امنیت اطلاعات دیجیتال ۱

فروردین ماه ۹۸

زیرا یکی از مهم‌ترین ویژگیهای محیط دیجیتالی، شکل‌پذیری و قابلیت تغییر شکل آثار به میزان بالاست. ناشران الکترونیک و کتابخانه‌های دیجیتالی به عنوان نگهبانان حقوق معنوی، نقش فراوانی در جلوگیری از اخلال حقوق مؤلفان دارند؛ زیرا پس از انتشار یک اثر به صورت آنلاین، امکان نسخه‌برداری الکترونیکی آن و دسترسی به حجم عظیمی از اطلاعات وجود دارد. بدیهی است، چنین سرقتی در محیط چاپی امکان‌پذیر نیست. جلوگیری از ورودهای غیرمجاز، از آن جهت نیز اهمیت دارد که اشتراک پایگاه‌های اطلاعاتی دارای بار مالی است و مرکز اطلاع‌رسانی خود نیز اقدام به دریافت وجه در قبال اطلاعات ارائه شده به مراجعان می‌کند. علاوه بر آن، جلوگیری از آسیبهای احتمالی از سوی هکرها و نفوذگران به شبکهٔ اینترنت نیز مسئله امنیت و حفاظت از منابع اطلاعاتی در کتابخانه‌های دیجیتالی را به عنوان یک امر حایز اهمیت مطرح می‌کند.

در هر دو مورد، زمان و تلاش زیادی برای بازگرداندن اطلاعات و ارتقای سیستم امنیتی جدید صرف شد . یک مورد دیگر از این‌گونه حمله‌ها، در یک کتابخانه در دانشگاه نوتردام رخ داد و در طی آن، اطلاعات موجود در معرض خطرهای امنیتی قرار گرفت . بی‌تردید، حفاظت بلند مدت دیجیتالی و ارتقای دسترس‌پذیری میراث مکتوب که هدفهای اساسی کتابخانه‌های دیجیتالی است، بدون لحاظ کردن مسائل امنیتی امکان تحقق نخواهد یافت. تحقیق جهانی امنیت اطلاعات درسال ۲۰۰۳نشان می‌دهد ٪۹۰ سازمانها معتقدند امنیت اطلاعات برای دستیابی آنها به هدفهای کلی‌شان بسیار حایز اهمیت است

برخی از مهم‌ترین مسائل مربوط به امنیت در کتابخانه‌های دیجیتالی می‌تواند شامل امنیت سخت‌افزارها و دیتا سنترها، جایگاه فیزیکی دیتاسنترها و سرورها، امنیت تبادل اطلاعات، امنیت نرم‌افزارهای کاربردی مورد استفاده، امنیت نرم‌افزارهای ضد ویروس و فایروال، الگوی قوانین و مقررات حاکم بر سایت باشد. علاوه بر آن، دیجیتالی کردن آثار، خطر تجاوز به حقوق مؤلفان و پدیدآوران را نیز افزایش می‌دهد،

مزایای ذخیره‌سازی اطلاعات به صورت الکترونیکی، کاربرد وسیع رایانه‌ها در فعالیتهای حرفه‌ای گوناگون را ناگزیر ساخته و استفاده از شبکه‌های رایانه‌ای و بویژه اینترنت، تغییرات اساسی در روند ارائه خدمات به وجود آورده است. این امکانات سبب شده حجم بسیار زیادی از اطلاعات تنها به اندازهٔ یک سرانگشت با کاربران فاصله داشته باشد. ناگفته پیداست، در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستمهای رایانه‌ای، سامانه‌های اطلاعاتی و فعالیتها و زیرساختهای حیاتی وابسته به آنها را تهدید می‌کند

سازمانها اغلب در معرض انواع تهدید مانند دستکاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی قرار دارند.

در چنین شرایطی، چنانچه عواملی که می‌توانند از مزایای سیستمها به شمار بروند (مثل سرعت و قابلیت دسترسی بالا) تحت کنترل نباشند، ممکن است باعث بروز آسیب‌پذیری شده، سوء استفادهٔ افراد بد نیت از آنها به نفوذ و خرابکاری، کلاهبرداری و یا اخاذی بینجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه ای رخ می دهد، درصورت نبود روشهای صحیح برای حفاظت از اطلاعات، می تواند نتایج مخربی را به بار آورد. چنان که حفاظت سیستمهای اطلاعاتی از حملات امنیتی یک چالش مستمر است که بسیاری از سازمانها با آن مواجهند.

با این اوصاف، تدوین و اجرای تدابیر امنیتی در قبال این تهدیدهای گسترده، ضرورتی اجتناب ناپذیر برای سازمانهاست. اتخاذ تدابیر مناسب می تواند احتمال وقوع مخاطرات را به حداقل برساند و یا درصورت وقوع آنها، میزان خسارتهای وارده را در حد بسیار ناچیزی نگه دارد. این‌گونه تدابیر امنیتی، موجب افزایش قابلیت واکنش سریع و مؤثر می‌شود و به این ترتیب سازمانها قادر خواهند بود برای ترمیم خسارتها از فرایندهای از پیش تعیین شده استفاده کنند و بهره‌وری و ایمنی اطلاعات، افزایش یافته، کسب و کار به صورت مطمئن‌تری تداوم یابد. امنیت اطلاعات عبارت است از حفاظت زیرساختهای فناوری اطلاعات و تضمین در دسترس بودن آن. از همین‌رو، حیات کتابخانه های دیجیتالی، ارتباط نزدیکی با سیستم های امنیت اطلاعات دارد.

قلمروِ توصیف شدهٔ کتابخانه های دیجیتالی، برخلاف کتابخانه‌های سنتی، بسیار وسیع است. در کتابخانه های دیجیتالی، کاربر به مواد و منابع متنوعی دسترسی دارد و مجموعه ها و امکانات موجود، نسبت به کتابخانه های سنتی در معرض مخاطرات بیشتری قرار دارند. این کتابخانه‌ها نیازمند پیاده‌سازی برنامه‌های دقیقِ کنترل و سازوکارهای لازم برای نگهداری داراییهای اطلاعاتی خود در دراز مدت هستند. کتابخانهٔ دیجیتالی، نهادی اجتماعی و چیزی بیش از مجموعه ای از فناوریهاست و باید از سازوکارهای جدید برای نگهداری مواد استفاده کند. دسترسی غیرمجاز به اطلاعات و حمله به کتابخانه های دیجیتالی، اتفاق های محتملی هستند که به عنوان نمونه‌هایی از آنها می‌توان به دو رخنهٔ امنیتی در دانشگاه ایندیانا در ایالات متحده آمریکا در تابستان ۲۰۰۲ و ماه می ۲۰۰۴ اشاره کرد