به نام خدا

امیرمهدی شاه حیدری

ازمایشگاه پایگاه داده

استاد میثاق یاریان

امنیت در پایگاه داده

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. پیش از آن، در ادامه و بخش بعدی این مقاله برخی از مفاهیم کلیدی در امنیت پایگاه داده شرح داده شده‌اند.

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 DES برای 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

تا این بخش از مقاله، برخی مفاهیم مربوط به امنیت پایگاه داده و همچنین تعدادی از دوره‌های آموزشی پایگاه داده فرادرس بررسی شدند. اکنون، در ادامه این مطلب، شاخص‌ترین مزیت‌های امنیت پایگاه داده شرح داده شده‌اند.

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

در این بخش از مقاله «امنیت پایگاه داده چیست» به بررسی انواع کنترل‌های امنیتی برای پایگاه داده پرداخته شده است.

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.