

در موسسات کوچک تر معمولاً برای مسائل امنیتی و حفاظتی یک مسئول در نظر گرفته می شود، در حالی که در موسسات بزرگ تر معمولاً کارکنان متخصص امنیتی جدای از ماموران حفاظتی وجود دارند.

در هر صورت مسئله امنیت در کتابخانه های مختلف متفاوت خواهد بود. نوع کتابخانه، ساختمان و تجهیزات، منابع موجود، تعداد کارمندان و بودجه اختصاص یافته به مسائل امنیتی در برنامه ریزی های مدیران در این زمینه دخیل هستند در واقع هیچ دو کتابخانه ای نیازهای امنیتی یکسان ندارند.

یافته های پژوهشی که اخیراً در مقیاس ملی صورت گرفته در مجموع حاکی از آن است که شیوه های نگهداری کتاب ها و سایر مواد در کتابخانه های ایران کاملاً ابتدایی است و استاندارد ایمنی بسیار پایین است در کتابخانه ها هزاران جلد کتاب نفیس و منحصر به فرد و نیز منابع اطلاعاتی مفید یافت می شود که به سبب بی توجهی در معرض فرسودگی است.

کتابخانه ها فاقد تجهیزات ایمنی هستند بسیاری از مسئولان به نکات ایمنی توجهی ندارند

انباشتنی کتاب ها به صورت فوق العاده متراکم ضریب نا امنی را افزایش داده است.

ساختمان بیشتر کتابخانه ها نا مناسب است و بسیاری از آنها برای کتابخانه ساخته نشده اند شیوه ساختمان سازی و راه های ورودی و خروجی نا مناسب باعث کند شدن دید واکنش های امدادی در مقابل حوادث است

بیشتر کتابخانه ها فاقد دستگاه های هشدار دهنده و اعلام حریق هستند

استفاده از وسایل گرمایی از قبیل بخاری نفتی در بسیاری از کتابخانه ها از نوع قابل اشتعال بوده و هنگام بروز آتش سوزی به گسترش آتش کمک می کند

نصب کپسول های آتش نشانی در قسمت های مختلف کتابخانه کاملاً استاندارد نیست و تقریباً هیچ کتابخانه ای از شیوه علمی آتش نشانی استفاده نمی کند

کتابخانه ها مورد بازدید منظم کارشناسان آتش نشانی قرار نمی گیرند و نظر های آنها اعمال نمی شود

اغلب کتابخانه ها فاقد دستگاه رطوبت و دما سنج هستند و هیچ کنترلی از نظر این دو عامل آسیب زا انجام نمی گیرند تقریباً هیچ یک از کتابخانه ها به دستگاه دزدگیر مجهز نیست

بیشتر کتابخانه ها در مقابل حوادث و بلایا با بیمه قرار دادی ندارند و

قریب به اتفاق کتابخانه ها فاقد طرحی برای مقابله با سوانح و بلایای طبیعی هستند

به این ترتیب می توان گفت که کتابخانه های ایران در واقع کاملاً بی دفاع هستند و شرایط لازم برای حفظ و نگهداری موارث فرهنگی و تاریخی کشور را ندارند



امنیت کتابخانه ۲



دانشکده پرستاری الیگودرز

خرداد ماه ۹۸

تهاجم (attack عملیاتی است که محوریت آن سوء استفاده از نقاط آسیبپذیر و پتانسیل های بروز یک رویداد مخرب می باشد. ارسال ورودی مخرب به یک برنامه و یا flooding یک شبکه به منظور از کار انداختن یک سرویس، نمونه هائی در این زمینه می باشد. یک تهدید پتانسیل بروز یک رویداد مخرب را فراهم می نماید که میتواند به سرمایه های یک سازمان آسیب برساند در حالی که در یک تهاجم موفقیت آمیز از نقاط آسیب پذیر موجود در سیستم استفاده می گردد. چگونه می توان یک برنامه وب ایمن را ایجاد نمود ؟

تا زمانی که شناخت مناسبی نسبت به تهدیدات وجود نداشته باشد، امکان ایجاد یک برنامه وب ایمن وجود نخواهد داشت. بنابراین قبل از هر چیز لازم است که با مدل تهدیدات موجود آشنا شویم. هدف مدل فوق، آنالیز معماری و نحوه طراحی برنامه به منظور شناسائی نقاط آسیب پذیری است که ممکن است به صورت تصادفی توسط یک کاربر ناآگاه و یا مهاجمان با اهداف مخرب مورد سوء استفاده قرار گرفته تا با استناد به آنان بتوانند موجودیت و امنیت سیستم را با خطر مواجه نمایند.

پس از آشنائی با تهدیدات، می بایست با بکارگیری مجموعه ای از اصول امنیتی اقدام به طراحی سیستم نمود. در ادامه، پیاده کنندگان می بایست از روش های ایمن به منظور نوشتن کدهای مطمئن، مستحکم و قابل اعتماد استفاده نمایند. پس از طراحی و پیاده سازی برنامه، می بایست از یک شبکه ایمن، یک host مطمئن و یک پیکربندی مناسب بر روی سرویس دهند، استفاده گردد. ایجاد یک برنامه وب ایمن، مستلزم اقدامات امنیتی چند جانبه ای است که موفقیت در تمامی آنان، ایمن بودن برنامه های وب را تضمین خواهد کرد. ایمن سازی شبکه، host و برنامه، رتوس مثلث امنیتی ایجاد برنامه های وب ایمن را تشکیل می دهند. ایمن سازی شبکه، host و برنامه به منظور ایجاد برنامه های وب ایمن، تبعیت از یک رویکرد جامع امری استالزامی. بنابراین، می بایست امنیت برنامه های وب را در سه لایه متفاوت بررسی و اقدامات لازم را در هر لایه با توجه به جایگاه آن انجام داد. شکل زیر سه لایه مهمه منظور ایجاد برنامه های وب ایمن را نشان می دهد. «امنیت معمولاً به نظام یا فعالیتی اطلاق می گردد که برای جلوگیری از سرقت و دانش ستیزی به کار می رود مثل نظام کنترل کتابخانه، نظام امنیتی کتاب، ناظر سالن، مطالعه یا حفاظ های امنیتی و نظایر آنها. امنیت همچنین یک فرایند است که حفاظت از

مجموعه، ابزار، اطلاعات، کارمندان و تسهیلات فیزیکی را فراهم میکند و از تاثیرات نامطلوب، غیر مجاز و زیان آور به اهداف کتابخانه و آرشیوها جلوگیری می نماید.

گروهی از مدیران، امنیت را زیر گروه برنامه های حوادث غیر مترقبه و اداره مجموعه می دانند و گروه دیگر جلوگیری از دزدی را یک عنصر مجزا از برنامه های دیگر به حساب می آورند. گروهی نیز فقط دزدی و دانش ستیزی را یک خط امنیتی به حساب می آورند و آسیب هایی دیگر از این دست را کنار می گذارند.

فقدان شفافیت در تعریف امنیت و تجزیه موضوعات امنیتی نه حفاظت موثر را تسهیل می کند و نه برنامه های امنیتی را در کتابخانه، حفاظت و امنیت شباهت های زیادی دارند. برای تامین بیشترین حفاظت از مجموعه ها و با توجه به مسائلی مثل دزدی، دانش ستیزی، آسیب های محیطی، حوادث پیش بینی نشده هر دو برنامه فوق باید منظور گردند.