикување

2.3. Последици

Прашање: **Зошто да се заштити?**

Со одговар на ова прашање се утврдуваат негативните последици што можат да ги предизвикаат идентификуваните закани. Некои категории на овие последици се: делумно или целосно оштетување, отуѓување, модификација на хардвер и софтвер, откривање на податоци, исклучување на системот... Сето ова влијае на зголемување на загубите и треба да ги намали загубите предизвикани од овие закани.

2.4. Мерки

Прашање: **Со што да се заштитиме**?

Добиваме идентификација за сите мерки кои ни се достапни при изградбата на целосен и сигурен систем за заштита. Сите овие мерки, според нивните природни својства што ги карактеризираат, можат да се класифицираат како:

- *Мерки од нормативен карактер* - законски, организациски и кадровски мерки кои спаѓаат во категоријата на нетехнички мерки. Главната карактеристика на овие мерки е тоа што тие не ја деградираат работата на системот, но значително придонесуваат за зголемување на неговата достапност и продуктивност, а истовремено и значително влијаат на ефикасноста на системот за заштита (на пример, права за пристап и употреба на податоци);
- *Физички и технички мерки* - ги условуваат нивните финансиски инвестиции пред да започнат да дејствуваат, т.е. однапред, плус трошоците за нивното тековно одржување. Таквите трошоци можат точно да се проценат и изборот да се прилагоди на достапните финансиски можности. Сепак, ефективноста на овие мерки се намалува кога нормативните мерки не се применуваат на соодветен начин (на пример, физичка безбедност на ИС, ограничувачки простор, кафез на Фарадеј, крипто уреди, итн.);
- *Логички мерки* - тие се моќно средство за заштита. Висок степен на ефикасност се постигнува со употреба на логички мерки „во пакет“. Од друга страна, овие мерки

повлекуваат т.н. скриени трошоци, бидејќи тие директно влијаат на намалувањето на достапноста и ефикасноста на компјутерскиот систем, а тоа е доволна причина да се пристапи кон нивната примена крајно одговорно, смислено и рационално;

- *Криптолошки мерки за заштита* – тие се многу важни мерки и во комбинација со мерките за заштита од компромитирачко електромагнетно зрачење, овозможуваат постигнување на високо ниво на заштита. Сепак, овие мерки не се доволни за да ја обезбедат потребната заштита самостојно, бидејќи ефективноста на овие мерки значително се намалува доколку нормативните мерки не се применуваат соодветно.

2.5. Политика

Главното прашање е: **Како да се заштити?**

Значи воспоставување стратегија за управување со ризик во опкружувањето на информациските системи. Затоа, се пристапува кон процесот на анализа и проценка на ризикот.

3. Анализа и процена на ризик

Анализата и проценката на ризикот ја одредува веројатноста за појава на ризик, анализа на меѓузависноста на ризични настани, квантифицирање на влијанието на одделни настани или нивна комбинација врз системот. Тоа е постапка што се користи за проценка на веројатноста за закани и потенцијална загуба што може да произлезе од чувствителноста на системот. Крајната цел на анализата на ризикот е да помогне во избор на ефективни заштитни мерки кои го намалуваат ризикот на прифатливо ниво.

Бројни методи и техники се достапни за да се изврши анализа на ризик, кои се разликуваат по природата, ширината и длабочината на покриеност. Нивната примена за проценка на проблемите со заштитата треба да се одлучи врз основа на нивната можност да обезбедат разумни и документирани одговори на основните прашања поврзани со дизајнирањето и спроведувањето на системите за заштита во одредена средина.

Големината на можното влијание на идентификацијата на ризикот може да се утврди преку:

- *Квантитативните анализи*, кои вклучуваат анализа во која ризикот се изразува и проценува (пресметува) со нумерички квантитативни параметри, како и влијанието на ризикот врз целите на проектот и веројатноста дека ќе се појават овие ризични настани.

- *Квалитативните проценки*, кои се вршат врз основа на факторите на системска флексибилност и веројатност за промени во ИС. На пример: ниско, умерено или високо ниво на ризик.

Управувањето со ризикот може да се дефинира како збир на методи и техники на управување кои ги минимизираат загубите и ги усогласуваат трошоците што ја намалуваат веројатноста за настанување на загуба со трошоците што би резултирале од ризик. Всушност, се спроведува некаков вид на анализа на трошоци / придобивки.

Клучните фактори на ризик се:

1. Ризичен настан, појава или активност што може да предизвика штета или несакани последици за информацискиот систем.
2. Веројатност за појава на ризичен настан.
3. Големината на влоговите, односно големината на загубата што може да настане ако се појави ризичен настан.

Равенката која се користи за проценка на ризик:

$$r = f \cdot g$$

каде што:

r - ризик,

f - фреквенција (веројатност) на појава на закана,

g - еднократна загуба (големина на можна штета).

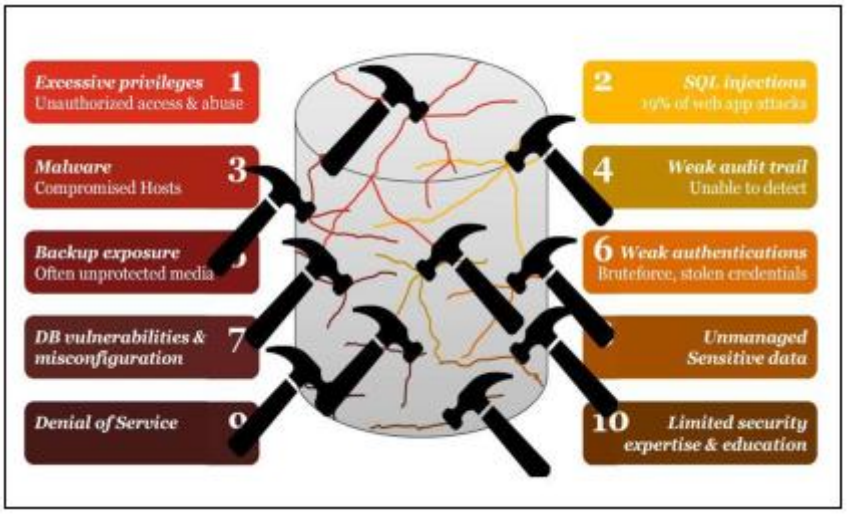
Ова се клучните елементи на анализата на ризик. За секоја идентификувана закана во однос на набљудуваниот предмет, треба да се утврди веројатноста за појава и големината на штетата (изразена со нумерички или вербален квалификатор) што заканата може да ја предизвика, имајќи предвид дека единствениот фактор на несигурност е временската рамка во која ќе се реализира заканата и дали ќе се реализира.

При утврдување на веројатноста за појава на идентификувани закани, мора да се започне од специфична средина и реални услови, бидејќи, на пример, веројатноста за појава на некои природни катастрофи може да биде многу голема во некои географски области, додека во други заканата е незначителна; изложеноста на терористички акции е карактеристична за контроверзните области и информациските системи со посебна

намена. Само систематска анализа на ризик може да обезбеди основа за формирање збир на ефективни мерки за заштита.[7]

4. Закани за базата на податоци

Базите на податоци денес се соочуваат со различен вид на напади. Пред да ги опишеме техниките за обезбедување на базите со податоци, подобро е прво да се опишат нападите што можат да се извршат врз базите на податоци. Најголем број од нападите врз базите со податоци може да се категоризираат како што е прикажано на слика 7. Овие напади понатаму се елаборирани во следните делови.



Слика 7. Закани за базите со податоци

4.1. Прекумерни привилегии

Привилегиите на базата на податоци можат да бидат злоупотребени на многу начини. Корисникот може да ја злоупотреби привилегијата за неовластена цел.

Злоупотребата на привилегиите може да се изведе на различни начини:

- прекумерна злоупотреба на привилегија;
- злоупотреба на легитимни привилегии;
- злоупотреба на неискористена привилегија;

Овој вид на злоупотреба на привилегиите како вид на закани е најопасен затоа што овластените корисници прават злоупотреба на податоци. Овие привилегии можат да

[7] Emil BURTESCU, Database Security- Attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009

бидат злоупотребени и да создадат непотребен ризик. Доделувањето на прекумерни привилегии е проблематично од две причини. Околу 80% од нападите врз податоците од базите со податоци во компаниите се всушност извршени од вработени или поранешни вработени. Доделувањето на прекумерни привилегии или ненавременото укинување на тие привилегии го прави многу едноставен начинот за да ги извршуваат своите напади. Некои од овие напади може дури и да се извршат ненамерно или без перцепција на тие дејствија како незаконски. Злоупотребата на легитимните привилегии може да се смета за ранливост на базата со податоци, доколку злонамерен корисник ги злоупотребува своите привилегии за пристап до базата со податоци.[8]

Контрамерки за злоупотреба на привилегија вклучуваат:

- Политика за контрола на пристап - да не се даваат непотребни привилегии на корисникот.
- Злоупотребата на легитимна привилегија може да се запре со обезбедување на добра ревизорска трага.

4.2. „SQL“ Вбризгување (SQL Injections)

Системите на бази со податоци се користат за функционалноста на позадинскиот дел (backend). За да добие податоци корисникот како влез често користи динамички напишани скрипти, коишто влијаат директно на базите на податоци. Внесувањето инјекција е напад кој има за цел да ја наруши оригиналната намера на апликацијата со поднесување напаѓач - доставени “sql“ скрипти директно во базата на податоци.[9]

Постојат два вида на “SQL” вбризгување:

1. „SQL“ вбризгување – SQL Injection
2. “NoSQL“ вбризгување – NoSQL Injection

SQL Injection: Целта на овој тип на напад е стандардниот систем на базата со податоци. Нападите обично вклучуваат инјектирање неовластени делови од скрипти во влезните полиња на апликациите.

NoSQL Injection: Целта на овој тип на напад се платформи со големи податоци. Овој тип на напад вклучува вметнување злонамерни скрипти во компонентите за големи податоци, како што се: „Hive“, „MapReduce“. „SQL“ и „NoSQL“ успешен напад со

[8] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[9] Jiping Xiong, Lifeng Xuan, Jian Zhao and Tao Huang, Web and Database Security, Zhejiang Normal University.

вбризгување може да му даде неограничен пристап на напаѓачот до целата база со податоци.

Контрамерки на напад со вбризгување:

- Користење на "store procedure" процедури наместо да се имплементираат директни пребарувања.
- Имплементирање на "MVC" архитектура.

4.3. Малициозен софтвер

Сајбер-криминалците, државно-спонзорираните хакери и шпионите користат напредни напади коишто вклучуваат повеќе тактики. Такви тактики се електронски фишинг пораки и малициозен софтвер. Со тоа се обидуваат да навлезат во организациите и да украдат чувствителни податоци. Не знаејќи дека малициозниот софтвер го заразил нивниот уред, легитимните корисници стануваат канал за овие групи да пристапат внатре во мрежите и чувствителните податоци.[10]

Контрамерки на малициозен софтвер:

- Да се направи заштита со заштитен ѕид (firewall) и да се инсталира антивирус.

4.4. Слаба ревизорска трага

Слабата ревизорска политика и технологија претставуваат ризици во однос на усогласеност, спречување, откривање, форензика и обновување. Автоматското снимање на трансакции во бази со чувствителни податоци треба да биде дел од кој било сегмент на базата на податоци. Неможноста да се соберат детални ревизорски записи за активности во базата на податоци претставува сериозен организациски ризик на повеќе нивоа. Компаниите со слаби механизми за ревизорска трага на базата со податоци сè повеќе ќе откриваат дека се во спротивност со индустријата и регулаторните барања на државата. Повеќето механизми за ревизија не знаат за тоа кој е крајниот корисник затоа што целата активност е поврзана со корисничкото име од апликацијата. Известувањето, видливоста и форензичката анализа се попречени затоа што нема врска до одговорниот корисник. [11]

[10] Debasish Das, Utpal Sharma & D.K. Bhattacharyya, An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications, Volume 1, 2010.

[11] D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: Sigurnost računarskih sistema i mreža, Beograd, 2007.

Конечно, корисниците со администраторски пристап до базата со податоци, легитимно или злонамерно, можат да ја исклучат ревизорската трага на базата со податоци за да се скрие измамничка активност. Ревизорските капацитети и одговорности идеално би требало да бидат одделени и од администраторите на базата со податоци и од платформата на серверите на базата на податоци за да се обезбеди силна политика на поделба на должности.

Контрамерки на слабата ревизорска трага:

- Ревизорски траги кои се засновани на ниво на мрежа се добро решение. Таквите решенија не треба да имаат влијание на перформансите на базата со податоци, да работат независно од сите корисници и да дадат грануларно собирање на податоци.

4.5. Изложеност на резервна копија

Медиумите за складирање на резервните копии честопати се целосно незаштитени од напади. Како резултат на тоа, се случуваат бројни прекршувања на безбедноста, вклучувајки кражби на резервни копии од бази со податоци. Токму поради тоа, неможноста да се изврши ревизорска трага и неможноста да се следат активностите на администраторите кои имаат ниско ниво на пристап до чувствителни информации, може да ги изложи на ризик базите со податоци. Преземањето на соодветни мерки за заштита на резервните копии на чувствителни податоци и мониторирањето на корисниците со највисоко ниво на привилегии не е само најдобра сигурносна практика за безбедност, туку е исто така е регулирано со многу прописи.[12]

Контрамерки на изложеност на резервните копии:

- Шифрирање на базите со податоци: Да се зачувуваат податоците во криптирана форма доколку тоа овозможува да се обезбеди продукцијата и резервните копии од базите со податоци. Потоа, да се направи ревизија на активностите и контрола на пристапот до чувствителни податоци од корисници кои пристапуваат до базите со податоци на оперативниот систем и нивоата за складирање. Со криптирање на податоците во базата со податоци и ревизорска трага заедно со криптирање,

[12] William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice Hall, 2006.

компаниите можат да ги мониторираат и да ги контролираат корисниците и внатре и надвор од базата на податоци.

4.6. Слаба автентификација

Слабите шеми за автентификација им овозможуваат на напаѓачите да го преземат идентитетот на легитимните корисници на базата со податоци. Специфични стратегии за напади вклучуваат напади со брутална сила (brute force attacks), социјален инженеринг итн. Имплементација на лозинки или автентификација со два фактори е задолжителна. За приспособливост и полесна употреба, механизмите за автентификација треба да бидат интегрирани во стратегиите на заштита на компанијата (корисник - менаџмент инфраструктурата).

Контрамерки на слаба автентификација:

- Користење на политика за комплексни лозинки

4.7. Ранливост на ДБ и погрешна конфигурација

Многу често може да се најдат ранливи и незаштитени бази со податоци или да се откријат бази на податоци кои сè уште имаат стандардни кориснички имиња и конфигурациски параметри. Напаѓачите знаат како да ги искористат овие ранливости за да започнат напади против компанијата, т.е. базата со податоци. Стандардните начини на напади во себе вклучуваат високи оптоварувања и закачуваат позадински логови за администраторите кои се поврзани со базите со податоци, комплексни барања коишто одземаат многу време за тестирање. Крајниот резултат е дека на организациите обично им требаат денови, па дури и месеци да ги оспособат базите со податоци, а за тоа време тие остануваат ранливи.[13]

Контрамерки на погрешно конфигурирани бази на податоци:

- Не треба да постојат стандардни кориснички имиња. Корисничките имиња мора да бидат креирани со користење на ново корисничко име и лозинка.

[13] Deepika, Nitasha Soni, Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

4.8. Неменаџирани чувствителни податоци

Многу компании се борат да одржат точен попис на нивните бази на податоци и критичните податочни објекти содржани во нив. Заборавените бази со податоци може да содржат чувствителни информации, а може да се појават и нови бази со податоци - на пример, во средини за тестирање апликации, без видливост на тимот за безбедност. Чувствителните податоци во овие бази на податоци ќе бидат изложени на закани доколку задолжителните контроли и привилегии за пристап не се имплементирани.

Контрамерки на менаџирани чувствителни податоци:

- Да се криптираат чувствителните податоци во базата со податоци.
- Да се имплементираат задолжителните контроли и привилегии на базата со податоци.

4.9. Одбивање на услугата

Одбивањето на услугата е општа категорија на напади во која пристапот до мрежните апликации или податоци е забранет за легалните корисници.

4.10. Ограничена безбедносна експертиза и едукација

Нетехничката безбедност исто така игра многу важна улога. Внатрешните безбедносни контроли не се во чекор со растот на податоците и многу компании се недоволно опремени за справување со нарушувањето на безбедноста. Честопати ова се должи на недостаток на експертиза потребна за спроведување на безбедносни контроли, спроведување на политики за безбедност или спроведување на процеси на одговор на инциденти.

Контрамерки на ограничена безбедност и едукација:

- Едукација и свесност за корисниците
- Негување на искуството за безбедност професионално.

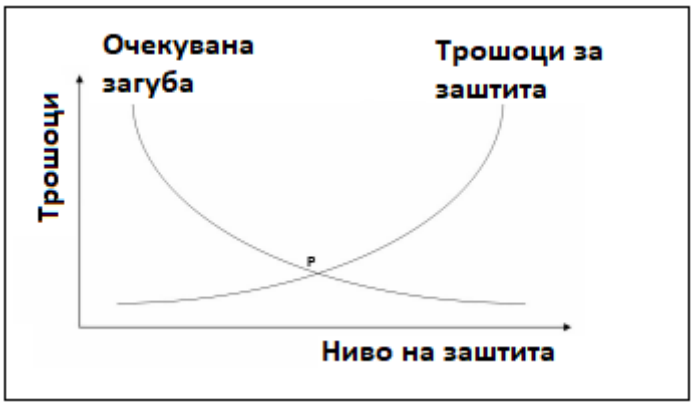
5. Стратегии за заштита на информациските системи

На компаниите им се достапни следните стратегии за заштита на информациските системи:

- *Избегнување ризик*: Привремено откажување на одредени функции и / или компоненти на системот кои се најзагрозени и без кои може да работи остатокот од системот (свесна и привремена деградација на системот);

- *Прифаќање на ризици*: Непреземање на какви било мерки за заштита во врска со идентификуваните закани, (штетата предизвикана од овие закани е помала од трошоците за преземање мерки);
- *Трансфер на ризик*: Пренесување на последиците од штетен настан на некој друг (гарантен рок, договор за одржување, полиси за осигурување);
- *Контролирање (ограничување) на ризик*: Преземање на соодветни мерки за заштита во врска со идентификуваните закани со цел да се елиминира или намали ризикот на прифатливо ниво, како и да се намали веројатноста за нивно појавување. Оваа стратегија има најголема тежина.

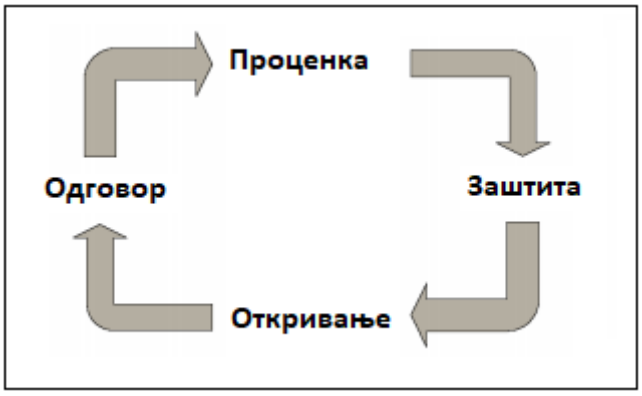
Безбедноста е процес на одржување на прифатливо ниво на ризик и бара време и ресурси за да се исполнат тие барања и одговорности. Постигнувањето безбедност значи одржување на системот во состојба на прифатлив ризик, т.е. компромис помеѓу неопходните инвестиции и намалувањето на можноста за штета предизвикана од таа инвестиција. Поголемите инвестиции во безбедноста ја намалуваат изложеноста на систем или компјутерска мрежа на ризик. Од друга страна, го изложува сопственикот на повисоки трошоци и ја намалува профитабилноста и удобноста при работа. Затоа е многу важно да се одреди точката во која се постигнува рамнотежа помеѓу безбедносните инвестиции и постигнатите ефекти (Слика 8). Пресекот на кривините (точка P) покажува оптимално ниво на заштита.



Слика 8. Сооднос на потенцијалната загуба и трошоците за заштита

Безбедноста како процес (слика 9) се заснова на четири основни чекори: проценка (планирање), заштита (превенција), откривање и одговор.

- *Проценката* е поврзана со правила, процедури, законски и други прописи, буџетирање, а исто така е поврзана и со техничка проценка на безбедносната состојба. Грешка во проценката може да им наштети на сите операции што следат.
- *Заштита*, т.е. превенцијата вклучува примена на контрамерки за намалување на можноста за компромитирање на системот. Ако заштитата не успее, се применува следниот чекор - откривање.
- *Откривање* или детекција е процес на идентификација на упад, т.е. прекршувања на безбедносните правила на незаконски, неовластени или неприфатливи дејствија преземени над компјутерски систем или преку мрежа.
- *Одговорот* е процес на опоравување, т.е. третмани поради напад. Активностите за реакција вклучуваат процедури „крпење и продолжување“ или „бркање и судење“. Претходно, првиот приоритет беше враќање на функционалноста на оштетените ресурси, како на пример, користење резервни податоци за враќање на системот во состојба пред нападот. Во последно време, сè повеќе се користат правни лекови (судски постапки против оние кои ја загрозуваат безбедноста), вклучително и претходно собирање докази со дигитални форензички методи користени за да се поткрепи судска постапка.



Слика 9. Сооднос на големината на ризикот и остварено ниво на заштита

При спроведувањето на системот за заштита, треба да се стремиме да се воспостави рамнотежа помеѓу големината на ризикот и постигнатото ниво на заштита, кое може да биде на стандардно, средно, повисоко и највисоко ниво, земајќи ги предвид трошоците (слика 10).

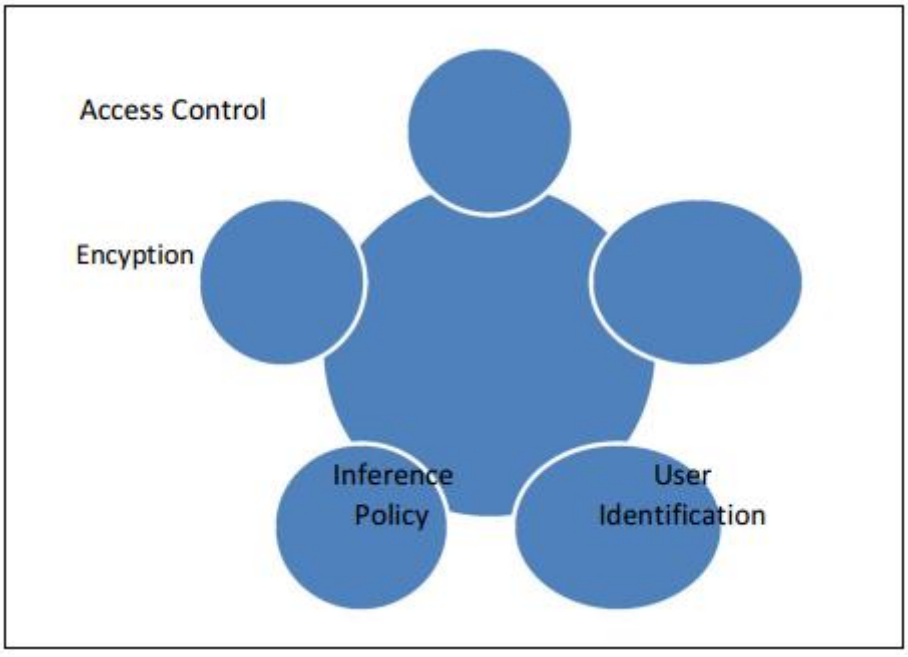


Слика 10. Сооднос на големината на ризикот и остварeното ниво на заштита

6. Методи за контрола на закани кон бази со податоци

За да се отстранат безбедносните закани, секоја организација мора да има безбедносна политика којашто треба да биде имплементирана за сигурност. Во безбедносната политика, автентификацијата игра важна улога, бидејќи ако автентификацијата е соодветна, тогаш шансите за закани се многу помали. Различни корисници имаат различни привилегии за пристап на различни објекти во базите со податоци. Механизмот за контрола на пристап управува со привилегиите за пристап.[14]

Тоа е основна техника за заштита на објектите во базите со податоци и е поддржана од повеќето од ДБМС. Слика 11 дава преглед на контролните методи што се користат за безбедноста на базата со податоци.



Слика 11. Контролни методи

[14] S. R.Petrović: Kompjuterski kriminal, II Izdanje, Beograd, 2001.

6.1. Контрола на пристап

Контролата на пристап е една од основните услуги што треба да ги обезбеди кој било систем за управување со податоци. Ги заштитува податоците од неовластени операции на читање и пишување. Контролата на пристап овозможува сигурност дека целата комуникација со базата на податоци и другите објекти од системот ги следат строгите безбедносни политики. Грешките можат да бидат толку големи, така што можат да создадат проблеми во работењето на компанијата. Преку контролирањето на привилегиите на пристап исто така може да се намалат ризиците што можат прецизно да влијаат на безбедноста на базата со податоци на главните сервери. На пример, ако некоја табела се избрише или пристапот се модифицира случајно, податоците можат да бидат повратени од бекап, но преку примена на контрола на пристапот, бришењето може да се ограничи.

Системите за контрола на пристап вклучуваат:

1. Привилегии за датотеки - креирање, читање, уредување или бришење на датотеки на сервер.
2. Привилегии за апликации - право за извршување на апликација на апликацискиот сервер.
3. Привилегии за податоци - право на добивање или ажурирање на информации во базата со податоци.

6.2. Полиси за заклучување

Многу е важно да се заштитат податоците на специфични нивоа. Може да се примени кога анализата на одредени податоците во форма на факти се неопходни за превенција на одредено повисоко безбедносно ниво. Тоа помага да се одреди како да се заштитат информациите од објавување. Целта на контролата на заклучување е да се избегне индиректно откривање на информации. Општо постојат три начини на неовластено откривање на податоци:

1. Поврзани податоци - типичен канал кога видливите податоци X се семантички поврзани со невидливи податоци Y;
2. Исчезнати податоци - резултатот од барањето содржи NULL вредности кои маскираат чувствителни податоци. Постоење на такви податоци можат на тој начин да се детектираат;

3. Статистички заклучок - типичен за базите со податоци кои обезбедуваат статистички информации за ентитетите;

6.3. Идентификација / автентификација на корисник

Основно безбедносно барање е секогаш да мора да се знаат кои се корисниците. Корисниците мора да се идентификуваат пред да им се одредат нивните привилегии и права за пристап и со тоа може да се прави ревизија на нивните постапки со податоците. Корисникот може да биде автентифициран на многу начини пред да му биде дозволено да се креира база со податоци. Автентификацијата на базата со податоци вклучува и идентификација и автентификација на корисниците. Надворешна автентификација може да се изврши од оперативниот систем или мрежните сервиси. Исто така, автентификацијата на корисникот може да биде дефинирана со слој на безбеден приклучок (Secure Socket Layer - SSL), преку привилегии за пристап, преку сервер за средно ниво на автентификација позната и како прокси-автентификација. Ова е основното барање за да се осигура безбедност бидејќи процесот на идентификација дефинира група на луѓе на кои им е дозволен пристап до податоците. За да се осигура безбедноста идентитетот се проверува и тој ги зачувува чувствителните податоци безбедни од промени од неовластени корисници. Напаѓачите може да преземат најразлични пристапи, како бајпас автентификација, стандардна лозинка, ескалација на привилегија, погодување на лозинка со напад на брутална сила или напад на виножито кога ќе се обидат да ја компромитираат корисничката идентификација и автентификација.

6.4. Отчетност и ревизија

Ревизијата е следење и снимање на конфигурираните активности на базата со податоци, и за корисниците на базите со податоци и за оние што не се корисници на базите со податоци. Собирањето е процес на одржување на ревизорска трага за дејствијата на корисниците во системот. Потребни се проверки на одговорноста и ревизија за да се обезбеди физички интегритет на податоците за коишто е потребно да се дефинира пристап до базите со податоци, а тоа се прави преку ревизија и чување на евиденцијата. Ако корисникот успеал успешно да се автентифицира и се обиде да пристапи до ресурс, двата и успешниот и неуспешниот обид треба да се следат од

системот, а обидите за пристап и нивните статуси треба да се појават во датотеките за ревизорска трага.[15]

6.5. Шифрирање (Енкрипција)

Шифрирањето е процес на претворање на информациите во шифри или кодови за да не можат да биде читливи за сите останати луѓе, освен за оние кои имаат клуч за шифрираниот текст. Шифрираниот текст или кодираниот текст се нарекува криптиран податок. Постојат две места каде што податоците од базата со податоци треба да се заштитат. Податоците може да бидат или во состојба на мирување - зачувани во база со податоци или во бекап или при пренос. Има различни решенија за криптирање на податоците кои патуваат низ мрежата. Шифрирањето на податоците може да реши некои од прашањата поврзани со податоците во состојба на мирување. За податоци при транзит потребни се покомплексни решенија како што се SSL / TLS.

При спроведувањето на стратегијата на заштита со шифрирање внатре во базата со податоци или надвор од неа, важно е да не се занемарат и следните принципи:

- шифрираните податоци треба да се чуваат одвоено од криптографските клучеви;
- неопходна е квалитетна автентификација којашто ќе биде користена за идентификација на корсниците пред дешифрирање на важните податоци;
- пристапот до клучевите треба да биде строго надгледуван, а исто така и лог фајловите;
- важните податоци мора да бидат шифрирани и кога се наоѓаат во комуникациските канали помеѓу базата со податоци и апликацијата;[16]

6.6. Правила за Лозинки

Лозинки користат и треба да користат сите корисници на информациските системи. Користењето на лозинката започнува со креирање на силна лозинка. Таа треба да задоволува критериуми за сигурност и не треба да биде можно лесно да се погоди. Многу корисници ги запишуваат лозинките на видливи места, а со тоа го загрозуваат самиот информационен систем и податоците. Лозинката треба да биде доволно силна, за да не

[15] M. Milosavljević, G. Grubor, Osnovi bezbednosti i zaštite informacionih sistema, Univerzitet Singidunum, Beograd, 2006

[16] Mark Stamp, „Information security principles and practice “, San Jose State University, 2006

може да се открие со која било програмска алатка во определен период. Исто така, лозинката треба да биде лесна за помнење и тајна. Карактеристики на силна лозинка се:

- Минимална должина од 8 карактери;
- Да содржи во себе комбинација од мали и големи букви;
- Да содржи во себе комбинација од бројки и букви;
- Да содржи во себе минимум еден специјален знак;
- Да содржи во себе некој интерпункциски знак;
- Да не се повторуваат знаците во лозинката;
- Да се менува лозинката на определен временски период;
- Да биде различна од претходната лозинка;

6.7. Автентификациски протоколи

Автентификација претставува процес со кој се потврдува дека корисникот, т.е. компјутерскиот систем со кој се комуницира, е оној којшто се претставува. После автентификацијата, може да се направи авторизација, т.е. да се направи комуникација во која ќе се користи енкрипција. Енкрипцијата често се користи за автентификација, а со тоа се воспоставуваат сесиски клучеви. Случајно генерираните сесиски клучеви се користат за намалување на податоците кои се испраќаат, користејќи приватен и јавен клуч. Штетата што може да настане доколку се пробие серискиот клуч е значително помала, затоа што сесиските клучеви се користат само за поединечни сесии. Истите може да се менуваат периодично за времетраење на сесиите.[17]

7. Напади и Ризици

7.1. Надворешни и Внатрешни напади

Надворешните напади на базите со податоци ги извршуваат напаѓачи кои доаѓаат од надворешните мрежи. Тие дејствуваат на таканаречениот “firewall”, со цел да поминат низ него и да дојдат до важни податоци или да ја нарушат оперативноста на системот. Со развојот на е-комерц апликациите, акцент се става на заштита внатре во деловното опкружување заради корисниците кои имаат пристап на мрежните ресурси одвнатре. Во вакви окружувања заканите и опасностите не доагаат само однадвор, туку и од внатре од страна на вработените коишто имаат пристап до важни податоци, при што многу

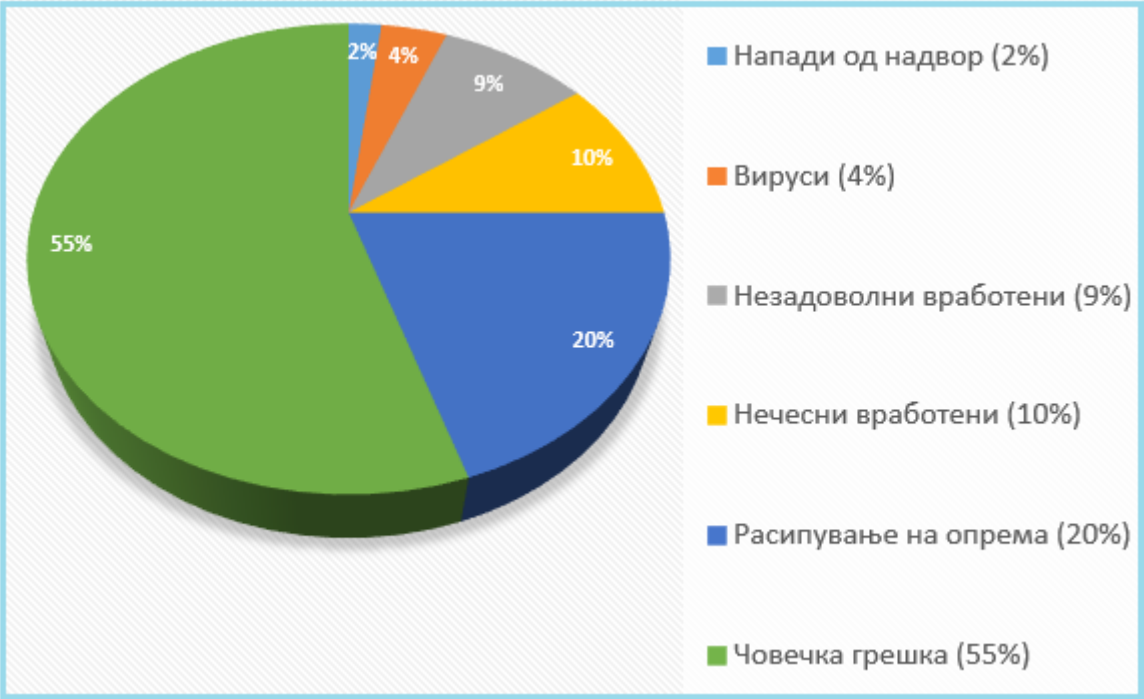
[17] Shivnandan Singh, Rakesh Kumar Rai, A Review Report on Security Threats on Database, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014.

често е тешко да се воспостави и дефинира превентивно поле на заштита. Кај овој тип на напади-одвнатре, “firewall”-от не ни е од корист. За заштита од внатре од најголемо значење е контролата на пристапот. Мора да се знае кој може да пристапи на одреден дел од базата со податоци. Покрај контролата на пристапот, треба да се контролираат и местата за чување на клучевите, како и пишување на сигурносни правила кои вклучуваат ревизија и мониторинг. Со оглед на тоа дека мрежните бази со податоци денес претставуваат платформа на секоја деловна апликација, опасностите од напади значително пораснаа. Без правовремено преземање на заштита на податоците во базите, приватноста на организацијата е изложена на ризик.

Заканите за сигурноста на информациониот систем може да биде поделена на:

- Луѓе – намерни закани;
- Луѓе – ненамерни закани;
- Опрема;
- Природни непогоди;

Иако многумина сметаат дека заканите најчесто доаѓаат однадвор (напади на хакери), истражувањата покажуваат дека не е така. Според истражувањето коешто е објавено во книгата на “D. Seger, K., VonStroch, W. «Computer Crime A Crimefighter's Handbook», O'Reilly & Associates”, е прикажано сосема спротивното. Статистичките податоци прикажуваат дека најголем процент од проблемите со сигурноста го предизвикуваат човечките грешки. Тие најчесто се случуваат поради недоволна претпазливост и едуцираност на вработените. Втора најголема причина за загрозување на сигурноста е расипување на опремата, а потоа следуваат вработените коишто својата позиција ја користат за сопствена корист и вработените коишто на ваков начин го изразуваат своето незадоволство спрема компанијата или надредените претпоставени (слика 12).



Слика 12. Проблеми со сигурноста во големи компании

7.2. Ризици од губење на податоци

Во деловниот свет, упадот во дигиталните системи и одземањето на податоците од страна на напаѓачите е убедливо најголем проблем. Според извештајот на компанијата "Cisco" од 2019 година, дури 31% од компаниите и организациите се соочиле со сајбер-напади. Секој успешен сајбер-напад води до губење на податоци, а тоа повлекува со себе губење на рејтингот, губење на купувачи, зголемување на трошоците.

Имајќи ги предвид наведените опасности, компаниите прават сè за да се намали ризикот од нивно појавување во најмала можна мера. Но, сепак многу ризици остануваат. Тука накратко ќе се фокусираме на три кои се меѓусебе поврзани:

- Ризик на рејтинг;
- Ризик на спроводливост;
- Ризик од судски спор;

7.3. Ризик на рејтинг

Многу добро е познато дека значењето на рејтингот во деловните кругови е многу големо, т.е. немерливо. Рејтингот има далекусежни последици. Добар рејтинг значи поголема доверба на постоечките потрошувачи и придобивање на нови, подобар квалитет на услугите во однос на конкуренцијата, поголем профит и можност за брз

напредок и раст на компанијата. Меѓутоа, губење на рејтингот значи и губење на сите погоре набројани работи.

Затоа ударот врз рејтингот се манифестира главно на три начини:

- Се намалува довербата на потрошувачите кон компанијата или потполно се губи;
- Се поднесуваат тужби за надомест на штета како резултат на неможноста компанијата да ги зачува податоците за потрошувачите;
- Паѓаат вредностите на акциите на компанијата;

Имајќи го предвид последно наведеното, според последните извештаи, многу компании ги осетиле последиците од падот на цената на акциите како последица на сајбер-напади, до минимум една година после објавување на податоците од сајбер-нападот. Кога се во прашање финансиски институции, со ризикот на рејтингот е поврзан и оперативен ризик, вклучувајќи и правен ризик, како и ризик за неодговорно управување со информациите и други технологии значајни за работењето на компанијата.

Секако, кога се во прашање таканаречените "Outsourcing" услуги, податоците се убедливо најголемото богатство на финансиската компанија, така што прашањата за ракувањето со податоците треба да се третира со најголема грижа и внимание.

7.4. Ризик на спроводливост

Сите компании, особено на оние кои се присутни глобално, мораат да ги почитуваат законите на матичната држава во која работат. Непочитување на истите може да ги доведе до сериозни казни од страна на државните власти. На пример, Велика Британија, во согласност со уредбите за заштита на податоци на ЕУ (GDPR – General Data Protection Regulation), во 2018 година го подигнала износот на максималната парична казна од 500 000 фунти на дури 17 милиони фунти или 4% од годишниот глобален приход (во зависност што е поголемо).

Според тие регулативи, управата за финансиско однесување на Велика Британија ја казнила компанијата "Tesco bank case" со казна од дури 16,4 милиони фунти по напад од сајбер-криминалци, поради нарушување на безбедноста и протекување на информации. Кога ќе се согледа овој ризик, се забележува дека се појавува посебна тешкотија за мултинационалните компании кои работат на глобално ниво, бидејќи националните права имаат различни дефиниции за ризик за казнување, што може да доведе до изрекување на казни во повеќе држави.

7.5. Ризик од судски спор

Кога го спомнавме ризикот на рејтингот, видовме дека со губењето на рејтингот, покрај губењето на довербата, паѓа и вредноста на акциите, а тоа повлекува со себе и тужби од оштетените лица.

Конкретно, законите за заштита на податоци пропишуваат дека може да се креира тело за заштита на потрошувачите и тоа тело да поднесува тужби во нивно име. Сепак, во многу од развиените држави такви тела веќе постојат или на веќе постоечки здруженија (на пример, Здружение за заштита на потрошувачите) им се даваат такви овластувања. Се креираат тужби за надокнада на штета за душевна болка и финансиски загуби предизвикани од сајбер нападите. Тие надокнади може да бидат и многу ниски, но сепак да предизвикаат сериозен удар врз компанијата и нејзиниот буџет, доколку таа работи со илјадници, а некогаш и со десетици илјади и милиони потрошувачи.[18]

8. Заштита на податоците со шифрирање

Цел на секое деловно опкружување е да ги заштити податоците за своите клиенти. Поради големиот број на места каде што се наоѓаат осетливите податоци внатре во едно деловно опкружување, неопходно е да се штитат архивираните податоци, кои се наоѓаат во компјутерите на вработените или на некои други медиуми. При развојот на стратегијата, за да бидеме сигурни дека податоците ќе бидат заштитени, мора да се исполнат два основни услови. Првиот услов е употребата на доверлив криптографски механизам, а вториот услов е стриктно дефинирано менаџирање на пристапот на криптографските клучеви. Само со исполнување на овие два услова, заштитата на доверливите податоци може да биде сигурна. Следен чекор е изработката на стратегија за процесот на шифрирање, а за нејзина реализација важно е да се направи следното:

- Да се одлучи каде ќе се прави процесот на шифрирање, внатре или надвор од базата со податоци;
- Прецизно да се оптимизира системот, сè со цел да се намали бројот на корисници коишто имаат пристап до криптографските клучеви;
- Да се определи сигурно место за складирање на криптографските клучеви;
- Да се раздвојат шифрираните податоци од клучевите (во овој случај шифрираните податоци се потполно бескорисни во рацете на напаѓачите)
- Да се направи баланс помеѓу перформансите и апликациите;

18 http://www.naumovic-partners.com/3-najveca-rizika-po-sajber-bezbednost-za-kompanije/

Со прецизна политика на контрола на пристапот и управувањето со криптографските клучеви, се постигнува високо ниво на доверба и контрола над информацискатa инфраструктура. Пристапот на дешифрираните податоци треба да биде стриктно ограничен со контрола на пристап, а корисниците коишто имаат пристап до овие податоци мора да бидат надгледувани со системи за мониторинг и анализа на лог фајлови.[19]

8.1. Социјален инженеринг како битен фактор при развој на стратегија

Шифрирањето на важни податоци е само првиот чекор при креирање на стратегија за заштита на базите со податоци. Без цврста проверка на идентитетот, од страна на технологијата, применета на страна на апликацијата, се отвора пат за пристап до механизмот за дешифрирање на податоците. Голем проблем претставуваат администраторите на базите со податоци и програмерите на деловните апликации кои знаат како може да се пристапи до тие информации, како и незадоволните вработени кои пронаоѓаат начини преку социјален инженеринг да дојдат до лозинките. Многу вработени ги компромитирале своите компании откривајќи податоци за месечните заработки, броеви од социјално осигурување, броеви од мобилни телефони, информации од надворешни соработници и др. Заштитата на базата со податоци не е само заштита на важните податоци, туку и заштита од вработените од ваков тип на експлоатација. Треба навреме да се размислува за развивање на безбедносна стратегија, првенствено на заштита на важните податоци, како што се: шифрирање, контрола на пристап, надгледување на настани и следење на логови.

8.2. Планирање на стратегија на шифрирање во база со податоци

Пред да се започне со дизајнирање на стратегија на шифрирање во базата со податоци, треба да се знае:

- како работат криптографските механизми;
- како изгледа текот на податоци во апликациите;
- како се вклопува заштитата на базата со податоци во безбедносната политика на организацијата;

Затоа постојат две стратегии:

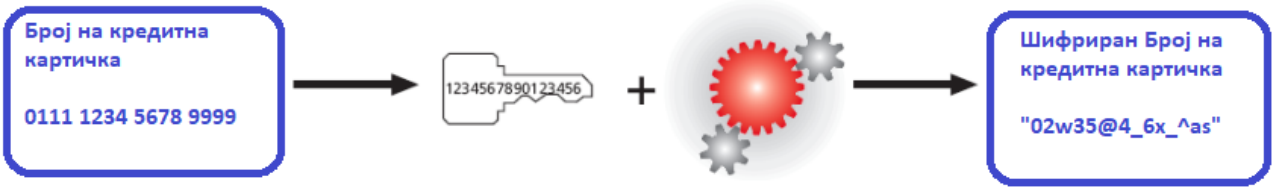
[19] D. Bulatović, B. Trifunović: Šifrovanje i zaštita podataka u elektronskom prenosu novca, Zbornik radova

- употреба на функциски механизми за шифрирање внатре во базата со податоци (DBMS);
- употреба на функциски механизми за шифрирање на страна на апликациите;

Секој од овие пристапи има свои предности и недостатоци. Важно е да се направи добар преглед и на едната и на другата стратегија, а во зависност од организациската инфраструктура, да се избере онаа којашто најдобро ќе се вклопи во функционирањето на организацијата.[20]

8.3. Криптографија и криптографски алгоритми

За да се достигне највисоко ниво на безбедност, податоците мора да се чуваат во шифрирана форма. Цел на шифрирањето е да ги направи информациите нечитливи за неовластените читатели и да ги заштити од дешифрирање во случај на напад. Операцијата на шифрирање се изведува со случајно генерирани криптографски клучеви. Со тоа шифрираните податоци се осигурени и отежнуваат напад или дешифрирање. Клучевите најчесто се чуваат во шифрирана форма (слика 13).



Слика 13. Процес на шифрирање на број на кредитна картичка

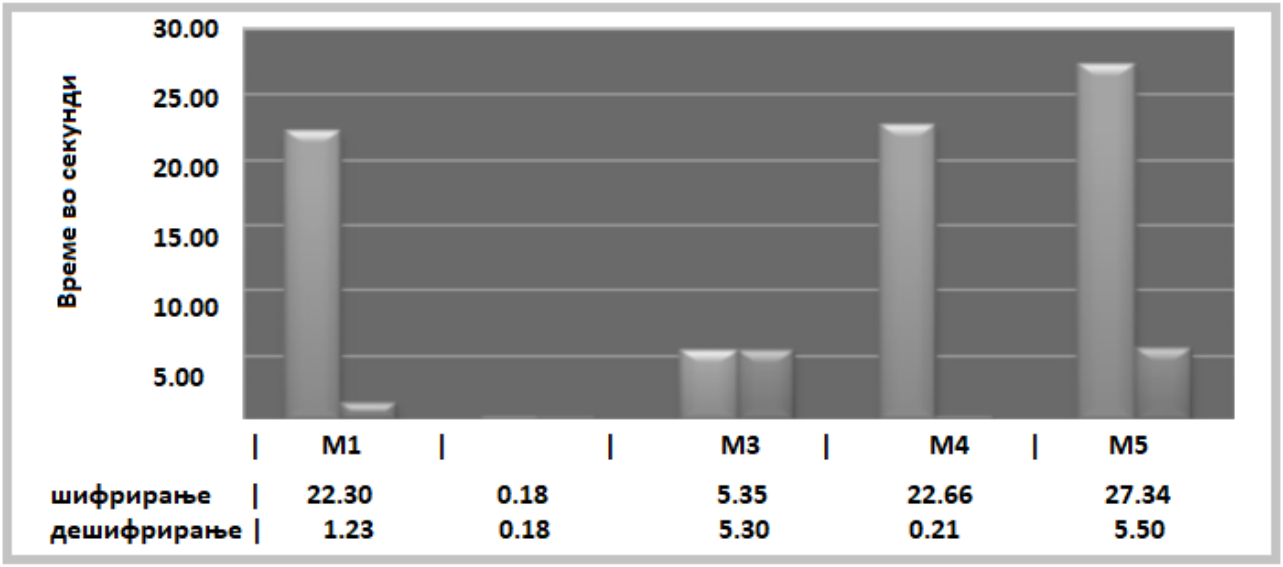
Не се исти сите процеси на шифрирање. Безбедноста на шифрираните податоци зависи од разни фактори, како што е должината на криптографскиот клуч, т.е алгоритмот и начинот на неговата имплементација во системот во којшто се користи. Многу бази со податоци користат “AES” и “DES” алгоритам за заштита на полињата со важни податоци. Но, “DES” веќе одамна се смета како несигурен за заштита. При одбирање на криптографски алгоритам, важно е да се пронајде доверлив добавувач на комерцијални алгоритми или да се оди со варијанта на сопствено решение. Освен квалитетот на криптографскиот алгоритам, многу е важно да се има и квалитетна стратегија за управување со криптографските клучеви. Во ваквите системи постои постојана

[20] Debasish Das, Utpal Sharma, D.K. Bhattacharyya, An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications, Volume No.1–25,2010.

напнатост во сферата на заштитата помеѓу контролите и пристапот. Во секој случај, системот мора да има пристап до клучевите за да може да дешифрира, а нивната дистрибуција е комплицирана и доведува до намалување на перформансите, а понекогаш и безбедноста. Администраторите и програмерите многу често се во недоумица околу примената на овие безбедносни мерки.

8.4. Влијание на шифрираните податоци на базата со податоци

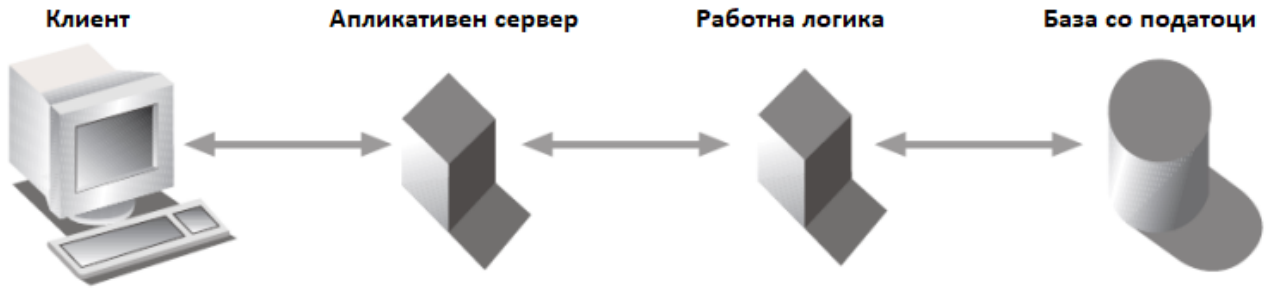
Шифрирањето обезбедува високо ниво на заштита и е прифатено како најдобра алатка во праксата во организациите за заштита на важни информации, но има влијание на податоците и на базите со податоци. Шифрирањето ја зголемува количината на податоците и ги намалува перформансите. Важно е при планирањето и развојот на апликациите да се предвидат можните влијанија предизвикани од примената на шифрираните системи. Знаејќи кои податоци треба да бидат заштитени, добиваме повеќе флексибилност, а и подобри перформанси. При обработка на кредитни картички, може да се шифрира комплетниот број или само поединечни цифри. Врз основа на познавањето на количината на податоците коишто треба да се заштитат, се врши проектирање на апликациите. Шифрирањето влијае на количината на податоците. Алгоритмите често може да ја променат големината на фиксниот податок од базата со податоци, така што податокот нема да биде сочуван. Особено шифрирањето на некој мал податок може многу да ја зголеми неговата големина, а тоа доведува до зголемување на големината на колоната во релационата база со податоци. Шифрирањето е процес во кој ги трансформираме карактерите во бинарни бесмислени низи коишто можат да влијаат на големината доколку шифрираните податоци ги трансформираме во карактери. Со употреба на алгоритмот BASE64, може шифрираните податоци да се конвертираат во низа од карактери, но со тоа би се зголемила големината на податоците за една третина. При одбирање на полиња во табелите од базите со податоци, коишто ќе бидат шифрирани, важно е да се води сметка за процесот на пребарување. Доколку при секое пребарување, во големи бази со податоци, следи процес на шифрирање и дешифрирање, тоа може да ги деградира перформансите на апликациите, како и нивното функционирање. Шифрирањето може да започне процес и да предизвика фрустрации кај корисниците на почетокот, а тоа наметнува нови размислувања и планирања околу избор на полиња за шифрирање (слика 14).



Слика 14. Влијание на шифрирањето врз перформансите

8.5. Текови на податоците на апликативно ниво

Добра стартна основа при развој на стратегија за заштита на податоци е потполно добро следење на тековите на податоците на апликативно ниво и разбирање на системските компоненти коишто ги обработуваат податоците. Дури после тоа може да се определат местата на коишто податоците може да бидат изложени на ризик.



Слика 15. Стандардна апликативна структура

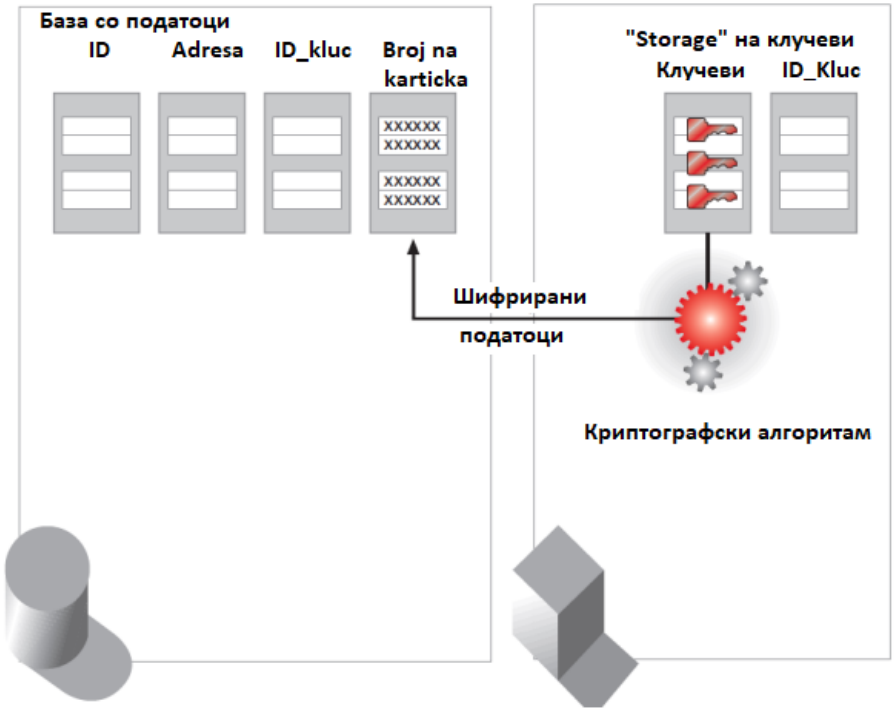
На слика 15 е претставена стандардна апликативна структура. Податоците може да бидат изложени на ризик на која било од наведените компоненти или во моментите на нивната меѓусебна размена на податоци. Шифрирањето на страна на базата со податоци, може да ги заштити податоците кои се наогаат во базата, но потребна е заштита и на податоците кои се наоѓаат во комуникациските канали помеѓу податоците и апликативниот сервер, како и податоците во апликациите. Во текот на обработката,

податоците во апликацијата може да бидат кеширани одреден период. Шифрирањето на податоците во базата со податоци обезбедува приватност, но податоците кои се разменети преку интернет или оние кои се во рамките на корпоративната мрежа се незаштитени (отворен текст). Добрата безбедносна пракса покажува дека податоците треба да се заштитат во сите случаи.

8.6. Стратегија за управување со криптографските клучеви

Криптографијата се заснова на криптографски клучеви од кои зависи чувањето на шифрираните податоци во базата со податоци. Тие имаат тајни места каде што се архивирани и тоа кој може да им пристапи. Контролата со управувањето со криптографските клучеви главно се предвидува при развојот на стратегиите за заштита на базата со податоци. Важна улога во планирањето на стратегија за контрола на клучеви (слика 16) :

- број на клучеви потребен за шифрирање;
- начин на којшто се користат;
- место на коешто се чуваат;
- заштитен и ограничен пристап;
- промена на клучевите;



Слика 16. Стратегија на безбедно сценарио при шифрирање

8.7. Потребен број на клучеви и начин на управување

Проблемот со управувањето со криптографските клучеви тешко се решава. Употребата на ист клуч во апликациите е едноставно за имплементација и одржување, но ако тој клуч се компромитира, податоците ќе станат ранливи. Доколку постои поголем број на корисници коишто побаруваат да пристапат со различни апликации, сценариото станува посложено. Тоа е така затоа што шифрираните податоци можат да бидат дешифрирани само со клуч којшто одговара. Исто така, секој систем или апликација мора да има пристап до клучот којшто одговара. Што повеке апликации имаат пристап до клучевите, толку е поголем ризикот од напади. Затоа треба клучевите да се држат во сигурен систем за управување. Добра пракса е да се користи помал број на клучеви за шифрирање, поедноставно е решението за управување со клучевите, но затоа критична точка е клучот.[21]

8.8. Сигурно место за чување на клучеви

При изработка на стратегија за контрола на клучеви, многу се внимава да се креира сигурно место за чување на клучевите. Едно од решенијата за чување на клучевите е во посебна база со податоци или во фајл со строго ограничен и контролиран пристап. Кај овие решенија проблем претставуваат администраторите коишто имаат овластен пристап до клучевите и можат да ги дешифрираат податоците, а после тоа да ги прикријат трагите. Во овој случај безбедноста на базата со податоци не зависи од најдобрите практики, туку од чесноста и доверливоста на вработените. За да се намали ризикот и да се има подобра контрола, најдобро е само едно лице да има пристап до клучевите. Друга можност којашто треба да се разгледа е раздвојувањето на клучевите од базата со податоци и нивно чување во шифрирана форма на некои хардверски уреди. Многу важно е клучот да не го напушти хардверскиот уред, пристапот да биде контролиран, т.е. и администраторот и напаѓачот да не можат да дојдат до него и да го земат.

8.9. Заштита на пристапот до клучевите

Сигурноста на клучевите зависи од доброто управување и местото за нивно складирање. Според некои истражувања, една третина од организациите своите важни

[21] M. Mihaljević, Z. Savić: Teorijski i praktični saveti kriptološkog kvaliteta zaštite privatnosti informacija, Stručni skup o zaštiti računarskih sistema, Savez inženjera i tehničara Srbije, Beograd 1995

податоци ги чува заедно со клучевите. Без стратегија за одвојување на клучевите од базата со податоци и чување на безбедни места со ограничен пристап, комплетниот систем е изложен на голем ризик од страна на многу корисници, програмери и администратори на бази со податоци. Системите коишто не ја поседуваат наведената стратегија опстојуваат благодарение на применети квалитетни аутентификациски методи за проверка на идентитетот и контрола на пристапот.[22]

9. Репликација на податоци и типови на репликација

Репликацијата на базите со податоци е една од мноштвото на алатки за заштита на податоците. Тоа е една од формите кои дозволуваат базите со податоци да ги имаме на повеќе различни места.

"Microsoft SQL Server" ги обезбедува следните видови на репликација, кои се користат во дистрибуцијата на апликации:

- Transactional - репликација;
- Merge - репликација;
- Snapshot - репликација;

Видот на репликација кој ќе биде употребен за апликација зависи од многу фактори, вклучувајќи ја физичката репликација на околината, видот и количината на податоците кои треба да се реплицираат и дали податоците се ажурираат на претплатникот (subscriber).

Физичката околина се однесува на бројот и локацијата на компјутерите коишто се вклучени во репликацијата и дали тие компјутери се клиенти (работни станици, лаптопи, преносни уреди) или сервери.

Секој тип на репликација вообичаено започнува со почетна синхронизација на објавените податоци помеѓу издавачот и претплатниците (Publisher and Subscribers). Почетната синхронизација може да се врши со репликација со слика (Snapshot), која е копија на сите објекти и податоци специфицирани од страна на Издавачот (Publisher). Откако ќе се креира сликата (Snapshot), таа се доставува до претплатникот (Subscribers). За некои апликации, snapshot-репликацијата е сè што им е потребно. За други видови на апликации е важно податоците да го менуваат протокот до претплатникот (Subscriber) со текот на времето. За некои апликации е исто така потребен променлив проток од претплатникот (Subscriber) па назад до издавачот (Publisher). Репликацијата

[22] A Menezes at all., "Handbook of Applied Cryptography", CRC Press, 1996

“Transactional” и репликацијата “merge” даваат можност за тој тип на репликации. Промената на податоците не се следат со Snapshot – репликацијата. Секогаш кога ќе се употреби оваа репликација, таа ги преклопува постоечките податоци. Репликацијата “Transactional” ги следи промените преку SQL Server transaction log. Исто така и “merge” репликацијата ги следи промените преку тригери и метадата табели.

9.1. Репликација Слика - “Snapshot”

Слика “Snapshot” репликацијата ги дистрибуира сите податоци идентично како што се во одреден момент и не ги мониторира измените коишто се прават. Кога синхронизацијата ќе се постави, сликата (shapshot) се генерира и се праќа на претплатниците (subscribers). Слика (“Snapshot”) репликацијата може да се користи сама по себе, но “Snapshot” - процесот (кој креира копија од сите објекти и податоци специфицирани од издавачот) е истотака често користен да обезбеди почетен сет од податоци и објекти за “transactional” и “merge” репликациите (слика 17)[23].

Користење на “Snapshot” репликација по себе е најсоодветно кога еден или повеке искази од следните е точен:

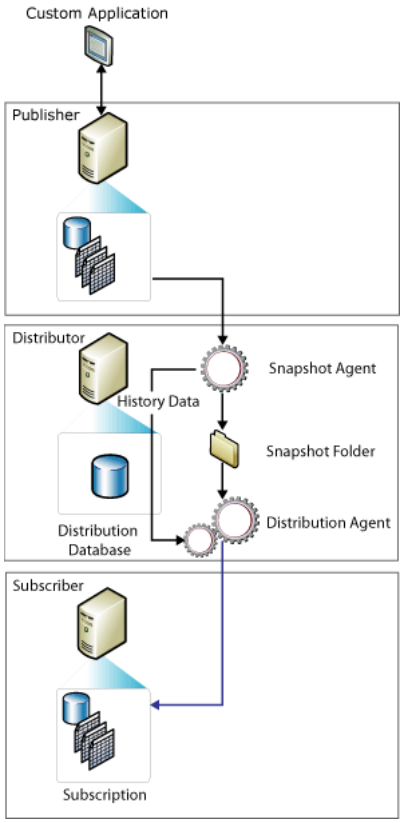
- Мала промена на податоци;
- Прифатливо е да се има копија на податоците којашто не е синхронизирана со издавачот подолго време;
- Се реплицираат малку податоци;
- Голем обем на промени се случуваат во краток временски период;

Значи, “Snapshot” репликација е најсоодветна кога имаме големи, значителни промени на податоци коишто не се фреквентни. На пример, во трговска организација која прави ценовник и сите цени се менуваат во исто време еднаш или двапати годишно, реплицирањето на податоците е задолжително. Кога има одредени типови на податоци, почесто правење на слики “Snapshot” е исто така соодветно. Пример, ако имаме релативно мала табела со податоци кај издавачот којашто се менува преку денот и мало доцнење е дозволено, промените може да се прават ноќе како “snapshot”.

“Snapshot” репликација има континуирано помал пристап до издавачот отколку кај “Transactional” репликацијата, затоа што поединечните промени не се следат. Како и да е, доколку опсегот на податоци за реплицирање е преголем, тој ќе побарува значително повеќе ресурси за генерирање и праќање на сликата (snapshot). Во зависност од

[23] http://www.link-university.com/lekcija/Replikacija/4851 [2016]

големината на податоците и фреквенцијата на промени на податоците, ќе оцениме дали треба да се користи овој тип на репликација.



Слика 17. Репликација “Snapshot”

9.2.Репликација Трансакциска - “Transactional”

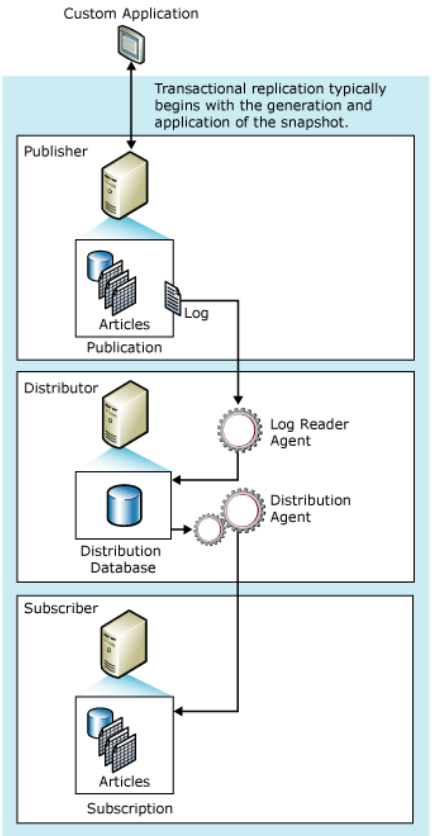
“Transactional” репликацијата обично започнува со слика на објавени објекти и податоци од базата на податоци. Штом е донесена првичната слика, секои промени на податоците и модификациска шема направени од издавачот (Publisher) обично се испорачуваат на претплатникот (Subscriber) онака (во моментот) кога се случуваат (во брзо реално време). Промените на податоците се пријавуваат кај претплатникот (Subscriber) во истиот редослед и граници - трансакции како што се случуваат и кај издавачот (Publisher), затоа трансакциската конзистентност е загарантирана (слика 18).

“Transactional” репликацијата обично се користи кај “server-to-server” околината и е соодветна- карактеристична во следните случаи:

- Доколку сакате поединечните промени да се пренесуваат на претплатникот (Subscriber) онака како што се случуваат;
- Апликацијата бара ниска латентност помеѓу промените во времето направени од издавачот (Publisher) и измена на промените кај претплатникот (Subscriber);

- Апликацијата бара пристап до членките на податоци. На пример, ако редот се менува пет пати, “Transactional” репликацијата ѝ дозволува на апликацијата да одговара на секоја промена (како отпуштање на чкрпалото), а не едноставно нет-податокот да се промени во редот;
- Издавачот (Publisher) има многу висок волумен на вметнување (insert), промена (update) и бришење (delete) активност;
- Издавачот (Publisher) или претплатникот (Subscriber) е non-SQL Server база на податоци како Oracle;

По дефолт претплатникот (Subscriber) кај “Transactional” објавата треба да биде сметан само како “read-only”, бидејќи промените не се пренесуваат назад кај издавачот (Publisher). Како и да е, “Transactional” репликацијата дозволува опција која му дозволува промени на претплатникот (Subscriber). Следната илустрација ги прикажува главните компоненти на “transactional” репликацијата:



Слика 18. Репликација “Transactional”

9.3. Репликација Спојување - “Merge”

Репликацијата “Merge”, како и “transactional” репликацијата стандардно започнува со слика од публицираните објекти и податоци.

Секоја промена на податоци и модификации на шема направени кај Издавачот (Publisher) и Претплатниците (Subscribers) се следат со “triggers” (окинувач). Претплатникот (Subscriber) се синхронизира со Издавачот (Publisher) кога се поврзува на мрежа и ги разменуваат сите редови кои биле сменети меѓу Претплатникот (Subscriber) и Издавачот (Publisher) откако последен пат се случила синхронизацијата.

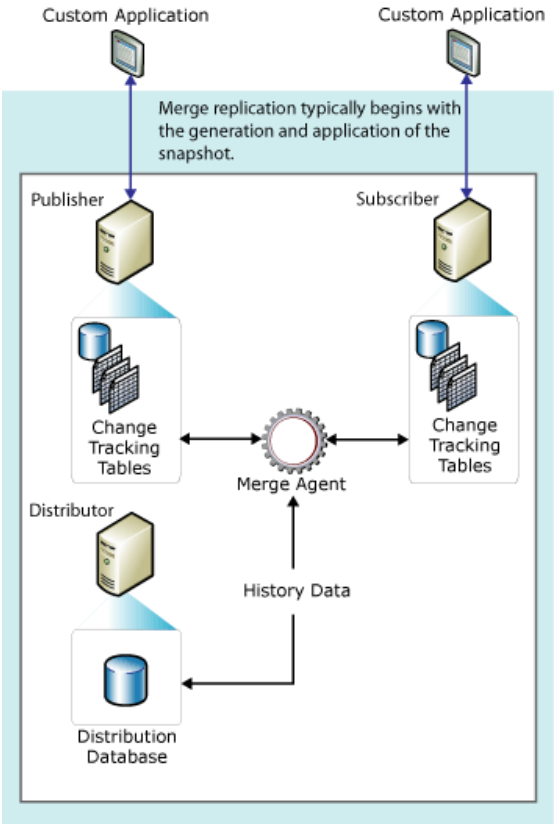
Репликацијата “Merge” вообичаено се користи кај “server-to-client” околина. “Merge” репликацијата е најсоодветна во некои од следните ситуации:

- Повеќе Претплатници (Subscribers) би можеле да ажурираат исти податоци во различно време и да ги пропагираат измените кај Издавачот (Publisher) и другите Претплатници (Subscribers);
- Претплатниците (Subscribers) е потребно да ги добијат податоците, да направат измени “offline”, и подоцна да ги синхронизираат измените со Издавачот (Publisher) и други Претплатници (Subscribers);
- Секој Претплатник (Subscriber) побарува различен сет на податоци;
- Може да се појават конфликти, а кога тие ќе се појават, треба да се има способност да се откријат и да се решат;

Апликацијата повеќе побарува помалку мрежни промени на податоците, отколку пристап до локалните податоци. На пример, ако кај Претплатникот (Subscriber) некој ред се менува пет пати пред да се синхронизира со Издавачот, тогаш кај Издавачот (Publisher) тој ред ќе се промени само еднаш за да се рефлектираат измените на тој ред.

“Merge” репликацијата им овозможува на различни точки да работат самостојно, а подоцна ги спојува во еден единствен резултат. Бидејќи промени се прават повеќе од еднаш, истиот податок може да биде променет –ажуриран од Издавачот (Publisher) и од повеќе од еден Претплатник (Subscriber). Затоа може да се појави конфликт кога ќе се спојат ажурирањата и “Merge” репликацијата овозможува повеќе начини за справување со конфликтот. Merge репликацијата се имплементира од “SQL Server Snapshot Agent”-от и “Merge Agent”-от. Ако публикацијата е нефилтрирана или има статичен филтер, “Snapshot” - Агентот креира една слика (snapshot). Ако публикацијата користи параметаризирани филтри, “Snapshot” - Агентот креира слика за секоја партиција од податоците. “Merge” Агентот ги доставува почетните слики до Претплатниците (Subscribers). Исто така, ги спојува поединечните промени на податоците што се појавиле кај Издавачот (Publisher) или Претплатниците (Subscribers) откако се креирала почетната слика и ги препознава и ги решава сите конфликти во согласност со конфигурираните правилата од страна на администраторот.

За да ги следи промените, “Merge” репликацијата (и “Transactional” репликацијата со редица ажурирани претплатници) мора да биде способна за уникатно идентификување на секој ред во секоја објавена табела. За да се постигне ова, “Merge” репликацијата додава колони “**rowguid”** на секоја табела, освен доколку табелата веќе содржи колона од дата тип “**uniqueidentifier”** со “**ROWGUIDCOL”** сет (во тој случај се користи оваа колона). Ако некоја табела се избрише (извади) од објавата, колоната “**rouwgid”** се отстранува, а ако се користи веќе постоечка колона за следење, тогаш таа колона не се отстранува. Филтерот не мора да го вклучи **“rowguidcol** “, кој се користи од репликацијата за идентификација на редовите. Функцијата “**newid()”** е предвидена по дефолт за колоната “**rouwgid”**, како и да е корисниците може да предвидат - добијат водич за кој било ред ако е потребно. Следниот дијаграм ги покажува компонентите кои се користат кај “Merge” репликацијата (слика 19).



Слика 19. Репликација “Merge”[24]

[24] http://www.link-university.com/lessons/details/4bd4b6ce-4bf5-11e0-b62b-00301bbbf52e [2016]

9.4. Хетерогени репликации на база на податоци

Оваа опција е применета во поновите генерации од ″SQL Server”. “SQL Server” ги поддржува следните хетерогени сценарија за Трансакциска и Слика репликација:

- Публицирање на податоци од “Oracle” до “SQL Server”;
- Публицирање на податоци од SQL Server до non-SQL Server Subscribers;

Хетерогената репликација на “non-SQL Server” претплатници е заостаната. “Oracle” публицирањето е заостанато. За пренесување на податоците, се создаваат - креираат решенија со промена на внес на податоци и “SSIS”.

10. Статистика која што загрижува

Во нашата држава, но и малку пошироко во регионот, многу малку се зборува за проблемот со нападите и со заштитата на базите со податоци. Многу малку или воопшто не може да се најдат податоци, статистики во овој домен. Затоа ќе земеме некои статистички податоци кои се на меѓународно ниво:

- На секои 39 секунди се случува по еден хакерски напад;
- Преку 90% од нападите на базите со податоци се случуваат во владините сектори, во малопродажната и во технолошката индустрија;
- 43% од сајбер - нападите ги погодуваат малите компании;
- 64% од компаниите претрпеле напади преку веб - апликациите;
- 62% од компаниите се соочиле со последици на фишинг и на социјален инженеринг;
- 59% од компаниите се соочиле со малвер и ботнет;
- 51% од компаниите претрпеле DDoS напади;
- Со оглед на растечкиот тренд на поврзување на деловната инфраструктура, просечната вредност на штетата којашто настанува со нападите на базите на податоци, во 2020 година преминува цифра од 150 милиони долари;
- Започнувајки од 2013 година, како последица од нападите на базите со податоци, скоро по 4,000,000 записи со податоци се крадат секојдневно, 158,727 секој час, 2,645 секоја минута или 44 секоја секунда;
- Во некои моменти преку 75% од здравствената индустрија била заразена со малвери;
- Кон крајот на 2016 година бројот на DDoS нападите се зголемил за 140%;
- Потребата од стручни лица за безбедност на бази со податоци ќе продолжи да отвора нови работни позиции во ИТ индустријата (проценка е дека само во САД бројот на

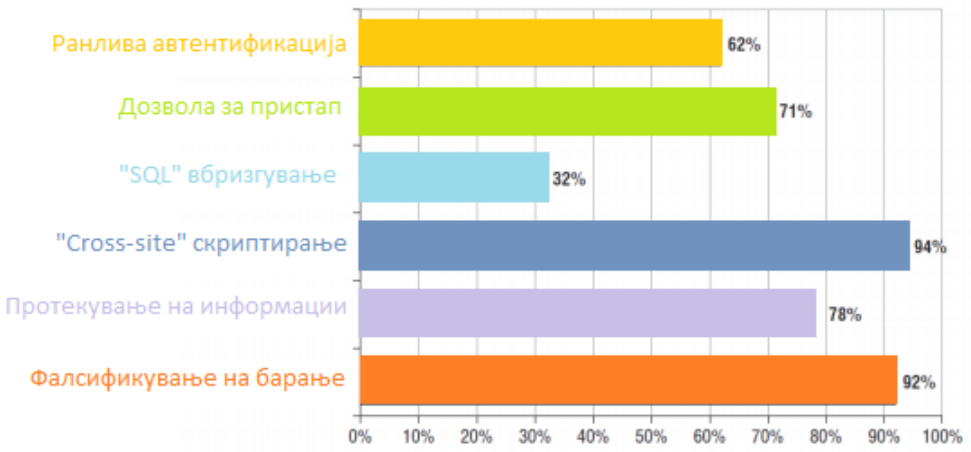
непотполнети работни позиции од наведените профили до 2020 година се искачила на 1.5 милиони);

- Интернетот со својот развиток продолжува да носи со себе можност за олеснување за размена на податоците, но и зголемен ризик од сајбер - напади. Се очекува бројот на поврзаните уреди до 2021 година да биде помегу 50 и 200 милијарди;
- Само 38% од компаниите на глобално ниво тврдат дека се соодветно подготвени за софистицирани сајбер - напади;

Направено е испитување на неколку стотини веб - апликации – бази со податоци, кои се тестирани во периодот од 2007 до 2011 година. Според направените анализи, добиени се следните резултати (слика 20):

- Ранлива автентификација [62%]. Се однесува на различни неправилности внатре во начинот на пријава. Тоа може на напаѓачите да им овозможи да погодат слаби лозинки, употреба на напади со брутална сила или заобиколување на пријавите;
- Дозвола на пристап [71%]. Се однесува на случаи кога апликациите не ги штитат доволно својата функционалност и податоците. Со тоа им се овозможува на потенцијалните напаѓачи пристап до базите со податоци, т.е. до осетливи податоци и информации, дури и можност за извршување на некои привилегирани акции;
- “SQL” вбризгување [32%]. Се однесува на ранливост на базите со податоци кога напаѓачите вметнуваат свој код во базата со податоци. Напаѓачите може произволно да ги користат податоците, да ја менуваат логиката или да извршуваат некои други операции над самата база со податоци;
- “Cross-site” скриптирање [94%]. Со овој напад се овозможува на напаѓачот да напаѓа други корисници на апликацијата, да добие пристап на нивните податоци, да извршува операции за кои не се авторизирани;
- Протекување на информации [78%]. Се однесува на ситуации кога апликациите дозволуваат откривање на осетливи информации коишто напаѓачите ги искористуваат . Во овој дел припаѓаат и случаите на неправилно ракување со грешките;
- “Cross-site request forgery” – Фалсификување на барање [92%]. Се однесува на случаи кога корисниците на апликациите се принудени да извршат ненамерни операции кон апликацијата од својот компјутер, според своите права и ограничувања. Оваа ранливост овозможува на малициозните веб - страници кои се посетени од страна на

корисниците да имаат интеракција со апликациите за да се изврши некоја акција за којашто корисникот немал намера да ја изврши;[25]



Слика 20. Инциденти од преку 100 тестирани апликации од страна на авторот на книгата "The Web Application Hacker's Handbook"[26]

11. Загуба на податоци

Губењето на податоците во компаниите може да се случи од повеќе причини. Најчеста причина се хардверските расипувања. Порано или подоцна, секој тврд диск може да се расипе. На секои 15 секунди по еден тврд диск доживува непоправливо расипување. Втора причина за губење на податоците може да биде негрижата на корисниците, во облик на губење на лаптопот, надворешни дискови или усб уреди. Губењето на податоците може да се случи и од софтверска грешка, вируси, природни катастрофи. Моментално во пораст е губењето на податоците поради сајбер - нападите.

Трошоци кои произлегуваат при губење на податоците се:

- Компензација и реконструкција на податоците;
- Замена на опремата;
- Истрага на инциденти;
- Повторно воспоставување на доверба кај купувачите;

Според определени студии на компанијата "Dell EMC"[27] дојдено е до следните заклучоци:

[25] https://www.itsvet.com/clico__cyber_beybednost-pcaa1-1901.i?id=206448

[26] Извор, авторите на книгата "The web application Hacker's Handbook", DAFYDD STUTTARD, MARCUS PINTO

[27] Студија на компанијата "Dell EMC"

- Вкупните трошоци поврзани со губењето на податоците и застојот, достигнуваат неверојатни 1.7 милијарди долари;
- Бројот на инциденти се намалува, но количината на изгубените податоци е во експоненцијален пораст;
- 51% од компаниите немаат план за спасување од катастрофа;
- Компаниите во Кина, Хонг Конг, Холандија, Сингапур и САД најмногу се грижат за бекап на базите со податоци;
- Компаниите во Швајцарија, ОАЕ и Турција најмалку се грижат за бекап на базите со податоци;

Според определени студии на компанијата "IDC" коишто ги покриле малите и средни компании:

- 40% од компаниите не прават бекап или барем 40% од податоците не е покриен со бекап процедури;
- 60% од податоците во компаниите се чуваат на компјутерите на вработените и не се покриени со бекап процедури;

Компанијата "British Chambers of Commerce"[28] има направено определени истражувања на компании кои претрпеле губење на податоци подолго од 10 дена:

- **50% престануваат со работа и згаснуваат веднаш**;
- **93% престануваат со работа и згаснуваат најдоцна за една година по инцидентот**;

Според истражувањето на компанијата "Diffusion Group"[29], направено врз мали компании кои претрпеле губење на податоци:

- **60% престануваат со работа најдоцна за 6 месеци по инцидентот**;
- **72% престануваат со работа најдоцна за 2 години по инцидентот**;[30]

12. Со броеви: Цена на чинење на губење на податоци на помала скала

Кога се испитуваат трошоците за загуба на податоци за компанијата, големи и нематеријални бројки нема да ве исплашат. Но, треба да се размисли за цената на чинење за загуба на податоците од само една индивидуална датотека. Кога се дискутира за бекап

[28] Студија на компанијата "British Chambers of Commerce"

[29] Студија на компанијата "Diffusion Group"

[30] https://hr.heptabackup.com/gubitak-podataka

и за стратегии за обновување од катастрофи (disaster recovery strategies), компаниите ги спомнуваат статистичките податоци за ризикот од загуба на податоци. Според компанијата “Seagate”, повеќе од 20% од компаниите коишто складираат околу 2-7 ТБ податоци, претрпеле загуба на податоците. Повеке од половината имале барем 2 до 3 настани за губење на податоците за една година.

Доколку овие бројки не Ви делуваат доволно застрашувачки, тогаш се појавуваат мерки кои се изразени во пари. Овие компании сакаат да направат проценка на трошоците на загуба на податоците. Според “Seagate”, 40 милиони долари годишно се губат поради настани поврзани со загуба на податоци. Според истражувачка студија на “Aberdeen”, просечно секоја компанија загубила 163,674 долари на неискористена работна сила и изгубила приход од секој час од застојот поради загубата на податоците.

Кога се разгледуваат овие бројки и проценти од една страна се добива впечаток дека заканите и не се така страшни, а загубата на податоците не е многу честа. Дури и да е толку често, сигурно цената на чинење не е толку висока?

Во вакви моменти на такво размислување, треба да се размисли за следната ситуација: Во компанијата се случува настан на загуба на податоци, без разлика од која причина, пожар, поплава, хардверска грешка, човечка грешка... Наместо да се разгледува варијантата за трошоците од загубата на податоците, може да се размисли колку чини доколку се загуби само една бела книга.

Да појасниме, бела книга е долга форма на информациски извештај креиран за едукативни цели. Вообичаено, тие се многу детални парчиња и треба да се вложи многу труд за да се создаде бела книга. Може да ги разложиме трошоците кои се потребни за развој на една бела книга од почеток до крај:

- **Истражување** – Директорот за маркетинг избира тема и ги започнува потребните истражувања за креирање на содржината на белата книга. Истражувањето вклучува работа со инженерскиот тим за да се пополнат соодветните технички детали. Вкупно време – 8 часа за директорот за маркетинг и 4 часа за инженерот;
- **Преглед** – Директорот за маркетинг започнува да ги реди деталите и да ја организира содржината. Вкупно време – 2 часа;
- **Нацрт** – Записничарот ги зема белешките од директорот за маркетинг и започнува да ја создава белата книга. Вкупно време – 8 часа;
- **Уредување** – Записничарот и директорот за маркетинг потоа заедно ја лекторираат, уредуваат и ја прегледуваат дотогашната работа, за да се потврдат дека сè е во ред. Вкупно време – 2 часа;

- **Слики** – Графичкиот дизајнер за одредени податоци од белата книга создава графици и графикони, вклучително и други визуелни претставувања. Вкупно време – 4 часа;
- **Изглед** – Графичкиот дизајнер ги зема сите копии и графици и ги поставува во читлив формат, креирајќи го финалниот производ. Вкупно време – 4 часа;

Вкупно, според погоренаведеното, за создавање на белата книга се потребни 34 часа. Земајќи ги предвид платите на секој од тројцата вработени (Директорот за маркетинг – 95К годишно, Инженер – 80К годишно, Записничар – 40К годишно, Графички дизајнер – 65К годишно) и времето потрошено за работа на проектот (директор за маркетинг – 12 часа, инженер – 4 часа, записничар – 10 часа, графички дизајнер – 8 часа), цената на белата книга ќе биде вкупно 1,144 долари.

Но, трошоците при губење на оваа датотека не завршуваат тука. Белата книга ќе треба повторно да се креира, а тоа е тешко бидејќи треба да се започне од нула. Можеби ќе се пронајдат некои рачно напишани забелешки или некој ќе се присети на она што е пишувано, но и во тој случај тоа само малку ќе го намали вкупното време за создавање на белата книга. Можеби вкупната цена на чинење ќе се намали на 800 долари.

Друга варијанта е враќање на податоците, што може да чини многу поскапо кај сериозно оштетени сервери и дискови. Кога сè ќе се собере, на крајот излегува дека губењето на една бела книга чини околу 2,000 долари. Една единствена бела книга. А да се замисли збирот на сите материјали што се создадени во компанијата, секој проект, сите сметководствени податоци, податоците за клиентите, сите податоци за сите документи и слично, исчезнати поради настан со кој е загубена базата со податоци. Цената во секој случај многу расте.

Секоја компанија што има многу податоци, губењето на податоците поради пожар, поплава, хардверска грешка, човечка грешка, неважно, претставува катастрофална загуба. Доколку дури и половина од загубените податоци побаруваат инвестиции како хипотетичкото создавање на белата книга, тогаш финансиската загуба ќе биде во многу голема.

Понатаму, се појавуваат трошоци кои не се финансиски. Губењето на довербата на клиентите кога ќе се изгубат податоци, кои може да бидат чувствителни или витални информации, може да го урнисаат работењето во следните години.

Може да се направи споредба на трошоците за загуба на податоците во пари (и главоболката) со цената на чинење на резервната варијанта. Резервната варијанта чини само еден мал дел од она што чини загубата на податоците.

Според сето погоренаведено, кога ќе се видат некои финансиски бројки при загуба на податоци, ќе имаме предвид дека бројките не се надувани. Дури и цената на чинење од губењето на една датотека е помало од трошоците на чинење за бекап варијанти.[31]

13. Реален пример на добра заштита на база со податоци

Од моето долгогодишно искуство во работата со бази на податоци и соработката со многу наши компании коишто имаат свои бази со податоци, ќе се обидам да сублимирам и да издвојам еден пример на добра ИТ - организација и заштита на база со податоци. Ќе биде наведено реално решение на заштита на база со податоци. Вистинското име на компанијата ќе го замениме со назив "Компанија Х".

Компанијата Х користи "ERP software"[32] којшто е составен од повеќе модули. Сите модули од апликативниот софтвер се засебни делови, но можат да функционираат и заедно. Модулите се хетерогени и независни еден од друг. Сите модули во апликативниот софтвер користат една заедничка база со податоци. Базата со податоци е од тип – релациона база со податоци.

Во компанијата е дефиниран таканаречен "домен" анг."domain"[33]. Со самото дефинирање на доменот, дефинирани се одредени правила како се приклучуваат корисниците во мрежата на компанијата. Поставено е користење на високо ниво на комплексност на лозинките на корисниците. Исто така, се води и политика на променливост на лозинките на одреден временски период и историја на употреба на лозинките[34]. Дополнително на работните станици е направено подесување на заклучување на истите после одреден временски период на неактивност. На корисниците на работните станици им се доделени кориснички имиња со одредени права и привилегии на пристап, како локално на самата работна станица, така и во целото мрежно опкружување на компанијата. На сите работни станици се инсталирани лиценцирани антивирусни апликации за заштита. На секоја работна станица е

[31] https://www.gillware.com/data-recovery-lab/numbers-cost-data-loss-smaller-scale/

[32] Enterprise resource planning (ERP) - Планирање на ресурсите на компанијата

[33] Доменот содржи група на компјутери до кои може да се пристапи и администрира со заеднички пакет правила. На пример, една компанија може да побара сите локални компјутери да бидат мрежни во истиот домен, така што секој компјутер може да се гледа од други компјутери во рамките на доменот или да се наоѓа од централен сервер.

[34] Историја на лозинки-не може да се употребува веќе еднаш искористена лозинка од корисникот

конфигурирано автоматско скенирање. Овој сет на мерки на заштита компанијата ја заштитува од неовластено влегување во мрежната околина на компанијата.

Модулите од ЕРП - софтверот се инсталирани на работните станици на корисниците според потребите. Кај секој корисник се инсталирани само модулите кои се потребни на тој корисник. За секој корисник, за влез во ЕРП - софтверот е дефинирано корисничко име со лозинка. Да напоменеме дека овие кориснички имиња и лозинки се различни од корисничките имиња и лозинки за најава на доменот. Во самиот ЕРП - софтвер е поставена контрола на комплексноста на лозинката на корисникот. Лозинката мора да биде дефинирана според добро познатите правила на комплексна лозинка, и тоа: минимална должина од 8 карактери, задолжителна употреба на голема буква, задолжителна употреба на бројка, задолжителна употреба на специјален знак. Во самиот ЕРП - софтвер се дефинираат групи на кориснички профили со точно и прецизно дефинирани права на пристап на корисниците. Откако ќе се дефинира корисникот, на корисникот му се определува на која корисничка група на профили припаѓа. Со тоа е строго определен пристапот на корисникот во ЕРП - софтверот, а со тоа и до самите податоци во базата со податоци. Корисниците можат да пристапат само до оние делови коишто му се претходно дозволени и може да ги извршуваат само оние операции коишто претходно им се доделени.

За секоја операција што се извршува во ЕРП - софтверот се води кориснички лог на активност. Со оваа операција во секое време овластените лица можат да ја видат и да ја проверат активноста на корисниците во апликацијата и во базата со податоци.

Базата со податоци е поставена на посебен, таканаречен “database”[35] сервер. Датабаза серверот е поставен во посебна сервер соба направена според определени правила за сервер - соби: обезбедено ладење на сервер - собата, направена посебна заштита од поплава на сервер - собата, обезбедено алтернативно напојување со електрична енергија, строго контролиран пристап во сервер - собата за точно определени луѓе по строго определен протокол, и др. Со ова е направена таканаречена физичка заштита на базата со податоци од несакани последици и неовластен пристап.

Поради тоа што компанијата е на неколку локации (во различни градови), на базата со податоци е дефинирана “merge” репликација. Со овој процес на репликација, компанијата има неколку придобивки. Како прво, се намалува протокот на податоци преку интернет, а со ова се зголемува брзината во работењето и се намалува ризикот од

[35] Физичкиот компјутер што се користи како домаќин на базата на податоци

злоупотреба на податоците преку интернет - мрежата. Како второ, податоците ги има на неколку локации и тоа ажурирани во реално време. Со ова е покриен сегментот на заштита на базите со податоци од природни непогоди, како што се: пожар, поплава, земјотрес и друго. Исто така, самите реплицирани податоци претставуваат дополнителни бекап варијанти на базите со податоци.

На базата со податоци е дефиниран автоматски бекап којшто се извршува во точно определено време. Спакувана копија од бекапот со точно определено име, автоматски се копира на друг дата сервер.

Во базата на податоци се содржат податоците коишто се за целата компанија. Меѓу останатите податоци, во базата со податоци се содржат и лични податоци од клиентите, вработените... Поради безбедносните политики на компанијата и заштитата на личните податоци, направено е криптирање на податоците за матичните броеви коишто се наоѓаат во базата со податоци. Направена е имплементација на соодветни "dll- dynamic link library" фајлови[36] со коишто се криптираат и декриптираат соодветните матични броеви. Штом ќе се внесе податок за матичен број во соодветно поле во апликативниот софтвер, апликацијата ќе го криптира тој податок и како таков ќе се запише во базата со податоци. Кога се пребарува во апликацијата, матичниот број се прикажува во криптирана форма. Само на определена форма во апликацијата којашто е строго контролирана (само определени корисници имаат пристап) може да се направи декрипција на матичниот број. Тоа значи доколку во определено поле на формата се внесе вредноста на криптираниот матичен број, во друго поле ќе ја добиеме вредноста на вистинскиот матичен број. Во базата со податоци не постои реален податок на матични броеви, туку матични броеви во криптирана форма. Тие матични броеви се нечитливи и неразбирливи за никого. Со тоа е направена максимална заштита на нивна намерна или ненамерна злоупотреба преку базата со податоци.

Дополнително, компанијата има дефиниран таканаречен "disaster recorery plan"[37]. Во тој план се точно наведени определени чекори и процедури на дејствување во зависност од дејството што се случило.

Во зависност од тоа кој дел од системот е оштетен, колкав процент од системот функционира или не функционира, се преземаат соодветни чекори.

[36] Датотека што содржи код за најчесто користени програмски функции на персонални компјутери (компјутери) што работат на оперативниот систем Виндоус на Microsoft Corporation.

[37] Збир на политики, алатки и процедури за да се овозможи обновување или продолжување на виталната технолошка инфраструктура на системите по природна катастрофа или катастрофа предизвикана од луѓе

Со сите горенаведени реални примери, спроведени во практичното и секојдневно функционирање на заштита на својот ИТ - систем, а со тоа и заштитата на базата со податоци, може да се каже дека “Компанијата Х” ги има спроведено сите мерки за заштита на базата со податоци. Но, како што и порано напоменавме, дека не постои унифициран стандардизиран систем и правилник за заштита на базите со податоци, може да заклучиме дека “Компанијата Х” треба постојано да ја контролира и да ја унапредува својата заштита на информациониот систем и на базата со податоци.

ЗАКЛУЧОК

Сумирајќи, заштитата за пристап започнува со тоа кој може да пристапи до податоците и каков вид напаѓачи на податоци сакаат да пристапат. Има голем опсег за подобрување на техниките што се користат за безбедност на базите со податоци. Според истражувањето, 84% компании сметаат дека безбедноста на базата на податоци е соодветна. 73% од компаниите кои предвидуваат додавање на базата на податоци ќе се зголемуваат од ден на ден. 48% од напаѓачите се овластени корисници. 48% од корисниците направиле злоупотреба на нивните привилегии. Разработивме и други прашањата поврзани со безбедносната база на податоци. Преку неколку предлози за дискрециono и задолжително обезбедување, претставени се модели за заштита на конвенционалните бази на податоци. Сепак, не постои стандард за дизајнирање на овие безбедносни модели. Работата презентирана во овој труд дава собрани информации за различни закани и нејзините безбедносни прашања на базата на податоци. Може да се прошири за да се дефинира, дизајнира и спроведе ефективна безбедносна политика на опкружување на базата на податоци и обезбедува консолидиран поглед на безбедноста на базата на податоци. Според истражувањето, овој труд се фокусираше на заканите и можните контрамерки што можат да бидат можни за да се обезбедат податоци во базите на податоци.

Комплексни процеси, кои се одвиваат во рамките на компјутерските системи во ниту еден момент не треба да се потценуваат, бидејќи опасностите што директно или индиректно, континуирано или повремено, ги загрозуваат овие процеси, во поголема или помала мера претставуваат закана за системот и нејзините објекти. Заканите се толку многубројни, меѓусебно поврзани и испреплетени, така што формираат комплексна мрежа на опасности во целиот информациски систем. Во таа смисла, важно е највисокото раководство на компанијата да разбере какви опасности можат да го загрозат информативниот систем, како и условите и околината што се погодни за појава на неповолни настани. Сите можни негативни последици што можат да се појават секогаш мора да бидат земени предвид.

Во денешниот свет на дистрибуирани информациски системи потребата за репликација на податоци сè уште е многу голема. Брзото темпо во секојдневниот живот, во бизнисот, во науката и во многу други области, наметнува потреба од брза достапност до информации. Најскапо нешто денес е информацијата.

И покрај тоа што жичаните и безжичните мрежи овозможуваат сè поголема брзина на пренос на податоци и мрежна пропустливост, сè уште постојат голем број на

информациски системи во коишто два или повеќе сервери не се поврзани во информациска мрежа. За нив констатираме дека е неопходно да прават постојана или периодична репликација на податоците.

Покрај сè што кажавме за репликацијата на податоци, може да се додаде дека тоа не е затворен процес. Не може еднаш да се направи репликација и да се очекува таа да остане така непроменета со години. Со оглед на тоа дека информациските системи непрестано еволуираат, се воведуваат нови технологии, нови можности, неопходно е и комерцијалното решение за репликација на податоци да мора да го следи тој тренд на технологијата. Мора да биде флексибилна и да овозможува секојдневни промени и напредок.

Нападите на базите со податоци од година во година растат, а со тоа и ризикот од компромитирање е сè поголем. Денес провајдерите на финансиски услуги, здравствените организации и сите оние коишто имаат бази со податоци мораат строго да ги почитуваат законите за лични податоци. Корисниците на услугите поради загриженост од откривање на податоците или злоупотреби, неминовно ќе ги зголемат одговорностите на секоја организација за давање на одредени услуги. Негативни ефекти кои настануваат како последица на напади, ќе се видат во законската одговорност, негативниот публицитет, изгубената доверба во јавноста, т.е. губење на пари и продуктивност. За да се избегнат наведените негативни ефекти во нашето опкружување, неопходно е да се планира стратегија за шифрирање во базите со податоци за заштита на важните податоци и стратегија против напади и други злоупотреби.

Користена Литература

[1]www. https://hr.heptabackup.com/gubitak-podataka

[2]https://www.gillware.com/data-recovery-lab/numbers-cost-data-loss-smaller-scale/

[3]http://www.link-university.com/lekcija/Replikacija/4851 [2016]

[4]http://www.link-university.com/lessons/details/4bd4b6ce-4bf5-11e0-b62b-00301bbbf52e [2016]

[5]https://technet.microsoft.com/en-us/library/ms152746.aspx [2016]

[6]https://technet.microsoft.com/en-us/library/ [2016]

[7]Robert Vierira: SQL Server 2005 Programiranje - 1/2006

[8]Gordana Pavlovic-Lazetic: Uvod u relacione baze podataka

[9]D. Bulatović, B. Trifunović: Šifrovanje i zaštita podataka u elektronskom prenosu novca, Zbornik radova

[10]S. R.Petrović: Kompjuterski kriminal, II Izdanje, Beograd, 2001.

[11]D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: Sigurnost računarskih sistema i mreža, Beograd, 2007.

[12]M. Mihaljević, Z. Savić: Teorijski i praktični saveti kriptološkog kvaliteta zaštite privatnosti informacija, Stručni skup o zaštiti računarskih sistema, Savez inženjera i tehničara Srbije, Beograd 1995.

[13]Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

[14]Sohail IMRAN, Dr Irfan Hyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009.

[15]Emil BURTESCU, Database Security- Attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009.

[16]Jiping Xiong, Lifeng Xuan, Jian Zhao and Tao Huang, Web and Database Security, Zhejiang Normal University.

[17]Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[18]Deepika, Nitasha Soni, Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

[19]Debasish Das, Utpal Sharma & D.K. Bhattacharyya, An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications, Volume 1, 2010.
[20]Shivnandan Singh, Rakesh Kumar Rai, A Review Report on Security Threats on Database, International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014.
[21]Debasish Das, Utpal Sharma, D.K. Bhattacharyya, An Approach to Detection of SQL Injection Attack Based on Dynamic Query Matching, International Journal of Computer Applications, Volume No.1–25,2010.
[22]A Menezes at all., "Handbook of Applied Cryptography", CRC Press, 1996.
[23]The Web Application Hacker's Handbook str. 7
[24]McDonald D., C. Metz, B. Phan, "PF_KEY Key Management API, Version 2" IETF RFC 2367, 1998.
[25]https://www.itsvet.com/clico__cyber_beybednost-pcaa1-1901.i?id=206448
[26]J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, September *3, 1999.*
[27]Mark Stamp, „Information security principles and practice ", San Jose State University, 2006
[28]M. Milosavljević, G. Grubor, Osnovi bezbednosti i zaštite informacionih sistema, Univerzitet Singidunum, Beograd, 2006
[29]William Stallings, "Cryptography and Network Security", Fourth Edition, Prentice Hall, 2006.
[30]http://www.naumovic-partners.com/3-najveca-rizika-po-sajber-bezbednost-za-kompanije/