اصول و مبانی امنیت پایگاه داده

کاردانی فنی پایگاه داده

در جهان کنونی، سیستم‌های مدیریت پایگاه داده (DBMS) به عنوان یک بخش جدایی‌ناپذیر در سازمان‌ها و شرکت‌های مختلف مورد استفاده قرار می‌گیرند. به همین دلیل، حفظ امنیت پایگاه داده (Database Security)یکی از مهم‌ترین موضوعاتی به حساب می‌آید که لازم است کسب‌وکارها به آن توجه ویژه داشته باشند. در این مقاله، یک راهنمای جامع و کاربردی در مورد چیستی امنیت پایگاه داده و روش‌های مختلف برقراری امنیت بانک‌های اطلاعاتی ارائه شده است تا بدین طریق، نقش آن بیش از پیش برای همگان روشن شود .

امنیت پایگاه داده چیست ؟

امنیت پایگاه داده به اقدامات مختلفی اطلاق می‌شود که سازمان‌ها از آن‌ها برای اطمینان از حفظ شدن پایگاه‌های اطلاعاتی خود در برابر تهدیدات داخلی و خارجی استفاده می‌کنند. منظور از امنیت پایگاه داده، محافظت از خود پایگاه داده، داده‌های موجود در آن، سیستم مدیریت پایگاه داده مربوطه و برنامه‌های کاربردی مختلفی است که دسترسی به آن‌ها در ارتباط با بانک اطلاعاتی وجود دارد. سازمان‌ها باید پایگاه‌های اطلاعاتی را در برابر حملات عمدی گوناگون مانند تهدیدات امنیت شبکه و همچنین سو استفاده از داده‌ها و پایگاه‌های اطلاعاتی ایمن کنند.

در طول چند سال گذشته، میزان نقض (Breach) اطلاعات و قانون‌شکنی در این زمینه به طور قابل توجهی افزایش پیدا کرده است. علاوه بر آسیب قابل توجهی که این تهدیدها به شهرت و اعتبار یک شرکت وارد می‌کنند، مقررات و مجازات‌های مختلفی برای نقض داده‌ها وجود دارند و لازم است سازمان‌ها با چالش نقض اطلاعات مقابله

کنند. یکی از این موارد مقررات عمومی حفاظت از داده‌ها (GDPR) به حساب می‌آیند که غالباً بسیار پرهزینه هستند. با توجه به نکات مذکور، می‌توان با قاطعیت، امنیت پایگاه داده موثر را برای سازگاری، حفاظت از اعتبار سازمان‌ها و حفظ مشتریان آن‌ها به عنوان یک امر کلیدی در نظر گرفت.

تهدیدات احتمالی امنیت پایگاه داده چه هستند؟

خطرات احتمالی مختلفی برای امنیت پایگاه داده وجود دارند که برخی از پراهمیت‌ترین آن‌ها در ادامه فهرست شده‌اند:

- اولین و به طور بالقوه، خطرناک‌ترین تهدیدی که امنیت پایگاه داده را به خطر می‌اندازد، دسترسی غیرمجاز هکرها و دستکاری‌کنندگان به سیستم‌های امنیتی و ایجاد مخاطره در اطلاعات مهم کاربر خارج از پایگاه داده است. آن‌ها به نوبه خود می‌توانند یا در نهایت به پایگاه داده آسیب برسانند یا سوابق را به گونه‌ای دستکاری کنند تا بتوانند به اهداف شوم خود برسند.
- حملات مختلف از طریق نرم‌افزار، اسکریپت یا سایر سیستم‌های غیرقانونی بالقوه مضر که شامل استفاده از بدافزارها و ویروس‌ها می‌شوند. این مسئله به هکرها اجازه دسترسی غیرمجاز به سیستم‌های پایگاه داده را می‌دهد.
- ممکن است تمام تهدیدات فوق منجر به بروز سربار سیستم، عملکرد نادرست برنامه‌های مختلف و قطع دسترسی مدیر مجاز به سیستم شود.
- اگر فایل‌های آلوده حذف یا از سیستم سرور پاک نشوند، ممکن است منجر به بروز آسیب‌های فیزیکی مختلفی مانند داغ شدن بیش از حد یا حتی خرابی کامل در موارد شدید شوند.

- علاوه بر موارد فوق، خرابی داده‌ها می‌تواند در موارد نقض یا تهدید در کنترل‌های امنیتی مختلفی رخ دهد که در وهله اول برای جلوگیری از وقوع چنین حوادثی به وجود آمده‌اند.

به طور کلی، روش‌های متعددی وجود دارند که از طریق آن‌ها می‌توان امنیت پایگاه داده را به خطر انداخت یا هک و دستکاری کرد. این موارد همگی عواقب شدیدی را به دنبال دارند. برای اطمینان از اینکه چنین اتفاق‌هایی رخ ندهند، کنترل‌های مختلفی وجود دارند که در بخش‌های بعدی این مقاله به معرفی آن‌ها پرداخته شده است.

مفاهیم اصلی در امنیت پایگاه داده کدامند؟

به طور کلی، امنیت پایگاه داده سه مفهوم کلیدی را در بر می‌گیرد که در ادامه به آن‌ها پرداخته می‌شود:

محرمانگی در امنیت پایگاه داده چیست ؟

در مفاهیم امنیت پایگاه داده، «حفظ محرمانگی اطلاعات (Confidentiality) «به عنوان اولین معیار در نظر گرفته می‌شود. امکان ایجاد محرمانگی از طریق رمزنگاری داده‌های ذخیره شده در پایگاه داده امکان‌پذیر است. رمزنگاری یک روش یا فرآیندی است که در آن داده‌ها کدگذاری می‌شوند. این کدگذاری به گونه‌ای انجام می‌شود که تنها کاربران مجاز امکان خواندن داده‌ها را داشته باشند. به بیان دیگر، رمزنگاری یعنی داده‌های حساس برای کاربران غیرمجاز به صورت غیرقابل خواندن هستند. الگوریتم‌های رمزنگاری مختلفی مانند DES ، AESو Triple DESبرای برقراری و حفظ محرمانگی در پایگاه داده استفاده می‌شوند.

تمامیت در امنیت پایگاه داده به چه معناست؟

مفهوم تمامیت (Integrity) در امنیت پایگاه داده از طریق تنظیمات مربوط به کنترل‌های دسترسی کاربری (UAC)اعمال می‌شود. با استفاده از این مفهوم، به هر کاربر دسترسی به پایگاه داده تا سطح مورد نیاز داده

خواهد شد. به عنوان مثال، ممکن است به یک کارمند اجازه دیدن رکوردها و تغییر بخش‌هایی از اطلاعات، مثل جزییات شماره تماس داده شود، اما کارمند بخش منابع انسانی دسترسی‌های بیش‌تری داشته باشد. برای اطمینان از تمامیت پایگاه داده روش‌هایی وجود دارند که در ادامه به آن پرداخته می‌شود:

- پس از نصب پایگاه داده، باید رمز عبور تغییر داده شود. علاوه بر این، بررسی‌های دوره‌ای گوناگونی لازم است تا این اطمینان به وجود بیاید که رمز عبور در خطر قرار نگرفته است.
- باید آن دسته از حساب‌های کاربری که استفاده نمی‌شوند، قفل شوند. در شرایطی که یک حساب کاربری به طور قطعی هیچ‌گاه دوباره استفاده نخواهد شد، بهترین اقدام حذف آن است.
- لازم است سیاست‌های پیشرفته مختلفی برای رمزهای عبور قوی ایجاد شوند. یکی از ایده‌های کارامد در این خصوص، الزام در تغییر رمز عبور به صورت ماهانه است.
- بررسی نقش‌ها و تنظیم دسترسی‌ها بر اساس آن‌ها بسیار اهمیت دارد. در واقع، باید این اطمینان حاصل شود که کاربران تنها به مواردی دسترسی دارند که مجاز به استفاده از آن‌ها هستند. با وجود اینکه بررسی این موضوع برای پایگاه داده‌های بزرگ بسیار زمان‌بر است، اما اگر دسترسی‌ها به درستی تنظیم شوند، ورود یا دسترسی غیرمجاز به راحتی قابل بررسی خواهد بود.
- بررسی اینکه آیا کسب و کار مربوطه چندین ادمین پایگاه داده دارد یا خیر؛ در صورتی که پاسخ این سوال مثبت باشد، بهتر است وظایف میان این مدیران پایگاه داده تقسیم شوند.

دسترسی پذیری در امنیت بانک اطلاعاتی چیست ؟

در یک سیستم کارآمد، نباید پایگاه داده از کارافتادگی بازه‌ای داشته و نرخ دسترس پذیری (Availability) آن باید قابل قبول باشد. در واقع، برای جلوگیری از رخداد برنامه‌ریزی نشده چنین اتفاق‌هایی، می‌توان از اقدامات مختلفی استفاده کرد که در ادامه فهرست شده‌اند:

- محدود کردن میزان فضای ذخیره‌سازی برای کاربران در پایگاه داده
- ایجاد محدودیت در تعداد نشست‌های(Session) های (موازی قابل دسترسی برای هر کاربر پایگاه داده
- پشتیبانی‌گیری از داده‌ها به صورت دوره‌ای به منظور کسب قابلیت بازیابی داده در صورت بروز مشکلاتی در اپلیکیشن
- ایجاد ایمنی در پایگاه داده در برابر آسیب‌های امنیتی
- استفاده از پایگاه داده‌های خوشه‌ای با هدف افزایش دسترسی پذیری

مزیت‌های امنیت پایگاه داده کدامند؟

برقراری امنیت پایگاه داده یک اقدام ضروری در سازمان‌هایی است که دارای پایگاه‌های داده و سیستم‌های مدیریت پایگاه داده مرتبط با یکدیگر هستند. در این سازمان‌ها، اقدامات مربوط به برقراری امنیت پایگاه داده در کنار عناصر عملکردی برنامه‌های کاربردی این سازمان‌ها مورد استفاده قرار می‌گیرند. در حقیقت، با به کارگیری اقدامات احتیاطی راه‌اندازی شده در جهت افزایش امنیت پایگاه داده می‌توان جلوگیری از بسیاری از عواقب احتمالی جدی نقض امنیت را تسهیل کرد. در ادامه برخی از ویژگی‌های مفید اجرای عناصر امنیت پایگاه داده فهرست شده‌اند:

- می‌توان پایگاه‌های داده را در برابر نقض‌های امنیتی و فعالیت‌های هک، از جمله نفوذ فایروال (Firewall) (Intrusion)، انتشار ویروس و باج افزار (Ransomware) محافظت کرد. اعمال اقدامات مربوط به امنیت پایگاه داده در نهایت محافظت از اطلاعات حساس شرکت را تسهیل می‌کند. بنابراین، در مواقع مختلفی که به هیچ دلیلی نمی‌توان اطلاعات را با افراد خارجی به اشتراک گذاشت، افزایش امنیت پایگاه داده بسیار مفید است.
- امکان توقف حملاتی مانند فایل‌های مسری بدافزار و سایر موارد مخربی فراهم می‌شود که ممکن است برای سیستم‌های پایگاه داده ناامنی ایجاد کنند.
- ارائه حفاظت تضمین شده برای سیستم‌های سرور فراهم می‌شود. بنابراین، امکان محافظت از این سیستم‌های سرور در برابر هر گونه آسیب قابل توجهی که منجر به شکست در پردازش یا بازیابی داده بشوند، وجود دارد.
- امنیت پایگاه داده با تعهد کاربران پایگاه داده و متخصصان مدیریت از حوزه کسب و کار همراه است تا داده‌های ادراکی را دقیقاً برای استفاده مناسب از اطلاعات جمع‌آوری کنند.

- زمانی که امنیت پایگاه داده با سیاست‌ها و شرایط شرکت مطابقت داشته باشند، اپلیکیشن‌ها از خطر خراب شدن عاری خواهند بود. به این دلیل که علاوه بر بهبود عملکرد سازمان با مقرون به صرفه‌تر کردن هزینه‌ها، از سازمان محافظت می‌کنند.
- با وجود اینکه افزودن ویژگی‌های جدید به امنیت پایگاه داده سازمان مربوطه برای کسب‌وکار هزینه‌زا است، اما با کمک این رویکرد، اطمینان حاصل می‌شود که هزینه‌ها به جای ضرر به سرمایه‌گذاری تبدیل خواهند شد.

در این بخش به این سوال پاسخ داده شد که امنیت پایگاه داده چیست و استفاده از آن در سازمان‌ها و کسب و کارهای مختلف چه مزیت‌هایی دارد. اکنون در ادامه مقاله «امنیت پایگاه داده چیست»، مهم‌ترین کنترل‌های امنیتی مورد بررسی قرار می‌گیرند.

کنترل‌های امنیتی برای برقراری امنیت پایگاه داده

داده‌ها در حمل و نقل و کنترل دسترسی در امنیت پایگاه داده

به طور کلی، کنترل دسترسی (Access Control) داده‌ها در حمل و نقل، به سیستم امنیتی خاصی اطلاق می‌شود که با کمک آن، اطمینان لازم از فرآیند انتقال حاصل خواهد شد. به بیان ساده، با استفاده از این نوع کنترل امنیت پایگاه داده هیچکس نمی‌تواند داده‌ها را هنگام انتقال بین سرورهای مختلف یا پیکربندی شبکه‌ها بخواند یا تفسیر کند.

هدف اصلی در این نوع از امنیت پایگاه داده محدود کردن هرگونه گره (Node) بالقوه مربوط به رخنه یا دسترسی غیرمجاز به سیستم‌های سرور در هر زمانی است. بنابراین، این تنظیمات داده‌ها به عنوان کنترل دسترسی نیز شناخته می‌شوند. هر گره داده مشخصی که از سیستم سرور ایمن خارج و وارد آن می‌شود، کاملاً رمزنگاری شده و غیرقابل خواندن است. مگر اینکه به طور امن در پایگاه داده سیستم ایمن سپرده شود یا به کاربر درخواست کننده آن دیتا، نمایش داده شود.

برخی از سازمان‌ها یا شرکت‌ها با این موضوع موافق نیستند و بر غیرضروری بودن اجرای این مورد تاکید دارند. با این وجود، در عمل این اقدام یکی از اصلی‌ترین گام‌هایی است که در جهت افزایش امنیت پایگاه داده کاربرد دارد. در طول چند سال اخیر، این مفاهیم در بهترین دوره‌های امنیت پایگاه داده متعددی نیز تدریس شده‌اند. این دوره‌ها برای پرسنل و متخصصانی اهمیت دارند که به عنوان کارشناس امنیت پایگاه داده و پیکربندی داده‌ها به دنبال مشاغل پرتقاضا هستند.

احراز هویت در کنترل‌های امنیت در پایگاه داده

احراز هویت (Authentication) به عنوان مورد بعدی از انواع امنیت پایگاه داده مطرح می‌شود و پس از تکمیل داده‌ها، لازم است این موضوع در پروتکل حمل و نقل اعمال شود. این پروتکل امنیتی دارای لایه‌های مختلفی در درون خود است. به طور کلی، احراز هویت راهی است که از طریق آن تأیید می‌شود آیا کاربر همان شخصی است که می‌گوید یا خیر؟

به عبارت ساده‌تر، Authenticationبه معنی احراز هویت درخواست یا کوئری ارسال شده توسط پرسنل مجاز یا کاربر اختصاصی است. به منظور عملی کردن احراز هویت، می‌توان از روش‌های مختلفی استفاده کرد. به عنوان مثال، استفاده از روش احراز هویت چند عاملی (Multi-Factor) که در آن لایه‌های امنیتی مختلف به طور ترکیبی اضافه می‌شوند. این فرآیند منجر به احراز هویت یک کاربر خاص و موفقیت او در دسترسی می‌شود. در

صورتی که فرآیند احراز هویت به عنوان یک عمل کاربردی در مورد پیکربندی و امنیت پایگاه داده اعمال نشود، هر کسی، حتی هکرهای غیرقانونی، به راحتی به سرورهای پایگاه داده دسترسی خواهند داشت و باعث خرابی و به مخاطره انداختن امنیت پایگاه داده می‌شوند. به منظور اعطای دسترسی و احراز هویت موثر کاربر، می‌توان از مواردی مانند احراز هویت دو مرحله‌ای (Two-Factor) و احراز هویت از طریق نام کاربری و رمز عبور استفاده کرد.

صدور مجوز در کنترل‌ها امنیت پایگاه داده

مرحله بعدی در این فرآیند و نوع سوم حفظ امنیت پایگاه داده ، صدور مجوز (Authorization) است. با به کارگیری این لایه امنیتی، مشخص می‌شود که کاربر اختصاصی (Dedicated) دقیقاً به چه عناصری دسترسی دارد. در صورت لزوم، می‌توان محدودیت‌هایی را برای یک کاربر مشخص اعمال کرد و دسترسی او تنها به یک نمای کلی از سیستم‌ها محدود شود. به عنوان مثال، ممکن است یک کاربر به محتوای کلی وب سایت دسترسی داشته باشد، اما اطلاعات محرمانه پراهمیتی مانند اطلاعات شخصی یا مالی سایر کاربران برای او یا هر کاربر Guestیا معمولی دیگری محدود شوند.

این مرحله از امنیت پایگاه داده از همه آن‌ها مهم‌تر است. چراکه به واسطه آن، اطمینان لازم برای برقراری امنیت پایگاه داده حاصل می‌شود. در حقیقت، با استفاده از Authorization هیچ‌کس نمی‌تواند به مناطق ناشناخته سرک بکشد یا بخش‌هایی را کاوش کند که قرار نیست مورد توجه آن‌ها قرار بگیرند. می‌توان سطح مجوز اختصاص داده شده به یک کاربر خاص را برای یک سازمان یا اپلیکیشن خاص، پیکربندی یا سفارشی‌سازی (Customized)کرد.

داده‌ها در حالت استراحت

پس از به اشتراک گذاشتن یا در دسترس قرار گرفتن داده‌ها توسط کاربر، این داده‌ها در سرور باقی می‌مانند. این شرایط با نام «داده‌ها در حالت استراحت (Data At Rest) «در نظر گرفته می‌شوند. لازم به ذکر است که حتی پس از خاموش شدن سرور، داده‌ها همچنان باقی می‌مانند. برای این وضعیت، فناوری‌های رمزنگاری منحصر به فردی به کار گرفته شده‌اند که اطمینان حاصل می‌کنند داده‌ها حتی زمانی که از دسترس خارج شده‌اند، همچنان به صورت رمزنگاری شده خواهند بود.

ممیزی و حسابرسی در امنیت پایگاه داده

با وجود اینکه هک و دسترسی غیرمجاز اهمیت بسیار زیادی دارد، اما این هک‌ها همچنان رخ می‌دهند و نمی‌توان هیچ کاری را در این زمینه انجام داد. بنابراین، پرداختن به امور ممیزی (Auditing) و حسابرسی سیستم بسیار حیاتی است. چون با کمک ممیزی می‌توان مطمئن شد که چه مواردی در خزانه (Inventory) وجود دارند. به عنوان مثال، آگاهی از اطلاعات ظریفی که در تلاش‌هایی برای هک کردن از دست رفته‌اند، یک ضرورت بخ حساب می‌آید. از این رو، باید گزارش‌گیری‌های ممیزی به طور مستمر انجام شوند تا اطمینان حاصل شود که سوابق مناسبی از همه موارد سیستم وجود دارند.

بازیابی در امنیت پایگاه داده

علاوه بر موارد موثر در امنیت پایگاه داده مذکور، بازیابی (Recovery) نیز به عنوان یک سیستم اولیه در نظر گرفته می‌شود که به امنیت پایگاه داده مرتبط است. در واقع، تهیه نسخه‌های پشتیبان از داده‌هایی که در پایگاه داده ذخیره می‌شوند یک امر ضروری به حساب می‌آید. چون در صورت رخنه یا هک سیستم توسط هکر، با کمک

این رویکرد سیستم مربوطه به طور کامل از بین نمی‌رود. علاوه بر این، باید این اطمینان حاصل شود که فایل‌های پشتیبانی کاملاً رمزنگاری شده و ایمن و دو نسخه از آن‌ها در مکان‌های مختلف موجود هستند.

در ادامه برخی از ابزارهای امنیت پایگاه داده معرفی شده‌اند.

ابزارهای امنیت پایگاه داده کدامند؟

برخی از رایج‌ترین ابزارهای امنیت پایگاه داده در ادامه فهرست شده‌اند:

- MSSQLMask
- IBM Guardium
- Scuba
- Hexatier
- Always Encrypted
- AppDetectivePro
- Nmap
- Gemalto SafeNet ProtectDB
- Zenmap
- BSQL Hacker
- Imperva SecureSphere
- SQLRecon
- Oracle Audit Vault

- Mentis Suite
- OScanner
- DB Defence

با توجه به اینکه امنیت پایگاه داده به عنوان یک موضوع پراهمیت در سازمان‌ها محسوب می‌شود، لازم است اقدامات کنترلی امنیت پایگاه داده به طور جامع‌تر و همراه با جزییات بیشتری شرح داده شوند. در بخش بعدی از مقاله «امنیت پایگاه داده چیست»، انواع قابلیت‌های کنترلی مختلفی بررسی می‌شوند که در افزایش امنیت بانک‌های اطلاعاتی نقش به سزایی را دارا هستند.

منظور از روش‌های کنترل امنیت پایگاه داده چیست؟

امنیت پایگاه داده با قابلیت‌های کنترلی مختلفی همراه است. به طوری که با پیروی از پروتکل‌های امنیتی، امکان جلوگیری از افشای اطلاعات محرمانه پایگاه داده فراهم می‌شود. در ادامه به برخی از راهبردهای کنترلی مورد استفاده در امنیت پایگاه داده پرداخته می‌شود.

- **تحکیم و نظارت مستمر :**طراحی ساختاری پایه در امنیت پایگاه داده به عنوان یک روش تکمیلی برای سیستم‌های مدیریت پایگاه داده یا بانک‌های اطلاعاتی مطرح می‌شود. این موضوع به روزرسانی ثابت و پایدار در سیستم، قابل اعتماد نگه داشتن سیستم‌های پایگاه داده را تسهیل می‌دهد. به طوری که این سیستم‌ها با اقدامات و تمهیدات ایمنی به عنوان بخشی از اقدامات احتیاطی امنیتی، به خوبی کار کنند. این امر با صریح نگه داشتن سیستم و عدم وجود نقطه نفوذ به آن و زیر نظر داشتن دائم عملکرد سیستم به دست می‌آید.

- **ساختار سیستم DBMS:** بخش مهمی از ارائه عملکرد موفقیت‌آمیز در یک سیستم پایگاه داده، مجموعه پیکربندی مورد استفاده برای سیستم مدیریت پایگاه داده است. این پیکربندی باید فعالیت‌ها و امتیازات مدیریت، از جمله فعالیت‌های مدیریت دسترسی را پوشش دهد. از این رو، هرگونه سو مدیریت در تنظیمات پیکربندی می‌تواند منجر به آسیب بزرگی در حفاظت از امنیت پایگاه داده و خود آن‌ها شود. این اقدامات هنگام راه‌اندازی سیستم امنیت پایگاه داده روی یک اپلیکیشن ساخته شده‌اند و با استفاده از آن‌ها فرآیند پیکربندی آسان می‌شود.
- **استحکام :**این روش‌ها شامل چندین ویژگی احراز هویت هستند. یعنی، رویکردهایی که به همراه پارامترهای مجوز مربوطه، مانند نام کاربری و رمز عبور، به تایید پرسنل و دسترسی آن‌ها به سیستم ختم می‌شوند. با کمک این رویکرد، امنیت پایگاه داده به صورت دستکاری نشده و دور از مخاطره می‌مانند و حفاظت از سیستم تسهیل می‌یابد.
- **معیارهای پذیرش :**یکی از موثرترین روش‌های استفاده از ویژگی‌های مربوط امنیت پایگاه داده ، ایجاد یک محدودیت ارزشمند است. این محدودیت برای سیستم‌ها یا پرسنل، جهت دستیابی به اطلاعات موجود در سیستم‌های پایگاه داده به کار می‌رود. محدودیت‌های تعیین شده اعمالی مانند حقوق دسترسی به سازماندهی و شفاف نگه داشتن عملکرد سیستم را تسهیل می‌کنند. زمانی که این جنبه امنیت پایگاه داده به سیستم‌های دیتابیس اضافه می‌شود، می‌تواند کیفیت امنیت پایگاه داده را به طور قابل توجهی افزایش دهد.
- **بازرسی دوره‌ای :**نظارت مداوم بر پایگاه داده در فواصل زمانی منظم همراه با فرکانس برنامه ریزی شده، نقش به سزایی در تامین امنیت پایگاه داده ایفا می‌کند. در بازرسی دوره‌ای (Periodical Inspection)به دلیل شفاف نگه داشتن کل سیستم تا حدی معین، مواردی مانند شناسایی رفتارهای نادرست، جلوگیری از نقص‌های احتمالی، کاهش خرابی عمومی مدیریت پایگاه داده تسهیل داده می‌شوند.

- **تصویربرداری و ایجاد کپی برای پشتیبان‌گیری :**تصویربرداری و ایجاد چندین نسخه از یک سیستم می‌تواند از آلوده نشدن یک پایگاه داده کاملاً کاربردی اطمینان حاصل کند. در حقیقت، در بیش‌تر مواقع این پشتیبان‌گیری‌ها حفظ پروتکل‌های امنیتی را آسان‌تر می‌کنند. با ذخیره کپی‌ها و تصاویر در یک مکان دیگر، در صورت از کار افتادن یا سقوط سیستم، می‌توان به راحتی به نسخه قبلی بازگشت. این روش، یک نوع فرآیند بازیابی اطلاعات است که تحت پوشش ویژگی‌های امنیت پایگاه داده قرار می‌گیرد. علاوه بر نکات مذکور، این رویکرد به بازیابی اطلاعات از دست رفته، پاکسازی داده‌های آلودگی، جلوگیری از هک و سایر موارد کمک می‌کند.
- **رمزنگاری :**متداول‌ترین نوع حفاظت از داده‌ها رمزنگاری (Encryption) است. می‌توان به راحتی این روش را روی محتویات داده‌ها یا خود پایگاه داده اعمال کرد. این فرآیند با مجموعه مسئولیت‌های مختلفی همچون مدیریت کلیدهای رمزنگاری، ایمن‌سازی واحد رمزنگاری، نظارت بر منابع پشتیبان، حفظ قوانین کنترل پذیرش و سایر موارد همراه است.
- **امنیت اپلیکیشن :**لازم است مواردی مانند ساخت، نصب و نگهداری امنیت پایگاه داده و اپلیکیشن از حملات رایج هکرها و سیستم‌ها محافظت شوند. چون چنین حملاتی با هدف استفاده حداکثری از اطلاعات به کار می‌روند. از این رو، به واسطه کنترل‌های امنیت پایگاه داده ، امنیت اپلیکیشن نیز تا سطوح بالایی پوشش داده می‌شوند.

در بخش بعدی از مطلب، تعدادی از رایج‌ترین مشکلات محتمل در امنیت پایگاه داده شرح داده خواهند شد.

رایج‌ترین مشکلات در امنیت پایگاه داده کدامند؟

شرایطی مختلفی وجود دارند که ممکن است هکرها به سازمان‌ها و اطلاعات شخصی مشتریان آن‌ها دسترسی غیرمجاز پیدا کنند. به عنوان مثال، در طول چند سال گذشته، در برخی از شرکت‌های مهم و سرشناس، از جمله Slack، یاهو وEquifax ، نقض داده‌ها رخ داده است. این فعالیت‌های فراگیر تقاضا برای نرم افزار امنیت سایبری و تست وب اپلیکیشن را بیش از پیش افزایش داده‌اند. در حقیقت این ابزارها با هدف محافظت از داده‌هایی طراحی شده‌اند که افراد با کسب و کارهای آنلاین به اشتراک می‌گذارند.

در صورتی که این اقدامات امنیتی به کار برده شوند، دسترسی هکرها به تمام رکوردها و اسناد موجود در پایگاه داده‌ها، غیرمجاز خواهد شد. علاوه بر این، با تطابق دادن قوانین با «مقررات عمومی حفاظت از داده‌ها عمومی « (GDPR)مراقبت و حافظت از داده‌های کاربری به مراتب قدرتمندتر می‌شود. در این بخش از مطلب «امنیت پایگاه داده چیست»، به انواع آسیب‌پذیری‌های رایجی پرداخته می‌شود که در سیستم‌های مبتنی بر پایگاه داده مشاهده شده است. علاوه بر این، در ادامه راه‌هایی برای رفع این مشکلات امنیت پایگاه داده ارائه خواهد شد.

عدم انجام تست امنیت پیش از مرحله استقرار

یکی از رایج‌ترین دلایلی که منجر به ضعیف شدن امنیت پایگاه داده می‌شود، عدم توجه به مرحله استقرار (Deployment)در فرآیند توسعه است. با وجود اینکه تست کارکرد (Functional Testing) به منظور کسب اطمینان از کارایی نهایی اعمال می‌شود، اما در صورت انجام عمل غیرمجاز توسط پایگاه داده، این نوع از تست امکان نمایش آن را نخواهد داشت. به همین دلیل، پیش از استقرار، بررسی امنیت وب سایت با انواع تست‌ها حائز اهمیت بسیاری است.

رمزنگاری ضعیف و نفوذ داده‌ها در کنار یکدیگر

ممکن است برخی، پایگاه داده را به عنوان بخش بک اند (Back End) تنظیمات در نظر داشته باشند و تمرکز اصلی را روی حذف خطرهایی بگذارند که از اینترنت حاصل می‌شوند. در حالی که این چنین نیست. رابط‌های اینترنت مختلفی درون پایگاه داده هستند که در صورت وجود ضعف امنیتی، به راحتی امکان پیگیری آن‌ها توسط هکرها ایجاد می‌شود. به منظور جلوگیری از چنین شرایطی، استفاده از پلتفرم‌های ارتباطی رمزنگاری، از جمله SSLو TLS ضروری به حساب می‌آیند.

ضعف در امنیت سایبری و به دنبال آن، پایگاه داده درهم شکسته

برای درک این مشکل امنیت پایگاه داده ، می‌توان به نقض داده‌های شرکت Equifax اشاره کرد. نمایندگان این سازمان اقرار کردند که داده‌های مربوط به ۱۴۷ میلیون مشتری در خطر افتاده بودند. بدیهی است که در چنین شرایطی، تبعات این ضعف امنیت پایگاه داده در سطح بسیار وسیعی باشد. در واقع، با توجه به این نمونه، اهمیت بیش از اندازه نرم افزار امنیت سایبری و نقش آن در حافظت از امنیت پایگاه داده به طور کامل نمایان می‌شود. متاسفانه به دلیل کمبود منابع یا زمان، اغلب کسب و کارها به عمل تست امنیت شبکه کاربر نمی‌پردازند و در سیستم‌های خود ازPatch های دارای نظم استفاده نمی‌کنند. این موضوع باعث می‌شود که این کسب و کارها و امنیت پایگاه داده آن‌ها مستعد نشت داده‌ها (Data Leak) شوند.

دزدیده شدن نسخه‌های پشتیبانی پایگاه‌های داده

به طور کلی، دو نوع خطر وجود دارند که به عنوان تهدید برای امنیت پایگاه داده شناخته می‌شوند. این تهدیدها در دو حالت خارجی و داخلی هستند. در برخی از مواقع، یک کسب و کار تهدیدهای داخلی متعددی را، حتی بیش‌تر از تهدیدهای خارجی، متحمل می‌شود. در حقیقت، هر اندازه که کارمندهای یک کسب و کار مسئولیت‌پذیر باشند و حتی، اگر هر نرم افزار امنیتی قابل قبولی استفاده شود، همچنان سازمان‌ها هیچ گاه نمی‌توانند به طور قطعی و صد در صدی از وفاداری کارمندان خود اطمینان حاصل کنند. چون هر شخصی که امکان دسترسی به داده‌های حساس و پراهمیت را دارد، می‌تواند به راحتی اطلاعات را دزیده و در جهت منافع خود، آن‌ها را به یک سازمان شخص ثالث بفروشد.

با این وجود، می‌توان با کمک اقدامات خاصی چنین ریسک‌هایی را حذف کرد یا به حداقل رساند. به منظور افزایش امنیت پایگاه داده و بهبود مشکل مذکور، مواردی مانند رمزنگاری آرشیوهای پایگاه داده، پیاده‌سازی استانداردهای امنیتی محکم، اعمال جریمه در صورت تخطی از قوانین و استفاده از نرم افزار امنیت سایبری به کار می‌روند. علاوه

بر موارد ذکر شده، لازم است به طور مداوم با افزایش آگاهی تیم کاری از جلسه‌های سازمان، امنیت پایگاه داده را افزایش و ریسک در خطر قرار گرفتن آن را کاهش داد.

وجود ضعف در ویژگی‌ها به عنوان یک مشکل امنیت پایگاه داده

در صورتی که درون ویژگی‌های پایگاه‌های داده ضعف‌های خاصی وجود داشته باشند، زمینه هک شدن آن‌ها توسط هکرها ایجاد خواهد شد. اساساً، هکرها می‌توانند اطلاعات کاربری و اعتبارات مربوطه را بشکنند و سیستم را وادار به اجرای هر کد دلخواهی کنند. با وجود اینکه این موضوع بسیار پیچیده به نظر می‌رسد، اما در واقع، این دسترسی‌ها از طریق ضعف‌های پایه مربوط به ویژگی‌های پایگاه‌های داده بدست می‌آیند. برای رفع این مشکل، می‌توان با تست امنیت پایگاه داده، Dataها را از دسترسی شخص ثالث حفظ کرد و بدین طریق امنیت پایگاه داده را تا حدی افزایش داد. علاوه بر این، هر چه ساختار کارکرد پایگاه داده ساده‌تر طراحی شود، احتمال اینکه ویژگی‌های پایگاه داده به طور مطلوب محافظت شوند بیش‌تر می‌شود.

زیرساخت پیچیده و ضعیف پایگاه داده

به طور کلی، معمولاً هکرها در یک عملیات، تمام پایگاه داده را تحت کنترل خود در نمی‌آورند. به بیان ساده، هکرها با هدف پیدا کردن یک ضعف خاص در زیرساخت پایگاه داده مربوطه و سو استفاده از آن عمل می‌کنند. هکرها یک رشته از حملات را اجرا می‌کنند و این عمل تا زمانی ادامه خواهد داشت که آن‌ها به بک اند دسترسی پیدا کنند. نرم افزار امنیت به طور کامل قابلیت محافظت از سیستم و چنین دستکاری‌هایی را دارا نیست.

حتی در شرایطی که به ضعف‌های ویژگی توجه شود، همچنان مهم است که زیر ساخت کلی پایگاه داده پیچیدگی بسیاری نداشته باشد. چون زمانی که زیرساخت پایگاه داده پیچیدگی زیادی دارد، این احتمال وجود دارد که

برخی از نقاط ضعف بدون بررسی و رفع شدن، فراموش یا نادیده گرفته شوند. به همین دلیل، لازم است که همه بخش‌های سازمان مورد نظر به اندازه یکسان روی سیستم کنترل داشته باشند تا بدین طریق، تمرکز به صورت غیرمتمرکز باشد و ریسک‌های احتمالی به خطر افتادن امنیت پایگاه داده به حداقل برسند.

دسترسی بدون محدودیت ادمین

تقسیم هوشمند وظایف میان ادمین و کاربر این اطمینان را ایجاد می‌کند که تنها افراد دارای تجربه کافی دسترسی بدون محدویت داشته باشند. با استفاده از این رویکرد، دیگر دزدیدن داده‌ها برای افرادی که در فرآیند مدیریت پایگاه داده مشارکت ندارند امری دشوار خواهد بود. حتی در صورتی که امکان محدود کردن تعداد حساب‌های کاربری وجود داشته باشد، معمولاً شرایط بهتر می‌شود. به این دلیل که در این شرایط، به دست گرفتن کنترل پایگاه داده توسط هکرها نیز با چالش‌های بیش‌تری همراه خواهد بود. می‌توان این موضوع را در کسب و کارهای مختلف اعمال کرد، اما معمولاً در صنعت مالی رخ می‌دهد. بنابراین، علاوه بر اینکه آگاهی از دسترسی افراد به داده‌های حساس مهم است، پیش از انتشار، مطلوب است که اجرای تست نرم افزار بانکداری نیز انجام شود.

ناکافی بودن مدیریت کلید

با وجود اینکه رمزنگاری داده‌های حساس حائز اهمیت است، اما علاوه بر آن، توجه به اینکه دقیقاً چه افرادی به کلیدها دسترسی دارند نیز بسیار مهم به حساب می‌آید. با توجه به اینکه معمولاً کلیدها روی هارد دیسک یک فرد ذخیره می‌شوند، واضح است که از این طریق می‌توانند به آن‌ها دسترسی غیرمجاز پیدا کرد و به راحتی آن‌ها را دزدید. در واقع، اگر این ابزارهای مهم امنیت نرم افزار بدون حفاظت، نادیده گرفته شوند، در چنین شرایطی سیستم مورد نظر نسبت به حملات آسیب‌پذیر خواهد بود. بنابراین برای افزایش امنیت پایگاه داده ، لازم است به مدیریت کلیدها نیز توجه شود.

بروز اختلالات در پایگاه‌های داده

یکی از مواردی که منجر به آسیب‌پذیری و به خطر افتادن امنیت پایگاه داده می‌شود، وجود ناسازگاری است. از این رو، لازم است تست امنیت وب سایت به طور مداوم انجام شود تا این اطمینان حاصل شود که داده‌ها حافظت خواهند شد. در شرایطی که مغایرت در سیستم مشاهده شود، باید در اسرع وقت این مغایرت‌ها رفع شوند. در حقیقت، بهتر است توسعه دهندگان سازمان مورد نظر از هر گونه تهدید احتمالی آگاه باشند. تا بدین طریق، از اثرگذاری این تهدیدهای احتمالی روی دیتابیس و کاهش امنیت پایگاه داده جلوگیری کنند. با وجود اینکه نمی‌توان این کار را به راحتی انجام داد، اما با پیگیری‌های مداوم، امکان مخفی نگه داشتن اطلاعات و حفاظت آن‌ها وجود دارد.

امروزه، اغلب کسب و کارها آگاهی کافی در مورد اهمیت تست امنیت و ضرورت وجود آن را دارند. با این وجود، در بسیاری از سازمان‌ها تست امنیت پیاده‌سازی نمی‌شود. این موضوع یک اشتباه محض است که در طول مراحل توسعه بیش‌تر از همیشه نمایان می‌شود. البته باید توجه کرد که در مراحلی مانند ادغام برنامه کاربردی یا به روزرسانی پایگاه داده نیز، اهمیت پیاده‌سازی تست امنیت به صورت کامل قابل مشاهده است. مجرمان سایبری از این مشکلات در جهت منافع خود سو استفاده می‌کنند و در نتیجه، کسب و کار مربوطه ریسک‌های متعددی را متحمل خواهد شد. در ادامه نحوه افزایش امنیت در MySQL مورد بررسی قرار داده می‌شود.

چگونه امنیت پایگاه داده MySQL را افزایش دهیم؟

با توجه به اینکه پایگاه داده MySQL به طور گسترده مورد استفاده قرار می‌گیرد، در این بخش، به بررسی برخی از روش‌هایی پرداخته می‌شود که امنیت این پایگاه داده را افزایش می‌دهند.

- **حذف تمام حساب‌های کاربری ناشناخته :**به طور پیش‌فرض، پس از نصب، MySQLتعدادی حساب کاربری ناشناخته ایجاد می‌کند که عملاً هیچ کاربردی ندارند. به همین دلیل، بهتر است این حساب‌های کاربری حذف شوند، چون وجود آن‌ها در سیستم به عنوان یک نقطه ورود به پایگاه داده برای هکرها به حساب می‌آیند.

- **تغییر نگاشت‌های پورت پیش‌فرض :**به طور پیش‌فرض، پایگاه داده MySQL روی پورت ۳۳۰۶ اجرا می‌شود. پس از نصب آن، لازم است این پورت عوض شود تا بدین طریق، شماره پورت‌های مربوط به خدمات حیاتی در حال اجرا، نامشخص شوند. نکته حائز اهمیت این است که هکرها در اولین حملات سعی می‌کنند مقادیر پیش‌فرض را بررسی کنند. بنابراین، استفاده از پورت پیش‌فرض MySQL می‌تواند امنیت پایگاه داده را به مخاطره بیاندازد.

- **تغییر دسترسی میزبان‌ها به MySQL:** اگر تنظیمات به گونه‌ای باشند که پایگاه داده MySQL به عنوان یک سرور واحد و مستقل (Standalone) راه‌اندازی شود، پیکربندی نمونه MySQL باید به صورتی باشد که فقط به میزبان‌های (Hosts) مجاز دسترسی بدهد. این امر با اعمال تغییرات لازم در فایل‌های hosts.deny و hosts.allow امکان‌پذیر است.

- **عدم اجرای MySQL همراه با دسترسی‌های سطح ممتاز Root:** بهتر است MySQL با استفاده از یک حساب کاربری مشخص و تازه ایجاد شده اجرا شود. علاوه بر این، حساب کاربری مورد نظر باید فقط به مجوزهایی دسترسی داشته باشد که برای اجرای خدمات ضروری هستند. این رویکرد علاوه بر جلوگیری از نفوذ هکرها و دریافت دسترسی از طریق حساب کاربریRoot ، برخی از فواید گزارش‌دهی و ممیزی را نیز به دنبال دارد. بنابراین با توجه به نکات ذکر شده، اجرای این پایگاه داده در سطح ممتاز ریشه یا همان Root مطلوب نیست و توصیه نمی‌شود.

- **حذف و غیرفعال‌سازی فایل تاریخچه MySQL:** به طور پیش فرض در حین نصبMySQL ، فایل تاریخچه (History) این پایگاه داده در مسیر /~.mysql_history ساخته می‌شود. با توجه به اینکه این فایل حاوی اطلاعات تاریخی زیادی در خصوص مراحل نصب و پیکربندی مورد استفاده است، بنابراین باید حذف شود. چرا که به صورت بالقوه، این موضوع می‌توانند منجر به افشا شدن غیرعمدی رمز عبور کاربران پایگاه داده‌های مهم شود. علاوه بر این، باید یک پیوند Soft برای فایل .mysql_historyبه دستگاه null ایجاد شود تا گزارش‌دهی در فایل متوقف شود.
- **غیرفعال کردن ورود از راه دور به حساب کاربری :**در صورتی که پایگاه داده MySQL فقط توسط اپلیکیشن‌های محلی مورد استفاده قرار بگیرد، می‌توان دسترسی از راه دور (Remote) به پایگاه داده را غیرفعال کرد. این امر با باز کردن فایل /etc/my.cnf و اضافه کردن یک نقطه فرار از شبکه (Skip Networking)در بخش mysqld امکان‌پذیر است. پیکربندی پایگاه داده MySQL& با توقف شنود در پورت‌هایTCP/IP ، از جمله ۱۲۷,۰,۰,۱، دسترسی پایگاه داده را به ارتباط‌های مبتنی بر سوکت MYSQL و محلی به طور موثر محدود می‌کند.
- **محدودسازی یا غیرفعال کردن دستور SHOW DATABASES:** همان‌طور که پیش‌تر به آن پرداخته شد، محدودسازی هکرها راه دور و قابلیت‌های آن‌ها در جهت جمع‌آوری اطلاعات، یکی از فاکتورهای حیاتی و مهم برای افزایش امنیت پایگاه داده است. به همین دلیل، لازم است یا دستور SHOW DATABASESبه طور کامل حذف یا تا حد ممکن محدود بشود. این امر با اضافه کردن skip-show-databaseبه بخش mysqld از فایل پیکربندی MySQL انجام می‌شود.
- **غیرفعال کردن امکان استفاده از دستور LOAD DATA LOCAL INFILE:** با کمک دستور مذکور، این امکان برای کاربران فراهم می‌شود که بتوانند فایل‌های محلی را بخوانند و حتی به سایر فایل‌های موجود در سیستم عامل دسترسی داشته باشند. در چنین شرایطی، هکرها می‌توانند از طریق

روش‌های مختلف، از جمله تزریقSQL ، به اکتشاف بپردازند. به همین دلیل، بهتر است دستور LOAD DATA LOCAL INFILEبا درج مقدار صفر به set-variable=local-infile غیرفعال بشود.

- **نامشخص کردن حساب کاربری ریشه :**تغییر نام حساب کاربری Root به اسمی که حدس زدن آن دشوار است نیز یکی دیگر از لایه‌های امنیت پایگاه داده به حساب می‌آید. چون پیش از تلاش برای Brute Forceکردن مقدارهای رمز عبور، لازم است هکرها نام حساب کاربری مورد استفاده را تعیین کنند.
- **تنظیم مجوزهای دسترسی به فایل مناسب :**برای افزایش امنیت پایگاه داده، باید اطمینان حاصل شود که my.cnf تنها از طریق Root قابل نوشتن است. علاوه بر این، باید توجه کرد که محل پیش‌فرض برای داده‌ها، یعنی مسیر/usr/local/mysql/data/ ، همراه با مجوزهای دسترسی، امنیت مطلوب را دارا باشد.