

امنیت در دانشگاه های مجازی

مسعود کیانی* - پیمان یارمحمدزاده** - دکترسید علی سیادت***

چکیده

تلاش انسان در قرن بیست و یکم برای کسب قابلیت های لازم برای زندگی که مملو از فناوری اطلاعاتی و ارتباطی است باید در جهت افزایش روز افزون دانش کاری و فناوری نوین باشد دانشگاه های مجازی امروزه با استفاده از تکنولوژی نوین و ابزارهای پیشرفته سعی دارند آموزش را به گونه اثربخشی در اختیار فراگیران خود قرار دهند امنیت اطلاعات و ارتباطات مسأله ای است که توجه به آن در دانشگاه های مجازی در جهت ایجاد یک محیط امن و مناسب آموزشی ضروری است امنیت در دانشگاه های مجازی در تمام مراحل طراحی، پیاده سازی، تست و اصلاح و هر یک از قسمت های این سایت ها با توجه به اهمیت و صحت و محرمانه بودن اطلاعات باید در نظر گرفته شود. پژوهش حاضر از نوع پژوهش های توصیفی - تحلیلی و به شیوه کتابخانه ای صورت گرفته است و بر طبق مدل تحلیل خطر در سیستم های امنیتی در پی پاسخ به سه سؤال اساسی است: کدامیک از بخش های سایت دانشگاه مجازی و تا چه میزان باید مورد حفاظت قرار گیرد؟ این حفاظت در برابر «چه کسی» صورت می گیرد؟ و نهایتاً «چگونه» این حفاظت می خواهد صورت پذیرد؟

کلید واژه ها: امنیت اطلاعات، امنیت شبکه، آموزش الکترونیکی، دانشگاه مجازی، آموزش مبتنی بر وب، امنیت الکترونیکی، کلاس های مجازی، سیستم مدیریت امنیت اطلاعات.

Keywords: Information Security, Network Security, Electronic Learning, Virtual University, web based Learning, Electronic Security, Virtual classrooms, Information security manage system.

مقدمه

تکنولوژی امروز با به کارگیری شبکه های اطلاعاتی و ارتباطی در یک جامعه دانش محور توانسته تأثیر قابل ملاحظه ای را بر بخش های مختلف اقتصادی، آموزشی، سیاسی و نظامی بگذارد. با ظهور رایانه و شکل گیری شبکه های ارتباطی، نظام آموزشی کشورها دچار تحول گردید و سعی شد با به کارگیری این فناوری ها تولید، توزیع و مصرف اطلاعات به عنوان اساسی ترین معیار توسعه هر کشور تسهیل گردد. پس از شکل گیری اینترنت به عنوان بزرگترین شبکه اطلاعات و ارتباطات جهانی، در آموزش رویکردی نوین پدید آمد در این دوره انواع آموزش های وب - محور از جمله: مکاتبه غیر همزمان در محیط وب، مکاتبه همزمان در محیط وب، کلاس های برتر وب، کلاس های تحت مدیریت وب و آموزش های مجازی مطرح گردیدند.

* - دانشجوی کارشناسی تکنولوژی آموزشی

** - دانشجوی کارشناسی ارشد مدیریت آموزشی

*** - عضو هیئت علمی دانشگاه اصفهان

با توجه به اینکه آموزش الکترونیکی دارای مزایای بسیاری نظیر عدم وابستگی به زمان، مکان و حضور فیزیکی استاد و دانشجو، کیفیت بالاتر ارائه درس، پشتیبانی از تعداد زیاد دانشجویان در یک کلاس، بالا رفتن میزان اثربخشی و بازده آموزشی و... است دانشگاه های امروز توجهی ویژه به این نوع از آموزش مبذول داشته اند. این دانشگاه ها با فراهم کردن زیرساخت های سخت افزاری، نرم افزاری و مخابراتی، تدوین محتوای آموزشی، برقراری رشته های آموزشی در محیط وب، تعیین شیوه جذب دانشجو، شیوه ارزیابی فراگیران و دانشجویان، گسترش روح آموزش مشارکتی در محیط وب و استفاده از سیستم های آموزش هوشمند سعی در ایجاد دوره های آموزشی مؤثر نموده اند. اما مسأله ای که کمتر در ساختار آموزش الکترونیکی به آن پرداخته شده است، مسأله امنیت می باشد. امنیت اطلاعات از جمله مهمترین چالش هایی است که امروز دانشگاه های مجازی با آن روبه رو هستند. بواسطه فقدان زیرساخت هائی از قبیل نظام ارزیابی امنیتی فضای تبادل اطلاعات، نظام صدور گواهی و زیرساختار کلید عمومی، نظام تحلیل و مدیریت مخاطرات امنیتی، نظام پیشگیری و مقابله با حوادث فضای تبادل اطلاعات، نظام مقابله با جرائم فضای تبادل اطلاعات و سایر زیرساخت های امنیتی فضای تبادل اطلاعات، دانشگاه های مجازی نمی توانند فضای آموزشی امنی را برای دانشجویان و اساتید خود فراهم سازند.

یافته ها

۱. هریک از قسمت های سایت های دانشگاه مجازی با توجه به سه اصل دسترسی، محرمانه بودن و صحت اطلاعات مورد محافظت قرار گیرد.
۲. توجه به حفظ امنیت در پنج لایه اصلی شبکه در دو حیطه سخت افزاری و نرم افزاری در سایت های آموزش مجازی امری ضروری می باشد.
۳. افراد و کاربران ناوارد، هکرها و افراد سودجو و... از جمله کسانی هستند که می توانند آسیب های جدی به سایت های دانشگاه مجازی وارد کنند و گاه تامدتی باعث از کار افتادن این سایت ها شوند.
۴. برای حفظ سایت های دانشگاه مجازی از خطرات احتمالی باید این سایت ها را با توجه به استانداردهای امنیتی و با امکانات سخت افزاری و نرم افزاری مناسب پشتیبانی کرد.

بحث و نتیجه گیری

اهمیت سیستم مدیریت امنیت در تبادل اطلاعات (ISMS) در حدی است که تا کنون استاندارد های مختلفی در این زمینه تدوین شده است از جمله این استاندارد ها می توان به استاندارد مدیریتی BS7799 مؤسسه استاندارد انگلیس، استاندارد مدیریتی ISO/IEC 17799 مؤسسه بین المللی استاندارد و گزارش فنی ISO/IEC TR 13335 مؤسسه بین المللی استاندارد اشاره کرد. با توجه به این استاندارد ها می توان یک چرخه ایمن سازی شامل چهار مرحله طراحی، پیاده سازی، تست و اصلاح برای ایجاد امنیت در سایت های آموزش مجازی در نظر گرفت. در دانشگاه های مجازی باید اطلاعات به طور صحیح طبقه بندی شوند و با توجه به اهمیت آن ها مورد حفاظت قرار گیرند. این امنیت باید در طی چهار مرحله بازرسی، حفاظت، ردیابی، واکنش و بازتاب و در پنج لایه پیرامون، شبکه، میزبان، برنامه کاربردی و

داده‌ها و بر طبق سه پارامتر دسترسی، محرمانه بودن و صحت ایجاد گردد. در این پژوهش بیشتر به مسأله امنیت در سه لایه میزبان، برنامه کاربردی و داده‌ها توجه شده و شرایط لازم برای ارائه آموزش با کیفیت در یک محیط مجازی امن در وب فراهم آمده است. همچنین به بخش‌های مختلف دانشگاه مجازی از جمله صفحه خانه، پرونده مدرسان، پرونده فراگیران، مشاوره، ثبت نام، کلاس درس، محدوده شخصی دانشجویان، ارزشیابی و امتحان و... و امنیت هر یک از این بخش‌ها پرداخته شده است. جنبه‌های مختلف امنیت (نفوذ، مکانیزم امنیتی و سرویس امنیتی) در سایت‌های آموزش مجازی باید به طور دقیق در نظر گرفته شود و آمادگی لازم برای دفاع در مقابل هر نوع حمله خارجی فراهم آید.

منابع

۱. بهشتی زهرا؛ بررسی نقش آموزش الکترونیکی در حل مشکلات آموزش سنتی، مجموعه مقالات دومین همایش آموزش الکترونیکی، ۱۳۸۳
۲. فراهی احمد و سعید جلیلی، مدرس مجازی هوشمند، مجموعه مقالات دومین همایش آموزش الکترونیکی، ۱۳۸۳
۳. حیدری آرام و افشین لامعی، امنیت الکترونیکی؛ نیازها، راه حل‌ها و چالش‌ها، همکاران سیستم، ۱۳۸۳
4. William Stallings, Cryptography and Network Security, Principles and Practice, Prentice-Hall, 1998
5. Christopher M.King, Curitis E.Dalton, Security Architecture, Design, Deployment & Operations, RSA Press
6. <http://www.fata.ir/bulletin/archives/000113.php>
<http://www.takfa.ir/portal/>