امنیت اطلاعات و ایمن‌سازی بانک های اطلاعاتی

امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای از جمله مسئولیت‌هایی است که مستلزم توجه همه کاربران صرفنظر از موقعیت شغلی آنها می باشد. برای بالا بردن امنیت در شبکه‌های رایانه‌ای و اطلاعاتی، آموزش و توجیه صحیح همه کاربران، وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، از جمله مسائلی است که عدم توجه به آنها عملکرد سازمان و افراد مرتبط با سازمان را تحت تاثیر قرار می دهد.

سه اصل کلیدی امنیت

در بحث امنیت اطلاعات رعایت سه اصل مهم ***حفظ محرمانگی، یکپارچگی و دسترس‌پذیری*** می تواند مشکلات زیادی از این حوزه را برطرف نماید. اگر این سه اصل به درستی رعایت شود اطلاعاتی که درون بانک‌های اطلاعاتی ذخیره می‌شوند قابل استناد بوده و این اطمینان خاطر وجود خواهد داشت که افراد غیرمجاز نمی توانند با دستکاری این اطلاعات، به سوءاستفاده از آنها بپردازند.

محرمانگی به معنای عدم دسترسی افراد غیرمجاز به اطلاعات است. برای محرمانه نگهداشتن اطلاعات، رمزنگاری می‌شود و در طی انتقال یا جاهایی که ممکن است ذخیره شود (در پایگاه‌های داده، فایل‌های ثبت وقایع سامانه، پشتیبان‌گیری، چاپ رسید، و غیره) رمز شده باقی می‌مانند.

اشکال مختلف نقض محرمانگی: ضبط اطلاعات محرمانه نمایش داده شده روی صفحه نمایش رایانه، سرقت رایانه قابل حمل حاوی اطلاعات حساس و یا ارائه اطلاعات محرمانه از طریق تلفن. موارد ذکر شده از مهمترین موارد نقض محرمانگی است.

یکپارچگی به معنای جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و یا تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات نه فقط در حین انتقال بلکه در حال استفاده یا ذخیره شدن به صورت غیرمجاز تغییر داده شود. سامانه‌های امنیت اطلاعات به‌طور معمول علاوه بر محرمانه بودن اطلاعات، یکپارچگی آن را نیز تضمین می‌کنند.

دسترس‌پذیری اطلاعات باید زمانی که مورد نیاز افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار کردن و جلوگیری از اختلال در سامانه‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سامانه‌ها باید در همه حال حتی در زمان قطع برق، خرابی سخت‌افزار، و ارتقاء سامانه نیز در دسترس باقی بمانند. یکی از راه‌های از دسترس خارج کردن اطلاعات و سامانه اطلاعاتی، درخواست‌های زیاد از طریق خدمات از سامانه اطلاعاتی مورد نظر می باشد، که در این حالت چون سامانه توانایی و ظرفیت چنین حجم انبوه خدمات دهی را ندارد از خدمات دادن به‌طور کامل یا جزئی عاجز می‌ماند.

امنیت در حوزه فناوری اطلاعات یک فرایند پیچیده نرم‌افزاری و سخت‌افزاری‌است. به‌طوری که سازمان‌ها برای پیاده‌سازی درست زیرساخت‌های ارتباطی و بانک‌های اطلاعاتی مجبور هستند بر مبنای خط‌مشی‌های دقیق و حساب شده‌ای از تجهیزات و ابزارهای امنیتی استفاده کنند تا داده‌های حساس سازمانی در امنیت بالا و خدمات ارائه شده توسط سازمان با چالش روبرو نشوند.