ویکی‌پدیا
دانشنامهٔ آزاد

امنیت پایگاه داده

از ویکی‌پدیا، دانشنامهٔ آزاد

امنیت پایگاه داده در رابطه با استفاده از طیف وسیعی از روش‌های کنترل امنیت اطلاعات است به منظور محافظت از پایگاه داده (شامل داده، برنامه‌های کاربردی یا توابع ذخیره شده، سیستم‌های پایگاه داده، سرورهای پایگاه داده) در برابر توافقات محرمانگی، جامعیت و در دسترس پذیری پایگاه داده. که این شامل انواع مختلف از روش‌های کنترلی مانند فنی، رویه‌ای و فیزیکی می‌باشد. *امنیت پایگاه داده* یک موضوع تخصصی در عرصه امنیت رایانه‌ای، امنیت اطلاعات و مدیریت ریسک است.

برای مثال، ریسک‌های امنیتی مرتبط با سیستم‌های پایگاه داده شامل موارد زیر می‌باشد:

- فعالیت‌های غیر مجاز یا ناخواسته یا سوء استفاده توسط کاربران مجاز پایگاه داده، راهبران پایگاه داده، مدیران سیستم / شبکه، یا توسط کاربران غیرمجاز و هکرها (برای مثال دسترسی نامناسب به داده‌های حساس، متا داده یا توابع درون پایگاه داده، یا تغییرات نامناسب در برنامه‌های پایگاه داده، ساختارها یا تنظیمات امنیتی)؛
- مشکلات بدافزارها که می‌تواند باعث بروز حوادثی مانند دسترسی غیرمجاز، افشای اطلاعات شخصی یا اختصاصی، حذف یا صدمه به داده‌ها یا برنامه‌ها، وقفه یا محرومیت از دسترسی مجاز به پایگاه داده، حمله به سیستم‌های دیگر و شکست غیرمنتظره از سرویس‌های پایگاه داده شود؛
- اضافه بار، محدودیت‌های کارایی و مسایل مربوط به ظرفیت و در نتیجه ناتوانی کاربران مجاز در استفاده از پایگاه داده.

آسیب‌های فیزیکی وارد شده به سرورپایگاه داده که ممکن است به دلیل آتش سوزی اتاق سرور، یا سیل، گرمای بیش از حد، رعد و برق و...

- عیوب طراحی یا باگ‌های برنامه نویسی در پایگاه داده ها و برنامه‌ها و سیستم‌های مرتبط، تولید آسیب‌پذیری‌های امنیتی مختلف (برای مثال تشدید)، گم / خراب شدن داده، کاهش کارایی و غیره
- خراب شدن داده یا از دست رفتن آن به دلیل ورود داده یا دستور غیر معتبر، اشتباهات در پایگاه داده یا فرایندهای مدیریت سیستم، خرابکاری‌های عمدی یا آسیب‌های جنایی و غیره.

خیلی از لایه‌ها و انواع روش‌های کنترل امنیت اطلاعات برای پایگاه داده مناسب هستند، از جمله:

- کنترل دسترسی
- رهگیری پایگاه داده (Database auditing)
- اصالت سنجی
- رمزگذاری
- یکپارچگی داده
- فرایند پشتیبان گیری
- امنیت برنامه کاربردی (Application security)

به‌صورت سنتی پایگاه داده تا حد زیادی در برابر هکرها از طریق اقدامات امنیتی شبکه مانند فایروال ها، سامانه تشخیص نفوذ مبتنی بر شبکه، امن شده‌اند. در حالیکه کنترل‌های امنیتی شبکه همچنان در این زمینه با ارزش هستند، ایمن ساختن سیستم‌های پایگاه داده، و برنامه ها/توابع و داده‌های درون آن، به‌طور مستدل بسیار بحرانی تر شده‌اند هنگامیکه شبکه‌ها به منظور

دسترسی گسترده‌تر بازتر می‌شوند، مخصوصاً دسترسی از طریق اینترنت. علاوه بر این، سیستم، برنامه، تابع و کنترل‌های دسترسی به داده، همراه با شناسایی کاربر مرتبط، تصدیق و توابع مدیریتی حقوق، همواره برای محدود کردن و در برخی موارد پیگیری فعالیت‌های مدیران و کاربران مجاز مهم است.

بسیاری از سازمان‌ها خط مبنای استانداردهای امنیتی و طرح جزییات اقدامات اساسی کنترل امنیتی برای سیستم‌های پایگاه داده خود را توسعه داده‌اند.

محتویات

ارزیابی آسیب‌پذیری و موافقت

یک روش برای ارزیابی امنیت پایگاه داده شامل انجام ارزیابی آسیب‌پذیری یا تست نفوذ به پایگاه داده می‌باشد. آزمایش کنندگان همواره تلاش می‌کنند تا آسیب‌پذیری‌های امنیتی را پیدا کنند که می‌تواند برای از بین بردن یا دور زدن کنترل‌های امنیتی استفاده شوند. مدیران پایگاه داده یا مدیران امنیت اطلاعات ممکن است به عنوان مثال از اسکن‌های خودکار آسیب‌پذیری برای یافتن اشکلات پیکربندی استفاده کنند. از نتایج چنین اسکنهایی باعث مقاوم شدن پایگاه داده (بهبود کنترل‌های امنیتی) و بستن آسیب‌پذیری‌های خاص شناسایی شده‌استفاده می‌شود، اما متأسفانه دیگر آسیب‌پذیری‌ها معمولاً ناشناخته باقی می‌ماند. برنامه نظارت مستمر برای پیروی از استانداردهای امنیتی پایگاه داده، یک وظیفه مهم دیگر در محیط پایگاه داده است. دو جنبه مهم از انطباق امنیت پایگاه داده عبارتند از: مدیریت وصله و بررسی و مدیریت مجوزها (به خصوص عمومی) که درون پایگاه داده به اشیاء داده می‌شود. اشیای پایگاه داده ممکن است شامل جدول یا اشیاء دیگر از طریق پیوند بین جداول به وجود می آیند، باشد.

انتزاع

مکانیزم‌های دسترسی و تصدیق در سطح برنامه‌های کاربردی باید به عنوان یک وسیله مؤثر جهت فراهم نمودن انتزاع در سطح لایه پایگاه داده در نظر گرفته شود.

نظارت بر فعالیت پایگاه داده

یکی دیگر از لایه‌های امنیتی که از یک ماهیت پیچیده تر برخوردار است شامل نظارت بر فعالیت‌های پایگاه داده، با استفاده از تجزیه و تحلیل ترافیک پروتکل (SQL) بر روی شبکه، یا با مشاهده فعالیت‌های پایگاه داده محلی بر روی هر سرور با استفاده از عوامل نرم‌افزار یا هر دو می‌باشد. استفاده از عامل‌ها به منظور ضبط فعالیت‌های اجرا شده بر روی سرور پایگاه داده، که معمولاً شامل فعالیت‌های مدیران پایگاه داده است، مورد نیاز می‌باشد.

تجزیه و تحلیل را می‌توان به منظور شناسایی سوء استفاده شناخته شده یا نقض سیاست، یا خطوط مبنایی که در طول زمان می‌تواند ضبط شود، اجرا کرد تا یک الگوی طبیعی را ساخت برای تشخیص فعالیت غیرعادی که می‌تواند نشان دهنده نفوذ باشد. این سیستم علاوه بر مکانیسم‌های تشخیص نفوذ می‌تواند دنباله‌ای جامع از بازرسی‌های پایگاه داده فراهم می‌کند، و همچنین برخی از سیستم‌ها به وسیلهٔ خاتمه دادن به جلسات کاربران یا با قرنطینه کردن کاربرانی که رفتار مشکوک دارند یک سطح از حفاظت را فراهم آورند.

بازرسی محلی

علاوه بر استفاده از ابزارهای نظارت یا بازرسی، قابلیت‌های بازرسی پایگاه داده به صورت محلی، برای بسیاری از پلتفرم‌های پایگاه داده موجود است. دنباله‌ای از بازرسی‌های محلی را می‌توان به صورت منظم استخراج کرده و به یک سیستم امنیتی طراحی شده انتقال داد که مدیران پایگاه داده به آن دسترسی نداشته باشند.

فرایند و رویه‌ها

یک برنامهٔ امنیتی پایگاه داده باید شامل یکسری بازدیدهای منظم از مجوزهایی که به حساب‌های کاربری شخصی و حسابهایی که توسط فرایندهای خودکار اعطا شده باشد. حسابی که توسط فرایند خودکار استفاده می‌شود باید کنترل‌های مناسبی در ارتباط با ذخیره رمز عبور داشته باشد به عنوان مثال رمزنگاری و کنترل‌های دسترسی کافی بمنظور کاهش ریسک توافقات. برای حساب‌های شخصی، یک نوع اصالت سنجی باید در یک محیط پایگاه داده در نظر گرفته شود جایی که ریسک متناسب با هزینه‌های مرتبط با سیستم‌های تصدیق باشد.

جستارهای وابسته

- Negative database
- دیواره آتش کاربردی

پیوند به بیرون

- https://web.archive.org/web/20080511155031/http://iase.disa.mil/stigs/checklist/index.html
- https://web.archive.org/web/20080515131426/http://iase.disa.mil/stigs/stig/index.html