امنیت درپایگاه داده ها

فهرست مطالب

مقدمه

یکی از مسائل قابل توجه در سازمان ها، در جهت محافظت از دارایی های با ارزش موجود در سازمان و همچنین جلوگیری از دسترسی های غیر مجاز به این دارایی ها، ایجاد امنیت در پایگاه های داده سازمان ها می باشد. بررسی های اخیر که از کارشناسان فناوری اطلاعات در سراسر جهان صورت پذیرفته است، نشان می دهد که 31.4 درصد از کارشناسان امنیت، معتقدند ایجاد و حفظ امنیت پایگاه داده، کار بسیار پیچیده ای بوده و از این پیچیده گی بعنوان مشکل و مانعی بزرگ در ایجاد امنیت در پایگاه های داده، یاد شده است. همچنین تقریبا 20 درصد از افرادی که مورد بررسی قرار گرفته اند، اعتقاد دارند که که نیاز به پرسنل متخصص و کارشناسان خبره، مانع دیگری در ایجاد امنیت پایگاه داده در سازمان ها است. اما جالبترین بخش این بررسی این است که، 13.2 درصد از افرادی که مورد بررسی قرار گرفته اند، اظهار داشته اند که مدیران سازمان ها هنوز میزان اهمیت امنیت پایگاه داده را درک نکرده و از اینرو اقدامات لازم، برای ایجاد امنیت در پایگاه های داده را نادیده می گیرند. با طرح این سوال از افراد مورد بررسی که "چالش اصلی در پیاده سازی امنیت پایگاه داده در سازمان چیست؟" نتایج زیر حاصل شد:

- پیچیدگی: 31.4 درصد
- نیاز به کارشناسان خبره و پرسنل متخصص: 19.9 درصد
- عدم درک مدیران از لزوم ایجاد امنیت پایگاه داده: 13.2 درصد
- هزینه: 9.1 درصد
- سایر موارد:26.4 درصد

"از نظر کارشناسان حوزه امنیت، تهدیدات ناشی از عدم وجود امنیت در پایگاه داده، بسیار خطرناک است، از اینرو امنیت پایگاه داده باید بعنوان عاملی اساسی در راهکارهای حفاظتی سازمان، درنظر گرفته شود". حملاتی که سبب دسترسی غیرمجاز به پایگاه داده می شوند، ممکن است در هر ساعت، بارها اتفاق بیفتند؛ باید توجه داشت که دارایی های باارزش سازمان در این پایگاه های داده قرار دارند و در نتیجه بدون اعمال راهکارهای حفاظتی، این اطلاعات به راحتی می توانند مورد دسترسی غیر مجاز و در دسترس مهاجمان قرار گیرند. عدم ایجاد امنیت در پایگاه داده، به معنای باز گذاشتن تمامی راه ها برای دسترسی های غیر مجاز به این اطلاعات و از دست دادن موجودیت های با ارزش سازمان است که ضرر و زیان های مالی و در نتیجه آسیب به اعتبار سازمان را بهمراه دارد

- **داده (Data)**

- به یکسری مفاهیم بی قاعده و نامنظم اطلاق می شود. به طور کلی داده عبارت است از نمایش ذخیره شده کلیه موجودیت ها، واقعیت ها و رخدادها که در تصمیم گیری به کار می آیند.

- تعریف داده از دیدگاه ANSI:

- هر نمایشی که توسط انسان یا یک سیستم مکانیکی خودکار معنایی به آن قابل انتساب باشد.

- نمایش واقعیات، مفاهیم، پدیده ها یا شناخت ها به طرزی صوری و مناسب برای برقراری ارتباط، تفسیر یا پردازش توسط انسان یا هر دستگاه خودکار.

- به طور کلی می توان گفت داده ها ارزشهای واقعی هستند که از طریق مشاهده و تحقیق بدست می آیند.

- **اطلاعات (Information):**

- ماحصل پالایش داده های خام اطلاعات است بدین مفهوم که داده ها بررسی شده و یکسری مفاهیم باقاعده و مفید از دل آنها با نام اطلاعات بدست می آید.

- هر نوع داده پردازش شده (ساخت یافته) را اطلاع می نامند.

- تعریف اطلاع از دیدگاه ANSI:

- معنایی که انسان از طریق توافقات و قراردادهای شناخته شده ای به داده منتسب می کند.

- نکته: اطلاع و داده با هم فرق دارند اطلاع دارای خاصیت ارتباط دهندگی و انتقال دهندگی است در حالی که داده مجرد این خاصیت را ندارد.

- **دانش :**

- عبارت است از نمایش نمادین بخش هایی از دنیای واقعی. به بیانی دیگر، دانش یک نوع شناخت است که از یک مجموعه از اطلاعات، بر اساس یک مجموعه از قواعد مشخص بدست می آید.

- داده ها حالت منفرد و مجزا دارند و لزوما اطلاعی از آنها بدست نمی آید مگر اینکه بنحوی بهم مرتبط شوند و معنایی به آنها منتسب شود و دانش را باید نوعی اطلاع سطح بالاتر دانست.

- در واقع هم اطلاع و هم دانش حاصل عملیاتی روی داده هستند. ولی نوع عملیات لازم برای حصول آنها متفاوت است.

- **روشهای ذخیره داده ها**

1) سیستم فایلی ساده (روش سنتی) (File System) 2) سیستم پایگاه اطلاعاتی (Database System)

1) سیستم فایلی ساده (روش سنتی) (File System)

- **داده ها در چند مجموعه مجزا و نامجتمع (از لحاظ منطقی و فیزیکی) و تا حدود زیادی نامرتبط با هم و بدون مدیریت متمرکز خواهند بود.**

ویژگیها :

- مجزا قرار گرفتن داده ها در فایلها و طراحی سیستم جداگانه برای استفاده از فایلهای داده
- هر فایل یکنواخت شامل آرایه های دو بعدی از اقلام اطلاعاتی
- وارد شدن داده ها از یک برنامه به برنامه دیگر
- ایجاد فایلهای داده به منظور تأمین یک سری نیازهای خاص پردازشی
- هدف هر برنامه رفع نیازهای یک واحد خاص یا یک گروه خاصی از کاربران
- ارجاع هر برنامه ی کاربردی تنها به فایل داده ای مربوط به خود

ذخیره اطلاعات بصورت رشتهء پیوسته ای از بایتها

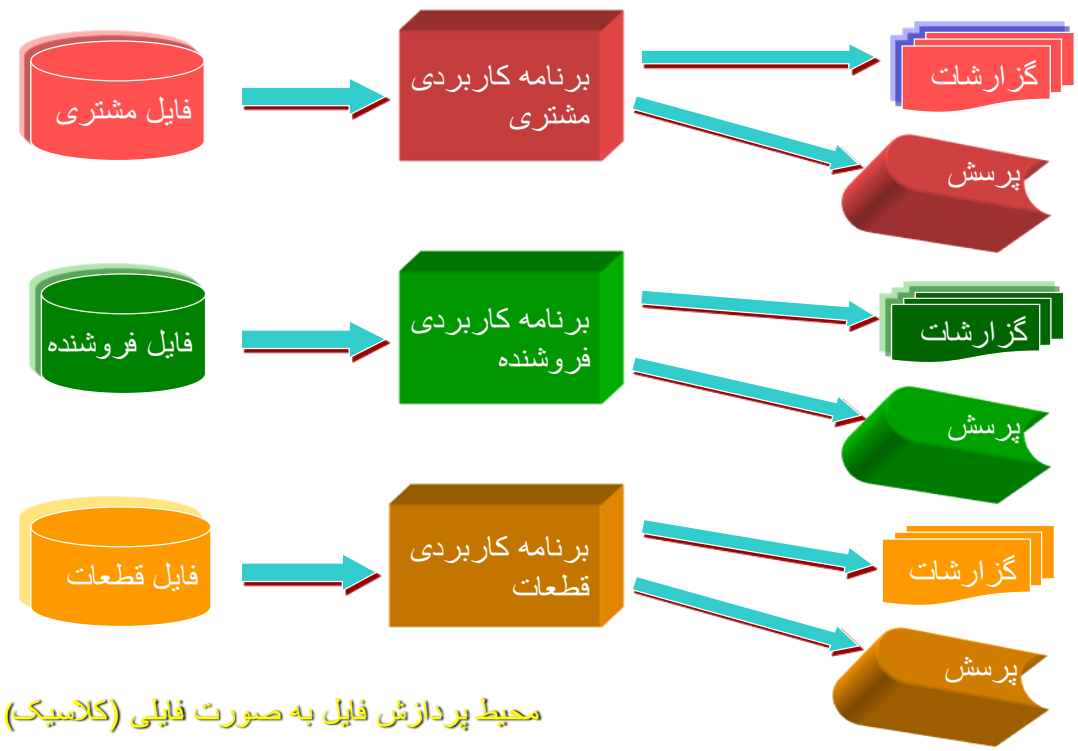
مزایا :

- کارآیی
- سادگی

- سفارشی کردن
- استفادهء مؤثر از فضا (حافظه)

معایب :

- مشکل بودن مکان یابی و عملیات آن روی داده ها
- تفکیک داده ها
- وابستگی داده ها و برنامه
- ناسازگاری (Data Inconsistency)
- افزونگی بیش از حد داده ها (Data Redundancy)
- مشکلات یکپارچگی (Atomicity)
- عدم دستیابی همزمان
- کاهش صحت داده ها (Data Correctness)
- عدم سهولت رعایت جامعیت (Universality)
- مشکلات امنیتی (Data Security)



محیط پردازش فایل به صورت فایلی (کلاسیک)

- **سیستم پایگاه اطلاعاتی (**Database System**)**

- تاریخچه پایگاه اطلاعاتی
- دهه ۱۹۶0 : گسترش اولین سیستم مدیریت پایگاه داده و ایجاد دو مدل سلسله مراتبی و شبکه ای (توسط پیشگامانی از جمله چارلز باخمن(
- : 1970ایجاد مدل رابطه ای توسطE. F. Codd
- اوایل دهه 1970 : بکار گیری عنوان بانک داده‌ای در اروپا
- اواخردهه 1970 : بکار گیری عنوان بانک داده‌ای در امریکا
- : 1980پژوهش بر روی مدلهای توزیع شده و ماشین‌های پایگاهی
- : 1990توجه به مدل شی گراء
- اواخردهه 1990 : رشد جهانی وب و پشتیبانیDBMS ها از واسط وب به داده
- 2000 : نوآوری پایگاه اکس‌ام‌ال (XML) و زبان تقاضای XQuery

تعریف پایگاه داده :

مجموعه ای است از داده ها که بصورت مجتمع و تاحد ممکن بصورت مرتبط بهم و با کمترین افزونگی ذخیره شده اند که این مجموعه تحت مدیریت یک سیستم کنترل متمرکز برای استفاده یک یا چند کاربر قرارگرفته اند .

- هر سیستم پایگاه داده از چهار جزء اساسی تشکیل می شود:
  - 1- داده ها : داده های کاربر- سیستمی

2- سخت افزار: ◦

1-2 : سخت افزار ذخیره سازی داد ه ها : منظور همان رسانه های ذخیره سازی خارجی است. ◦

- 2-2 سخت افزار پردازشگر : منظور خود کامپیوتر (یا سرور) است.
- 2-3 :سخت افزار برقرار کننده ارتباط : منظور از سخت افزار برقرار کننده ارتباط، سخت افزار ارتباطی بین کامپیوتر و دستگاه های جنبی و نیز بین کامپیوتر هاست.
- 2-4 : امکانات محلی: برای ایجاد ارتباط بین کامپیوتر و دستگا ههای جنبی آن در یک سایت به کار می رود.
- 2-5 : امکانات شبکه ای: در ایجاد سیستم پایگاه داده های با معماری نا متمرکز به کار می رود .

- 3- نرم افزار: بین داده هایی که به صورت فیزیکی روی دستگاه های ذخیره سازی مناسب استقرار می یابد و پایگاه داده ها را به وجود می آورند و استفاده کنندگان یک می نامند. (DBMS)گیرد که آن را سیستم مدیریت پایگاه داده لایه نرم افزاری قرار می

- نرم افزار ها خود به دو دسته تقسیم می شوند:

- 1- نرم افزار کاربردیAPPLICATION 2- نرم افزار سیستمی DBMS

4- کاربر:

- کاربران پایگاه داده را می توان به سه گروه اساسی و متفاوت تقسیم نمود:

- **برنامه نویسان کاربردی** : افرادی هستند که با اطلاعاتی که در مورد پایگاه داده پیدا می کنند می توانند برنامه های مناسبی جهت بروز کردن اطلاعات و یا استفاده از اطلاعات موجود در پایگاه داده تهیه نمایند .

- **کاربران واقعی یا نهایی** : افرادی هستند که با استفاده از امکاناتی که پایگاه داده در اختیار آنها قرار می دهد می توانند امور مربوط به خود و موسسه و سازمان را انجام دهند.

- **مدیر پایگاه داده ها** : مدیر پایگاه داده مسئولیت کنترل متمرکز سازمان بر داده های عملیاتی را بر عهده دارد.

ویژگیها :

- کانون توجه، داده هاست و نه شیوه های پردازش آنها
- داده ها بعنوان یک منبع مشترک مورد استفاده کاربران مختلف
- سیستم مدیریت پایگاه داده (DBMS) بعنوان واسطه بین برنامه های کاربردی و پایگاه داده
- الصاق بر چسب و دسته بندی قطعات مختلف داده ها
- فراهم کردن ابزار بسیار قدرتمندی برای مدیریت اطلاعات
- ذخیره کلیه داده ها به صورت مجتمع در پایگاه داده
- سیستم پایگاه اطلاعاتی (Database System)

مزایا :

- تجمع: وحدت ذخیره سازی داده های عملیاتی و کنترل متمرکز آنها
- کاهش افزونگی داده ها (Non Redundancy)
- کنترل بهتر
- پرهیز از ناسازگاری (سازگاری) (Consistency)
- استقلال برنامه های کاربردی و داده (Independence)
- قابلیت انعطاف (Flexibility)
- به اشتراک گذاشتن داده ها (Shared)
- سیستم پایگاه اطلاعاتی (Database System)
- ماندگاری (Persistence)
- اعتبار (Validity)
- افزایش مسائل امنیتی و اعمال آسان محدودیتهای آن (Security)
- ایجاد تعادل بین درخواستهای تداخلی
- راحتی پیاده سازی برنامه های کاربردی جدید
- تعدد شیوه‌های دستیابی و تسهیل دستیابی به داده‌ها
- مدلینگ داده‌های عملیاتی بر اساس ساختار آنها

سیستم پایگاه اطلاعاتی(Database System)

معایب : پیچیدگی و دشواری و زمانبر بودن طراحی این سیستمها

صرف هزینه قابل توجه برای سخت افزار و نصب نرم افزار

تأثیر آسیب دیدن پایگاه داده روی کلیه برنامه های کاربردی

هزینه زیاد برای تبدیل سیستم فایلی به سیستم پایگاه داده

نیازمند تعلیم اولیه برنامه نویسان و کاربران

نیاز به تهیه چندین کپی پشتیبان از پایگاه داده

فاجعه انگیز بودن خطاهای برنامه

طولانی بودن زمان اجرای هر برنامه

وابستگی زیاد به عملیات سیستم مدیریت پایگاه داده

- **تعریف پایگاه اطلاعاتی (**Database**)**
- مجموعه ای سازمان یافته و بدون افزونگی از اطلاعات و داده های مرتبط بهم
- مجموعه ای از فایلهای مرتبط بهم
- مجموعه‌ای از رکوردها یا تکه‌هایی از یک شناخت
- مجموعه‌ای از رکوردهای ذخیره شده در رایانه، با یک روش سیستماتیک (اصولی)
- مجموعه‌ای از داده‌هایی با خصوصیات یکسان
- مجموعه‌ای از موجودیتهای مرتبط به هم، شامل جداول، فرمها، گزارشها، پرس و جوها و اسکریپتها

مدل کردن پایگاههای اطلاعاتی (Data Modeling)

- مدل داده نشان دهنده طرح خاصی از بانک اطلاعاتی
- روشی برای توصیف داده ها و عملیات روی آنها در سطوح مختلف معماری پایگاه داده
- قالب قراردادی برای ساخت و کارکردن با داده
- توصیف پدیده های دنیای واقعی و تعریف ساختار داده
- تعیین چگونگی نمایش داده ها توسط یک DBMS
- ساختاری منطقی از نحوهء ذخیره سازی رکوردها در یک پایگاه اطلاعاتی

- روشی برای به تصویر کشاندن روابط انتزاعی بین داده ها

- **مدلهای پایگاههای اطلاعاتی (**Database Models**)**

شیوه های مختلف مدل سازی داده ها در پایگاه طراحی:

- تخت (Flat or Table Model)
- سلسله مراتبی (Hierarchical Model)
- شبکه ای (Network Model)
- رابطه ای (Relational Model)
- شیء گرا (Object Oriented)
- نیمه ساخت یافته (XML)

سیستم مدیریت پایگاه اطلاعاتی (DBMS)

- Database Management System : برنامه ای که بمنظور ساخت پایگاههای اطلاعاتی بکار می رود و عملیات درونددهی داده ها در پایگاههای اطلاعاتی و سپس پردازش داده ها را انجام می دهد.
- مهمترین نرم افزاری در سیستم پایگاه داده است که به عنوان رابط بین پایگاه داده و کاربر و برنامه های کاربردی عمل می نماید.
- برنامه رایانه‌ای که برای مدیریت و پرسش و پاسخ بین پایگاه‌های داده‌ای استفاده می‌شود.

- کلیه فایل های پایگاه داده فقط در اختیار این نرم افزار قرار گرفته و دستیابی تنها از طریق آن امکان پذیر است.
- مجموعه ای پیچیده از برنامه های نرم افزاری است که ذخیره سازی و بازیابی داده های سازمان را (فیلدها، رکوردهاوفایلها) در پایگاه داده ها، کنترل میکند.
- این سیستم، کنترل امنیت و صحت پایگاه دادهها را نیز بر عهده دارد.

سیستم مدیریت پایگاه اطلاعاتی(DBMS)

وظایف DBMS ها:

زبان تعریف داده ها(Data Definition Language) (DDL)

زبان پردازش و مدیریت داده ها (Data Manipulation (DML) Language)

دیکشنری داده ها (Data Dictionary)

- مزایای DBMSها :
- جامعیت داده ها
- دسترسی سریع به داده ها
- افزایش کنترل داده ها
- سهولت استفاده از برنامه کاربردی و مدیریت آن
- امنیت مناسب داده ها
- استقلال داده ها
- روابط پیچیده بین داده ها
- کنترل افزونگی داده
- عمومیت کاربردها
- سهولت استفاده

- سهولت در اعمال تغییرات

- **سیستم مدیریت پایگاه اطلاعاتی (**DBMS**)**

فهرستی از DBMSها :

از معروفترین DBMSمی‌توان به چند نمونه زیر اشاره کرد :

- Oracle
- Microsoft SQL Server
- MySQL
- PostregSQL
- DB2
- Microsoft Access

بخش دوم

امنیت درپایگاه داده ها

با گسترش روزافزون استفاده سازمانها از پایگاه دادهها در امور روزانه و تصمیم سازیهای سازمانی، نقش امنیت اطلاعات و دادهها اهمیت روزافزونی یافته است .گسترش سریع کاربردهای مبتنی بر وب از سیستم-های پایگاهی این مقوله را اهمیتی مضاعف بخشیده است . امروزه حفاظت از اطلاعات سازمانی نه تنها درارتباط با کاربران خارجی که در برابر سوءاستفاده کاربران داخل سازمان مورد توجه قرار گرفته است.

داده از سرمایههای اصلی هر سازمان است که روز به روز بر حجم آن و میزان استفاده از آن افزوده می-شود .این دادهها در سازمانها نقش اساسی اسفا میکنند و مبنای تصمیمگیریهای استراتژیک، مدیریتی واستراتژیک هستند .حفاظت از دادهها در قبال خطراتی که سازگاری، صحت، دقت، خصوصیبودن ومحرمانگی آنها را تهدید میکنند، امری اجتنابناپذیر است .اهمیت و حساسیت ایمنی پایگاه دادهها بویژهبه گسترش دانش و تکنولوژی دادهکاوی 1 و کشف دانش 2 بیشتر عیان میشود.

امنیت اطلاعات و جایگاه امنیت در پایگاه داده رابطه ای

ایمنی عبارت است از حفاظت دادهها در قبال دستیابی غیرمجاز، تغییر غیرمجاز یا تخریب آنها و نیز درقبال دستیابی به دادهها با سوء نیت .تفاوت مفهوم ایمنی با جامعیت 3در نوع کاربر مورد نظر در تعریفآنهاست .در ایمنی مورد بحث کاربر خارجی و جلوگیری از دسترسی او به دادهها است؛ در صورتی که درجامعیت بحث بر سر کاربر مجاز و حصول اطمینان از صحیح بودن عملیات او در دادههاست.

نفوذهای امنیتی را میتوان به سه گروه

1- مشاهده غیرمجاز دادهها،2- تغییر غیرصحیح دادهها 3- دردسترس نبودن دادهها تقسیم کرد .

بر این اساس یک راه حل کامل برای تامین امنیت داده باید به سه نیازمندی زیر

پاسخ گوید:

.1محرمانگی که حفاظت دادهها در مقابل افشاسازی غیرمجاز است،

.2جامعیت که پیشگیری از تغییر غیرمجاز و نامطلوب دادهها است و .3در دسترس بودن که پیشگیری و ترمیم خطاهای نرم افزاری و سخت افزاری و نیز عدم پذیرش دسترسی های ناجور به دادهها است.

در کنار این نیازمندیها، نیازمندیهای پوشیدگی- 2 که عبارت است از امکان استفاده از داده توسط کاربرمجاز فقط به شکلی که تعیین شده است -نیز اهمیت ویژهای یافته اند.

حفاظت از دادهها توسط مولفههای مختلفی از یک سیستم مدیریت پایگاهی تامین میشود .یک مکانیزم کنترل دسترسی 3محرمانگی دادهها را تضمین میکند .عملیات مجازشناسی 4امکان انجام عملیات توسط فرد را روی شیء خاص بررسی و کنترل میکند .از تکنیکهای رمزنگاری 5در ذخیره و انتقال دادهها برای حفظ محرمانگی استفاده میشود که در این باره چگونگی پاسخ به پرسشها از روی داده رمزنگاری- شده مورد توجه خاص قرار گرفته است.

نیازمندیهای امنیتی

در اینجا دستهبندی دیگری از نیازمندیهای امنیتی برای تامین ایمنی پایگاه دادهها ارائه میگردد .این موارد در واقع نمونههای متمایز نیازمندیهای امنیتی نسبت به سایر سیستمهای اطلاعاتی هستند.

.1جامعیت فیزیکی پایگاه -ایمنی دادههای موجود در پایگاه نسبت به مخاطرات فیزیکی .2 جامعیت منطقی پایگاه -ایمنی ساختار پایگاه بعنوان مثال در مقابل انتشار تغییرات ناخواسته .3جامعیت عناصر -دقت دادههای موجود در هر عنصر پایگاه

امکان ردگیری عامل انجام عملیات) دسترسی یا تغییر (در داده .4 (Auditability)- -نظارت پذیری های پایگاه .5 کنترل دسترسی -امکان محدود ساختن هر کاربر به دادههایی که مجاز به دسترسی یا تغییرآنهاست .6هویت شناسی کاربران -بررسی هویت کاربران در ارتباط با ردگیری نظارتی و اجازه دسترسی بهدادههای خاص .7در دسترس بودن -امکان دسترسی به پایگاه در همه شرایط جامعیت پایگاه بصورت کلی از مسئولیتهای سیستم مدیریت پایگاه، سیستم عامل و مدیر سیستمکامپیوتری است .از منظر سیستم عامل و مدیر سیستم، پایگاه داده بعنوان مجموعهای از فایلها و برنامه ها دیده میشود .بدین ترتیب تهیه نسخههای

پشتیبان از این فایلها میتواند بعنوان راهحلی برای مقابله باخرابیهای فاجعهآمیز مورد استفاده واقع شود .قابلیت ترمیم نیز از ویژگیهایی است که سیستم پایگاهی باید بدان مجهز باشد.

جامعیت عناصر پایگاه شامل درستی 1 و دقت 2 آنهاست .با این وجود که کاربران در نهایت مسئول وارد کردن دادههای صحیح در پایگاه هستند، میتوان تمهیداتی را در جهت پیشگیری از ورود دادههای نادرست در هنگام ورود و تصحیح آنها پس از ورود دادهها بعمل آورد .

روشهای مختلف تامین جامعیت پایگاه به سه

دسته بررسی فیلدها، کنترل دسترسی و نگهداری ثبت تغییرات 3تقسیم میشوند.

امکان نظارتپذیری به دو صورت مورد استفاده قرار میگیرد .در صورت نخست میتوان از روی یکثبت به فعالیتها و دسترسیهای یک کاربر) احتمالا پس از انجام عملیات (پی برد . صورت دوم شامل امکان بررسی دنبالههای دسترسی یک کاربر به منظور تصمیمگیری در مورد اعطاء دسترسیهای بیشتر درحالاتی است که امتیاز دسترسیهای جدید در پی انجام یک سری عملیات یا دسترسیها واگذار میگردد.

بعضی از سیستمها کاربران خود را به گذراندن مراحل متعدد هویتشناسی ملزم میکنند . بعنوان مثال یک پایگاه داده ممکن است کاربران خود را در معرض درخواست نام کاربری و گذرواژه و نیز بررسی ساعت از روز قرار دهد .این نیازمندیهای هویتشناسی به نیازمندیهای سیستم عامل) هویتشناسی سیستمعامل (اضافه میشوند.

داده حساس

داده حساس عبارت از دادهای است که نباید بصورت عمومی مورد دسترسی قرار گیرد . تعیین این دادههاوابسته به پایگاه مورد نظر و معنای دادهها در آن دارد .در حالتی که تمام دادهها حساس یا غیرحساس هستند، کنترل دسترسی به این دادهها سادهترین حالت ممکن را دارد.

در حالتی که پایگاه همزمان شامل دادههای حساس و غیرحساس است، بر مبنای میزان حساسیت داده محدودیت دسترسی کاربران مختلف به دادهها متفاوت خواهد بود .در این حال گاه اطلاع از وجود دادهای) و نه اطلاع از مقدار آن (نیز میتواند دارای حساسیت باشد . بدین برتیب نه تنها مقادیر دادهها بلکه زمینه و معنای آنها نیز شامل موضوعات امنیتی میشوند.

عواملی که باعث حساس بودن داده می شوند، عبارتند از:

.1ماهیت حساس) محل موشکهای دفاعی(

.2منبع حساس) دادهای که منبع آن در اثر افشای داده افشا میگردد(

.3اعلان خارجی) دادههای نظامی طبقهبندیشده(

.4جزئی از یک داده حساس) رکوردی که نشاندهنده یک ماموریت موشکی مخفی است(

.5حساسیت در ارتباط با دیگر داده ها) طول جغرافیایی یک معدن مخفی اورانیوم در ارتباط با عرضجغرافیایی آن(

انواع افشای دادههای حساس بشرح زیراند:

.1مقدار داده

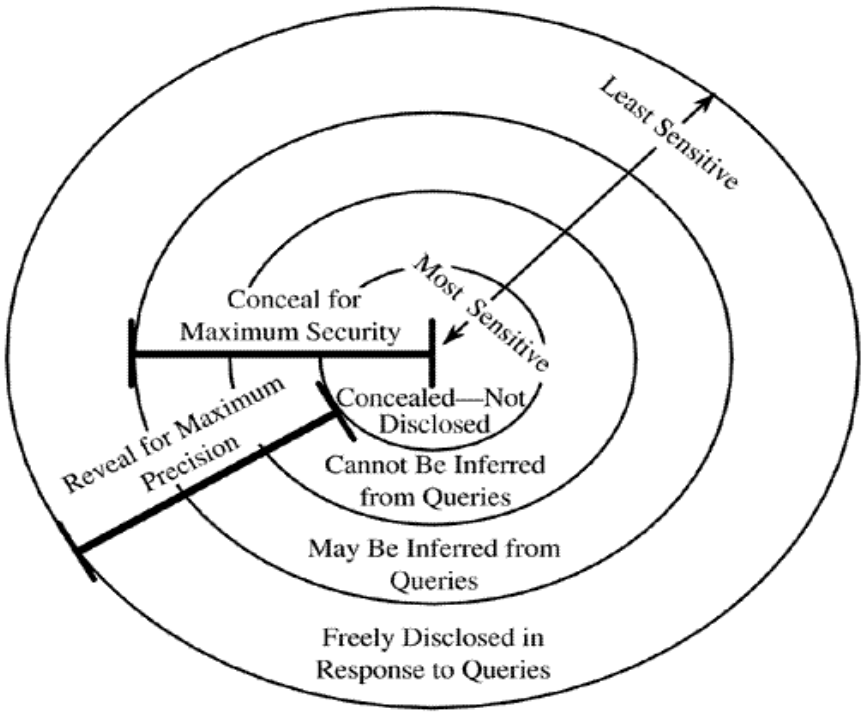
.2محدوده داده

.3نتایج منفی -درخواست عکس یک پرسش

.4وجود

.5مقادیر احتمالی -تعیین احتمال وجود یک مقدار در پایگاه از روی پرسشهای مرتبط

در این میان باید در نظر داشت که افزایش امنیت نباید به قیمت کاهش دقت سیستم در ارائه اطلاعات مورد نیاز کاربران تمام شود .رابطه امنیت با دقت در نمودار زیر آمده است.



روش های کنترل دسترسی در نرم افزار

اصطلاح کنترل دسترسی مدتها بصورت مفهومی مبهم مطرح می گردید. گاهی بعنوان کنترل دسترسی به یک سیستم از طریق منابع خارجی تفسیر می شد، مثل کنترل کردن روند ورود

کاربران برای دسترسی داشتن به سرور و یا دسکتاپ. بدین طریق به این اصطلاح بعنوان روشی برای تایید و اهراز هویت کاربران نگاه می شد، درحالیکه مبحث اهراز هویت کاملا مستقل می باشد.

اصطلاح کنترل دسترسی در واقع به کنترل بیشتر بر روی دسترسی به منابع سیستم اشاره دارد یعنی فرض را بر این می گذاریم که هویت کاربر مورد تایید قرار گرفته است و اکنون چگونگی نحوه دسترسی کاربر به منابع باید کنترل گردد.

در محیط رقابتی امروز، تامین امنیت داده ها و تعیین نحوه دسترسی به آنها بصورت حداقل لازم (privilege leat) ،یکی از مباحث لازم و ضروری می باشد، به همین منظور راهکارها و مدل های متفاوتی ارائه شده است که در اینجا ما به 4 مدل اساسی می پردازیم .

انواع مدل های کنترل دسترسی

- ☑ کنترل دسترسی اجباری(Mandatory Access Control-MAC)
- ☑ کنترل دسترسی اختیاری(Discretionary Access Control-DAC)
- ☑ کنترل دسترسی مبتنی بر نقش(Role Based Access Control-RBAC)
- ☑ کنترل دسترسی مبتنی بر قوانین(Rule Based Access Control-RBAC)

اما توجه داشته باشید یک مدیر، طراح و یا تحلیلگر همیشه بر اساس نیازها و قابلیت های تعریف شده برای محیط کاری خود، مدلی را انتخاب می نماید.

کنترل دسترسی اجباری (Mandatory Access Control-MAC)

در این مدل اشیاء تشکیل دهنده هر کدام از منابع سیستم کاملا مشخص می گردند و به هر شی برچسب امنیتی اختصاص داده می شود. هر کدام از این برچسب ها شامل اطلاعات زیر می باشند که بصورت هارد کد در برنامه مشخص می شوند :

☑ طبقه بندی اطلاعات بصورت بسیار سری، محرمانه و(classification) ...

☑ تعیین گروه هایی که می توانند به این شی دسترسی داشته باشند مثلا مدیران، مسئول پروژه و(categories) ...

به طور مشابه کاربران سیستم هم دسته بندی می شوند یعنی مشخص می گردد هر کاربر در چه طبقه ای از اطلاعات و در چه گروهی قرار دارد.بدین ترتیب هر زمان کاربری بخواهد به یک شی دسترسی داشته باشد، برچسب امنیتی شی را با مشخصات کاربری، مورد مطابقت قرار می دهند و نتیجه آن وضعیت دسترسی کاربر را مشخص می نماید. توجه داشته باشید که حتی اگر کاربری در طبقه اطلاعات سری قرار گیرد اما در گروهی باشد که در گاتالوگ شی نیامده است، مجوز دسترسی به او داده نمی شود. البته کاربری که در بالاترین سطح دسترسی قرار دارد ، مجوز دسترسی به اطلاعات سطوح پایین تر از خود را هم دارد. یعنی رابطه سطوح بصورت سلسه مراتبی می باشد.

در این روش امنیت تا حد بالایی لحاظ می شود اما کم هزینه هم نیست، چرا که اولا باید دقت زیادی صرف مشخص نمودن تمامی اشیاء سیستم و طبقه بندی آنها شود و ثانیا بعد از پیاده سازی، تمامی درخواست ها مبنی بر بروزرسانی کردن اشیاء و برچسب های آنها و یا تغییر موقعیت یک کاربر و سطح دسترسی آن، به مرکز مدیریتی ارسال می گردد که برای محیط های بزرگ و پویا بسیار وقت گیر خواهد. یکی دیگر از محدودیت های این مدل این است که کاربران نمی توانند داده های خود را به اشتراک بگذارند چرا که همه دسترسی ها از قبل و بصورت ایستا مشخص شده اند.

کنترل دسترسی اختیاری (Discretionary Access Control-DAC)

برخلاف کنترل دسترسی اجباری که در آن دسترسی به منابع توسط سیستم عامل و تحت کنترل مدیر سیستم صورت می گیرد، مدل کنترل دسترسی اختیاری به هرکاربر این اجازه را می دهد که نحوه دسترسی به داده های خود را تحت کنترل داشته باشد.

در این مدل دیگر از برچسب امنیتی استفاده نمی شود بلکه برای هر شی یک لیست کنترل دسترسی (Control List Access) ، تعریف می گردد که شامل فهرستی از کاربران و گروه هایی که به کاربر اجازه دسترسی می دهند و سطح دسترسی برای هر گروه ، می باشد.. یکی از مزایای این روش امکان به اشتراک گذاشتن دیتاها است، مثلا کاربر A می تواند اجازه فقط خواندن را در مورد فایل خود ، به کاربر B بدهد.

در این مدل تعریف لیست کنترل دسترسی می تواند بصورت متمرکز و یا توزیع شده باشد. در روش متمرکز، تنها مدیر سیستم می تواند لیست دسترسی ها را بروز رسانی نماید اما در مدل توزیع شده چنانچه مدیر مجوز تعریف و بروزرسانی لیست را به کاربری بدهد، او هم می تواند این تغییرات را اعمال نماید.

این روش برای سازمان های بزرگ و پویا به دلیل قابلیت انعطاف پذیری و صرفه جویی در وقت، مناسب می باشد ،البته از لحاظ امنیتی در سطح پایین تری نسبت به mac ، قرار دارد چرا که ممکن است حق دسترسی ای به کاربری داده شود در حالیکه مورد نیاز او نمی باشد.

کنترل دسترسی مبتنی بر نقش (Role Based Access Control-RBAC)

با توجه به عدم انعطاف پذیری مدل کنترل دسترسی اجباری و کنترل دسترسی اختیاری ، مفهوم امنیتی نسبتا جدیدی با عنوان کنترل دسترسی مبتنی بر نقش توسط موسسه ملی استاندارد و فناوری (NIST) مطرح گردید.

در روش کنترل دسترسی مبتنی بر نقش، حق دسترسی ها بستگی به عملیاتی دارد که کاربران در سازمان می توانند انجام دهند. در این مدل مجوز ها به نقش های تعریف شده اختصاص داده می شوند و سپس نقش هر کاربر در سازمان مشخص می گردد. به عنوان مثال کاربر حسابدار یک شرکت، نقش حسابداری به او انتصاب داده می شود از این طریق کاربر می تواند از مجوزهای تعیین شده برای نقش حسابدار ، استفاده نماید .بدین ترتیب اگر شرکت دارای چند حسابدار هم باشد، همه آنها دقیقا حق دسترسی های یکسانی خواهند داشت، نه بیشتر و نه کمتر.

کنترل کاربران در این مدل به سادگی امکان پذیر است، چرا که می توان به کاربران تنها با انتصاب نقش جدید و یا انتقال به نقش دیگر، حق دسترسی های جدید داد. از طرفی با اختصاص دادن یک مجوز جدید به یک نقش و یا گرفتن مجوزی از یک نقش، تمامی کاربرانی که آن نقش به آنها انتصاب داده شده است، موقعیت جدیدی در مورد حق دسترسی ها پیدا می کنند.

اجزاء تشکیل دهنده این مدل عبارتند از :

- آبجکت : (object) موجودیتی که حاوی اطلاعاتی باشد که نیاز به تعیین دسترسی (محافظت) دارند.
- عمل : (operation) مجموعه عملیاتی که میتوان بر روی یک آبجکت انجام پذیرد و نیاز به تعیین دسترسی (محافظت) دارد.
- مجوز : (permission) بررسی امکان انجام عمل بر روی یک آبجکت و دادن اجازه انجام آن.
- نقش / جایگاه : (role) بیانگر موقعیت شغلی در قالب چهارچوب سازمانی است و توضیحی در رابطه با اختیارات و مسئولیت ها در این موقعیت.
- کاربر : (user) شخصی است که مجاز به استفاده از قسمت‌هایی از نرم‌افزار می‌باشد. این شخص به جز انسان می‌تواندیک قطعه نرم‌افزاری هم باشد.

- جلسه : (session) مشخص می‌کند که کاربر با کدام(یک یا چند) از نقشهای خود در حال فعالیت در سیستم می‌باشد. هر کاربر می تواند دارای چندین session باشد وی هر session تنها به یک کاربر اختصاص داده می شود.
- تفکیک وظائف : تفکیک وظائف برای جلوگیری از ایجاد تضاد بین قوانین حاکم در یک سازمان، است. ایجاد تضاد بین قوانین تعریف شده، ممکن است در اثر انتصاب چند مسئولیت به یک نفر و یا فعال شدن یک نفر با چند نقش بصورت همزمان، بوجود آید. تفکیک وظائف به دو صورت امکان پذیر می باشد:
  - ایستا:(SSD) چنانچه مسئولیت های a و b هر کدام عملیاتی را انجام دهند که انتصاب آنها به یک نفر سبب شود قوانین امنیتی سازمان خدچه دار شود، با انتصاب مسئولیت a به یک نقش دیگر نمی توان مسئولیت b را به او اختصاص داد و بالعکس.
  - پویا:(DSD) چنانچه نقش های a و b هرکدام دارای مسئولیت هایی باشند که انجام دادن آنها بصورت همزمان سبب شود قوانین امنیتی سازمان خدچه دار شود، می توان هر دو نقش را به یک کاربر اختصاص داد اما در صورتیکه کاربر با نقش a فعال بود، دیگر نمی تواند بصورت همزمان و با یک session با نقش b هم فعال باشد.

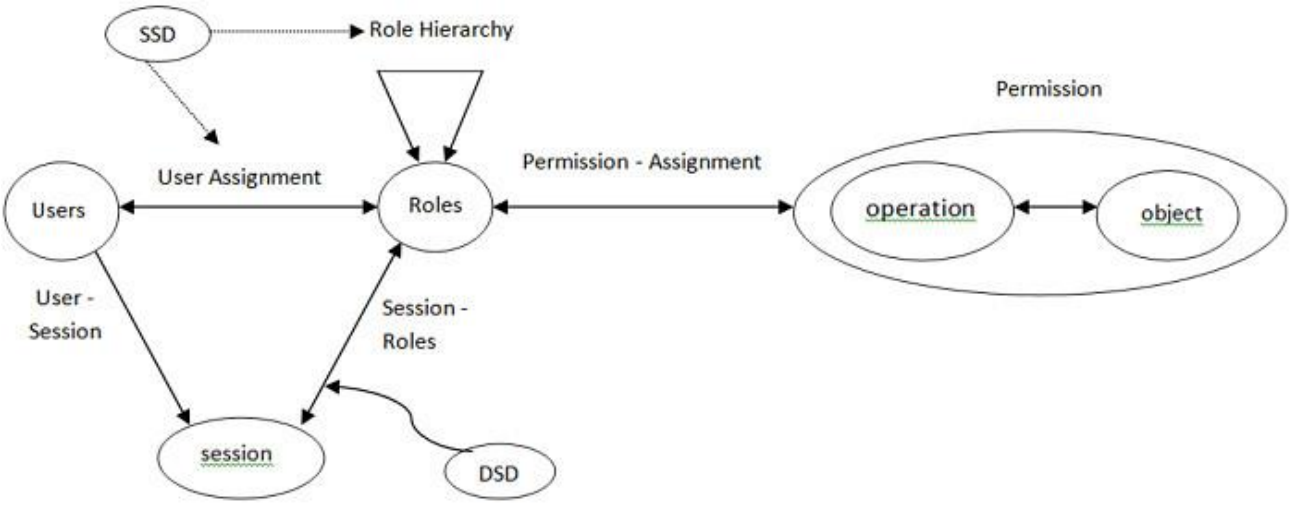
قوانین پایه ای حاکم بر سیستم مبتنی بر نقش:

1- Role assignment : یک کاربر در صورتی مجوز انجام عملی را در سیستم دارد که نقشی(role) به آن انتصاب داده شده باشد.

2- Role authorization :نقشی که کاربر با آن فعالی می شود، باید حتما مورد تایید سیستم قرار گیرد. این قانون به همراه قانون اول، تضمین می نماید که هر کاربر تنها می تواند در نقش هایی فعال شود که مجوز آنها را دارد.

3- Permission authorization : یک کاربر تنها می تواند حق دسترسی هایی را داشته باشد که براینقشی که با آن فعال است، تایید شده باشد. این قانون به همراه دو قانون قبلی، تضمین می نماید که کاربران تنها می توانند حق دسترسی هایی را داشته باشند که برای آنها مجاز است.

نمای کلی از RBAC بصورت زیر می باشد:



کنترل دسترسی مبتنی بر قوانین (Rule Based Access Control-RBAC)

در ابتدا لازم به ذکر است به عبارت مخفف در نظر گرفته شده برای کنترل دسترسی مبتنی بر قوانین اشاره نماییم که دقیقا شبیه به مخفف مدل کنترل دسترسی مبتنی بر نقش است (RBAC).

در این مدل، اجازه دسترسی یا عدم صدور مجوز برای دسترسی به اشیاء تعریف شده ی منابع سیستم، بر اساس یک سری از قوانین که توسط مدیر تهیه شده است، مورد بررسی قرار می گیرد. همانند روش کنترل دسترسی اختیاری، در این روش هم برای هر شی لیستی (ACL) تهیه می گردد که در آن قوانین لازم برای داشتن حق دسترسی مطرح می گردد.

بروز رسانی و تغییر این قوانین شبیه به مکانیزم مطرح شده در مدل کنترل دسترسی اجباری است، یعنی امکان تغییر قوانین و بروز رسانی کردن لیست توسط کاربران وجود ندارد و همه مجوز ها صرفا توسط مدیر سیستم کنترل می شود. به عنوان مثال می توان کاربر یا گروهی از کاربران را در نظر گرفت که تنها در روزهای خاصی از هفته و در ساعات مشخصی می توانند به شبکه متصل شوند.

آسیب پذیری های امنیتی درپایگاه داده ها

۱ -عدم موفقیت در استقرار

شایع ترین علت آسیب پذیری پایگاه های داده عدم توجه کافی به استقرار آن است.

مطمئناً پایگاه های داده اغلب از لحاظ عمل کردی مورد آزمون قرار می گیرند تا این اطمینان حاصل شود که عملیات اصلی فراخوانی در برنامه های کاربردی به خوبی انجام می گیرد. درواقع در اکثر آزمون های پیش از استقرار این مسأله بررسی می شود که یک پایگاه داده کاری را که باید، به خوبی

انجام دهد و خیلی کم پیش می آید که بررسی کنیم که پایگاه مذکور کارهایی را که نباید نیز انجام ندهد.

هر پایگاه داده باید فهرست طولانی از آزمون ها را پیش از استقرار بگذراند. این فهرست تنها جنبه ی کوچکی از پایگاه داده را پوشش می دهد که اغلب مستقیماً به شیوه های نفوذی رایجی مربوط می شود که مورد استفاده ی بیشتر مهاجمان است. هر بستر پایگاه داده ی رابطه ای (مانند اوراکل، اس کیو ال سرور، مای اس کیو ال، دی بی ۲ و سای بِیس) بلافاصله پس از نصب ناامن است و تا زمانی که به تعمیر و اصلاح آن نپردازید، همان طور خواهد ماند.

فهرستی از کارهایی که مدیران پایگاه داده باید پیش از استقرار پایگاه داده به دنبال آن باشند در اینجا ذکر می شود:

ویژگی هایی که به طور عمومی در دسترس هستند. به این معنا که برای دسترسی به آن ها وارد کردن اطلاعات محرمانه نیاز نیست.

تنظیمات پیکربندی پیش فرض که راه های متعددی را برای نفوذ مهاجمان می گشاید.

گذرواژه های پیش فرض که غلبه بر پایگاه داده را برای مهاجمان آسان تر می کند.

حساب های کاربری عمومی که ابزاری را برای تشخیص هویت کاربر ارائه نمی کنند و تشخیص شخص مهاجم به پایگاه داده را دشوارتر می سازند.

مجوزهای پرونده که اجازه ی بررسی پرونده های خام پایگاه داده را به کاربران می دهد.

باید بدانید که لازم نیست یک کارشناس حرفه ای پایگاه داده باشید تا بتوانید این مشکلات را برطرف کنید. بیشتر تولید کنندگان پایگاه داده ابزار لازم برای تنظیمات امنیتی اساسی را در اختیار شرکت ها قرار می دهد تا تنظیمات ضعیف پیکربندی را شناسایی کنند. برای این کار ایجاد یک سند از شیوه های پیکربندی مناسب در هر پایگاه داده و هر بازبینی از پایگاه داده، ایده ی خوبی است.

۲ -پایگاه های داده ی نقض شده

کرم رایانه ای Slammer توجه مدیران پایگاه داده را به مسئله ی آسیب پذیری بستر در سال ۲۰۰۳ جلب کرد و هزاران پایگاه داده را در عرض چند دقیقه دچار مشکل ساخت. این بدافزار از یک آسیب پذیری سرریز بافر بهره می گیرد و به مهاجم اجازه می دهد پایگاه داده ی آلوده را دچار توقف ناخواسته کند و کنترل آن را به دست بگیرد.

اِسلَمِر اولین مورد از چنین آسیب پذیری هایی است و درواقع برای اولین بار توسعه دهندگان را وادار کرد که وصله های امنیتی را ارائه کنند. اکنون دیگر آسیب پذیری هایی مثل تزریق فرمان و سرریز بافر مانند گذشته سرتیتر خبرهای امنیتی نیستند؛ بلکه مشکلات امنیتی کم تر شناخته می شوند و توسعه دهندگان نیز کم تر درباره ی زمان ارائه ی اصلاحیه ها پاسخ گو می باشند.

اما این بدان معنی نیست که نفوذها و آسیب پذیری های جدید دیگر وجود ندارند. بلکه برعکس! نفوذهای جدید نیز به طور منظم یافت می شوند و شاهد وصله های امنیتی حیاتی هستیم که چندین بار در سال برای آن ها ارائه می شود. با این حال شاید باورکردنی نباشد که بسیاری از شرکت ها این اصلاحیه های امنیتی را اعمال نمی کنند و سامانه ی پایگاه داده ی خود را در برابر حملات هم چنان آسیب پذیر باقی می گذارند. دلایلی که شرکت ها برای این کار ذکر می کنند، متفاوت است؛ اما چیزی که اغلب می شنویم این است که آن ها فاقد زمان و منابع کافی برای آزمودن وصله ها پیش از استقرار هستند و از این رو عمل کرد و ثبات وصله ها را بررسی نمی کنند.

قطعاً تست وصله ها وقت گیر است، اما اکثر وصله ها در بازه ی زمانی منظم و تقریباً هر ۳ ماه یک بار ارائه می شوند. یک آزمون رگرسیون جزئی برای تست عمل کرد زیاد هم طول نمی کشد. علاوه بر این ابزارهای تست نیز به گونه ای طراحی شده اند که فرآیند تست را خودکار کرده اند. بنابراین اطمینان پیدا کنید که برنامه های کاربردیتان را دچار مشکل نمی کنید.

توصیه ی کارشناسان در این مورد برای ایمن نگاه داشتن پایگاه داده ساده و غیرقابل مذاکره است: پایگاه های داده ی خود را وصله کنید!

۳ -اطلاعات افشا شده

برخی از مدیران پایگاه داده امنیت شبکه را به کل فراموش می کنند. طرز فکر رایج این است که پایگاه های داده در) back office شبکه ای که از اینترنت جدا شده است) هستند. از این رو نیازی نیست که ارتباطات داده ای مربوط به پایگاه داده رمزنگاری شود. چیزی که این کارشناسان فن آوری اطلاعات فراموش کرده اند یا بدان توجه ندارند، واسط شبکه ای پایگاه داده آن هاست. فراموش نکنید که ثبت ترافیک شبکه و تجزیه اطلاعات جذاب ناشی از چندین اتصال کاربر به پایگاه داده (یعنی اطلاعاتی که به پایگاه داده وارد می شود یا از آن خارج می گردد)، امر بدیهی و ساده ای برای مهاجمان به شمار می آید.

در همه ی موارد شما باید Transport Layer Security را فعال سازید .SSL دارای تأثیر بسیار کمی بر عمل کرد شبکه است و از شنود اطلاعاتِ در حال تبادل توسط اشخاص مهاجم پیشگیری می کند.

اکثر بسترهای رابطه ای از ارتباطات SSL یا TLS پشتیبانی می کنند و این ویژگی را در بسته بندی اولیه ی پایگاه داده قرار داده اند که از طریق تغییر کوچکی در پیکربندی حاصل می شود.

برای بسترهایی که فاقد ویژگی رمزنگاری ارتباطات هستند، باید خود گزینه ی شخص ثالثی را اضافه کنید. بسیاری از این دست موارد در انجمن های متن باز موجود است.

توجه به دیگر تنظیمات شبکه در پایگاه داده نیز گامی ضروری است. به عنوان مثال می توانید محدودیت هایی را قرار دهید که کدام کارگزار به پایگاه داده متصل شود و یا آدرس های آی پی خاصی را از بسترهای قابل اعتماد فهرست کنید تا مهاجم نتواند اتصالات موردی۲ به پایگاه داده ایجاد کند. برخی از پایگاه های داده اتصال پرس و جویی بجز SQL را ارائه می دهند مانند FTP و .XML در صورتی که در پایگاه داده ی خود بدان نیاز ندارید، حتماً آن ها را غیرفعال کنید.

۴ -پرونده های پشتیبان سرقت شده

همان طور که مهاجمان به اطلاعات نفوذ می کنند، کارکنان داخلی نیز احتمال دارد که اقدام به سرقت پرونده های بایگانی کنند؛ به ویژه محتوای پایگاه های داده. با وجود اینکه این روزها که حملات بزرگی علیه وب گاه ها صورت می گیرد، سرقت و گم شدن پرونده های پشتیبان کم تر عناوین خبری را به خود اختصاص می دهد، اما همچنان خطر این گونه حوادث بسیاری از شرکت ها را تهدید می کند. به منظور کاهش خطر، رمزنگاری اطلاعات باید به بخش اساسی در فرآیند بایگانی تبدیل شود. اما اغلب چنین اتفاقی نمی افتد؛ چرا که استقرار اولیه به کندی صورت می گیرد و فاقد مدیریت کلیدی خارجی است. با این حال اکنون محصولات و سرویس هایی وجود دارند که این فرآیند را ساده تر می کنند.

دو راه وجود دارد تا مطمئن شوید که پرونده های بایگانی رمز شده اند. یکی رمزنگاری شفاف پایگاه داده است و دیگری خرید سیستم های بایگانی که قابلیت رمزنگاری خودکار را ارائه می کنند.

به شرط آن که سامانه ی بایگانی شما پرونده ها را از فایل سیستم جمع آوری کند، رمزنگاری شفاف پایگاه داده گزینه ی جالبی است. سامانه های شفاف اطلاعات را به محض نوشته شدن در دیسک رمز می کنند و بلوک های پرونده را هنگامی که در پایگاه داده خوانده می شوند، رمزگشای می نماید. این یعنی می توانید بدون تغییر در ساختار پایگاه داده و یا پرس و جوها رمزنگاری را در آن ایجاد کنید و تأثیری بر عمل کرد پایگاه داده نیز ندارد. این فن آوری مزیت دیگری را نیز به همراه دارد و آن عبارت است از اینکه مدیران پایگاه داده نیز حتی با دسترسی ادمین به کارگزار قادر نیستند پرونده های پایگاه داده را بخوانند.

گزینه ی دیگر تعبیه کردن رمزنگاری در روال بایگانی است. این کار با خرید رسانه ی بایگانی انجام می شود که اطلاعات را پیش از بایگانی رمزنگاری می کند. این فرآیند همچنین از طریق دستگاه رمزنگاری پروکسی نیز قابل انجام است که اطلاعات را پس از ترک پایگاه داده و پیش از ورود به سیستم بایگانی رمز می کند.

۵ -سوء استفاده از ویژگی های پایگاه داده

در طول ۳ سال گذشته هر نفوذ به پایگاه داده بر اساس سو ء استفاده از ویژگی استانداردی در پایگاه داده رخ داده است. مهاجم معمولاً از طریق اطلاعات محرمانه ی ورودی به پایگاه داده دسترسی می یابد و سپس از برخی سرویس های پایگاه داده استفاده می کند تا قابلیت های مدیریتی را برای وی ایجاد کنند و سرویس معتبر مذکور را وادار می کند که کد دلخواهش را اجرا کند. برخی از این حملات پیچیده هستند اما در بسیاری از موارد یک کاربر چیزی کشف می کند که می تواند با آن محدودیت خاصی را دور بزند. از این رو نفوذهای انجام شده به پایگاه داده لزوماً توسط نفوذگران قدرتمند انجام نمی شود. بلکه اغلب توسط کاربران معتبری انجام می شود که از خطای ساده ای سوء استفاده می کنند که ناشی از شیوه ی استفاده ی نادرست برنامه ی کاربردی از پایگاه داده به وجود آمده است.

اکثر مدیران پایگاه داده به طور کامل نمی دانند که ویژگی های آن چه طور کار می کند. البته این یک انتقاد نیست؛ بلکه واقعیتی است که ناشی از پیچیدگی بسترهای رابطه ای با هزاران ویژگی است. مدیران پایگاه داده معمولاً سعی نمی کنند اجرای کد باینری و مجوزهایی را که توسط سرویس های مدیریت داخلی استفاده می شود، درک کنند. با این حال مهاجمان زحمت زیادی بابت درک این ضعف های بالقوه متحمل می شوند. اگر آن ها بتوانند کنترل آن ویژگی یا فرآیند را با مجوزهای لازم به دست آورند می توانند هر کاری که مایلند، انجام دهند.

مقابله با سوء استفاده از ویژگی ها کار ساده ای نیست. بهترین حالت این است که تولید کننده ی پایگاه داده از مشکل موجود باخبر می شود و کد خود را اصلاح می کند و وصله ای برای آن عرضه می کند. اما در واقعیت به ندرت این اتفاق می افتد. بسیاری از مشکلات شناخته شده هستند اما توسط سازندگان اصلاح نمی شوند. گاهی اوقات اعمال وصله بسیار دشوار بوده و نیاز به تغییر در معماری و کدنویسی مجدد سرویس ها دارد؛ از این رو عرضه ی اصلاحیه سال ها به طول می انجامد. در دیگر موارد یک آسیب پذیری خاص سال های سال و پیش از آن که یک کاربر گرفتار آن شود، وجود دارد: یعنی تولید کننده زمانی از آسیب پذیری مطلع می شود که یکی از مشتریانش تحت تأثیر آن قرار گرفته باشد. این آسیب پذیری روز صفرم خوانده می شود؛ چرا که تولید کننده هیچ زمانی برای وصله ی آسیب پذیری پیش از سوء استفاده از آن ندارد.

در اینجا می توانید سوء استفاده از ویژگی ها را با حذف هر آنچه بدان نیاز ندارید، کم کنید. پایگاه های داده ی رابطه ای در ۳۰ سال گذشته بسیار رشد کرده اند و دارای هزاران ویژگی و مولفه شده اند. ممکن است شما تنها از نیمی از آن ها استفاده کنید. از این رو برای کاهش خطر باید ویژگی هایی که از آن ها استفاده نمی کنید را غیرفعال سازید. اما این کار ممکن است کمی دشوارتر از آن باشد که به نظر می رسد. زیرا ممکن است ندانید چه ویژگی هایی در شرکت شما استفاده می شود و کدام موارد بلااستفاده اند. همچنین تعامل پیچیده ای بین قابلیت های پایگاه داده وجود دارد. به عنوان مثال ویژگی Aممکن است برای شرکت شما نیاز نباشد، اما اگر ویژگی B وجود داشته باشد و به A متکی باشد، شما نمی توانید A را حذف کنید. از این رو توصیه می کنیم یکی از این دو شیوه را به کار گیرید: هر ویژگی که بدان نیاز ندارید را مستند کنید و اسکریپتی برای حذف آن ها ایجاد کنید. همچنین می توانید اسکریپتی برای نصب پایگاه های داده ای بنویسید که نیازهای اساسی را برآورده می کند و با گذشت زمان تغییراتی را در آن اعمال کنید. بسیاری از شرکت های بزرگ تنها نسخه های خاصی از پایگاه داده را تأیید می کنند؛ از این رو می توانید این نسخه را ذخیره کنید و وصله ها را به صورت داخلی اعمال کنید.

۶ -عدم تفکیک

اساساً تفکیک توان ها و وظایف شیوه ای است که ارتکاب جرم و تقلب را برای افراد دشوارتر می سازد و تشخیص آن را در صورت رخ دادن آسان تر می کند. این شیوه همچنین می تواند ابزار موثری برای این باشد که مهاجم کنترل کامل پایگاه داده را به دست گیرد. در صورتی که وظایف مدیریت را به چندین نقش تفکیک کنید که توسط چندین حساب کاربری ادمین در پایگاه داده تعریف شده اند، در صورتی که یک حساب کاربری در معرض خطر قرار گیرد، کنترل کامل سامانه از دست نمی رود. به عبارتی این کار یعنی یک حساب کاربری مدیر در پایگاه داده برای پشتیبان گیری، یک حساب کاربری برای مدیریت کاربران، یکی برای افزودن و حذف کردن ویژگی ها، و ... تعریف شود. در صورت افشای گذرواژه ی مدیر در این مدل، میزان خسارت وارده کم تر است.

۷ -بازی لی لی که اشاره به انجام مرحله به مرحله کار دارد.

تنها در صورتی که تزریق SQL و یا سوء استفاده از سرریز بافر صورت گیرد، نفوذگران می توانند دسترسی مستقیم به پایگاه داده پیدا کنند. در سایر موارد آن ها ضعفی را در ساختار پایگاه داده پیدا کرده و از آن در سایر حملات استفاده می کنند تا بتوانند به خودِ پایگاه دست یابند. به عنوان مثال در نفوذ صورت گرفته به سامانه های پرداختی Heartland مهاجمان ابتدا به گروه حساب داری دست یافتند که این اتفاق منجر به دسترسی به سامانه های پردازش کارت های اعتباری شد.

به همین دلیل است که توصیه می کنیم کارگزارها، برنامه های کاربری(مانند پایگاه های داده) و شبکه ها حساب های کاربری، گذرواژه ها و کاربران مجزایی داشته باشند.

در شرکت های کوچک و متوسط در حقیقت تیمی از مدیران پایگاه داده وجود ندارد؛ بلکه یک شخص نقش چندین مدیر را در بخش های پایگاه داده و شبکه ایفا می کند. در حالی که کارشناسان به شدت توصیه می کنند که سامانه ها نیز جداسازی شوند.

۸ -تزریقSQL

حدود یک دهه است که تزریق SQL در صدر تهدیدات پایگاه داده قرار دارد. اما همچنان به عنوان یک مشکل بحرانی وجود دارد.

چیزی که بیشتر در تزریق SQL نگران کننده می باشد این است که این حمله علیه هر پایگاه داده ای می تواند صورت گیرد؛ زیرا نویسندگان برنامه ی کاربردی موفق به پاک کردن متغیرهای ورودی نمی شوند. از این رو در بسیاری از موارد مدیر پایگاه داده نمی تواند کاری در مقابل آن انجام دهد.

یعنی این توسعه دهنده ی برنامه است که عامل ایجاد این مشکل است و این مدیران پایگاه داده هستند که باید این مشکل را رفع کنند. دیگر آن زمان که پرس و جوهای SQL به صورت رویه های ذخیره سازی شده پیاده می شد و در آن ها این اطمینان حاصل می گردید که متغیرهای ورودی از نوع صحیحی هستند، گذشته است. بنابراین مزایای ذاتی پایگاه داده دیگر نمی تواند اهرمی برای خنثی کردن این مشکل باشد. تنها دو راه وجود دارد که مدیر بتواند از پایگاه داده ی خود محافظت کنند. اولین و رایج ترین شیوه این است که پایگاه های داده ای وب را توسط یک دیواره ی آتش ویژه ی برنامه های تحت وب محافظت کنیم. این بسترها همه ی درخواست های برنامه های کاربردی وبی را که به دنبال حملات شناخته شده ای هستند و یا سرنخی از حمله در آن ها یافت می شود، فیلتر می کنند. روش دیگر تمرکز بیشتر است. بدین معنی که از پویش فعالیت های پایگاه داده استفاده کنیم. این محصولات بر زبان SQL تمرکز دارند و نه تنها شیوه های شناخته شده ی حمله را به کار می برند بلکه نمایه های رفتاری را ترکیب می کنند و تجزیه لغوی زبان SQL را انجام می دهند و پرس و جوها را در فهرست سفید و سیاه قرار می دهند. این تمرکز بیشتر بر SQL کنترل بیشتری را بر پرس و جوهای انجام شده از پایگاه داده ارائه می کند. آخرین ترفند یک مدیر تشویق تیم برنامه نویس به آزمودن همه ی متغیرهای ورودی در تزریق SQL در حین فرآیند توسعه است.

۹ -مدیریت ضعیف کلیدها

امروزه زمانی که شرکت ها را از لحاظ امنیت پایگاه داده بررسی می کنیم به کلیدهای رمزنگاری در دیسک می رسیم. ظاهراً بسیاری از مدیران درک نمی کنند که سامانه های مدیریت کلید است که این کلیدها را ایمن نگاه می دارد و آن ها توجهی به این مسأله ندارند که کلیدها بدون حفاظت در یک پرونده ی آسیب پذیر قرار گرفته اند. این مدیران پایگاه داده عقیده دارند که کلیدها باید در دیسک ذخیره شود تا در صورت شروع کار مجدد پایگاه داده مثلاً به سبب قطعی برق، موجود باشند. در غیر این صورت به اعتقاد این افراد این کلیدها موجود نخواهد بود و پایگاه داده به حالت عادی باز نخواهد گشت. در صورتی که این عقیده غلط است و محصولات مدیریت کلید امنیت کلیدها و قابلیت شروع مجدد آن ها را تأمین می کنند.

اگر کلیدها بدون حفاظت رها شوند، اطلاعات رمزنگاری شده عملاً بی ارزش است. و در صورتی که فکر می کنید مهاجمان نمی توانند کلیدها را بیابند، باز هم اشتباه فکر می کنید. چرا که آن ها اسکریپت های خودکاری دارند که به دنبال پرونده هایی می گردد که حاوی چنین عباراتی است «... BEGIN PGP KEY HERE».

بنابراین توصیه می شود که به دنبال سامانه های مدیریت کلیدی باشید که از واسط پایگاه داده ی شما و نوع کلیدهایی که استفاده می کنید، پشتیبانی کند. بیشتر پایگاه های داده ی تجاری سامانه های مدیریت کلیدی را با کیفیت های متفاوتی ارائه می کنند.

۱۰ -ناسازگاری

همه ی مواردی که در بالا بدان اشاره شد بر سطوحی تمرکز داشتند که فن آوری های پایگاه داده مورد سوء استفاده قرار می گیرد. با این حال موضوع رایج در میان همه ی آن ها نیاز به سازگاری است. نیاز به سازگاری مشکل فن آوری در پایگاه داده نیست بلکه یک فرآیند مدیریتی است. استقرار ایمن معمولاً به ۲ چیز بستگی دارد: دانستن اینکه کدام جنبه های پایگاه داده معمولاً هدف حمله قرار می گیرد و بررسی اینکه آیا به خوبی این زمینه ها را از طریق مدیریت پیکربندی پوشش داده اید یا خیر.

همه ی این ها به این معنا نیست که رسیدن به سازگاری آسان است. مدیران پایگاه داده هر کدام با سطح درک متفاوتی از امنیت و پرداختن به جزییات وارد سیستم شده و روزی هم می روند. امروزه در محیط های ابری و مجازی توسعه ی پایگاه های داده ی جدید آسانتر شده است. زمانی که این دو امر را ترکیب کنید، پایگاه داده های جدید و ناامنی در محیط شما ظاهر می شوند و این پایگاه های داده ای موجود فاقد تنظیمات امنیتی تأیید شده هستند.

بهتر است که با تنظیمات ناسازگاری از طریق مستندسازی و اتوماسیون مقابله کنیم. حتماً اطمینان پیدا کنید که تنظیمات صحیح برای پایگاه داده مستند شده است و مدیر جدید این راهنما را مطالعه کرده و درک می کند. شما قادرید بسیاری از این دستورالعمل ها را با اعمال سیاست هایی در ابزارهای پایگاه داده اتوماسیون سازید. این ابزار شبکه ی شما را به منظور پایگاه داده ی جدید جستجو می کند و بررسی می نماید که تنظیمات پیکربندی برای محیط شما مناسب است یا خیر. در پایان فرآیند پویش طی یک گزارش، هر گونه ناسازگاری که کشف شده باشد را مستند می کند.

نتیجه گیری

بسیاری از اقدامات پیش گیرانه ی امنیتی و شیوه های تشخیص رفتار ناهنجار چیزی بیش از تمرین عمل کرد خود پایگاه داده نیست. مثلاً تأیید اینکه یک مدیر پایگاه داده وظایف محوله را به طور کامل به انجام رسانده و یا تفکیک وظایف در میان کاربران به خوبی انجام شده است.

مقابله با بسیاری از این مسائل زمانی که می دانید به دنبال چه هستید، آسان است. صرف زمان کافی برای تشخیص اینکه شیوه ی صحیح پیکربندی تنظیمات امنیتی پایگاه داده باید چگونه باشد و تأیید اینکه سامانه ی شما این استانداردها را رعایت می کند(با استفاده از اسکریپت های خودکار و سایر ابزار) از ضروریات است. اعتبارسنجی امنیت از پشتیبان گیری چندان سخت تر نیست بلکه نیازمند این است که زمان بیشتری صرف کنید و یاد بگیرید که چه چیزی نیاز است و تا آن جا که می توانید کارها را اتوماسیون کنید.