
بسم الله الرحمن الرحيم

سمینار

عنوان
مطالعه و ارزیابی امنیت در تجارت الکترونیک

توسط:

چکیده

به دلیل اینکه تجارت الکترونیک در فضای مجازی انجام می شود وعملیات آن برای طرفین معاملات ملموس نیست، حفظ امنیت داده‌ها بعنوان یکی از راه‌های جلب اعتماد مشتریان به تجارت الکترونیک از اهمیت بالایی برخوردار است. امنیت عنصر کلیدی استکه توسعه تجارت الکترونیکی را تضمین می‌کند. شبکه‌های عمومی نظیر اینترنت دارای ضعف امنیتی زیادی می‌باشد، به همین دلیل در تمام لایه‌های این شبکه پروتکل‌های امنیتی مختلفی شکل گرفته‌اند. این سمینار ضمن بررسی انواع تهدیدات امنیتی در عرصه تجارت الکترونیکی به طبقه‌بندی و ارزیابی آنها می‌پردازد. و آخر روش‌های افزایش امنیت در تجارت الکترونیک را مورد مطالعه و ارزیابی قرار می‌دهیم. خطرات امنیتی ناشی از عملکرد نامطلوب افراد، نرم افزارها و سخت افزارهایی است که درحوزه‌ی ایجاد و بهره برداری از تجارت الکترونیکی فعالیت دارند. اینگونه تهدیدات که منشاء ایجاد ناامنی در شبکه‌های کامپیوتری محسوب می‌شود می‌تواند به شیوه‌های مختلفی ازجمله: استراق سمع، از کاراندازی سرویس، تجسس و دسترسی غیر قانونی ، فعالیت ویروس‌ها و کرم‌ها، ارسال داده‌ها با حجم زیاد، بهره‌گیری از روش‌های مهندسی اجتماعی، بکارگیری درهای پشتی و همچنین حملات فیزیکی انجام پذیرد.

کلمات کلیدی: حملات، تجارت الکترونیک، امنیت، اینترنت

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

فصل اول

مقدمه

۱-۱- مقدمه

در حال حاضر به طور فزاینده‌ای اطلاعات مالی، اعتباری و شخصی از شبکه‌های مبتنی بر اینترنت در سرتاسر جهان استفاده می‌نمایند. از سوی دیگر از آنجایی که مسیر گردش اطلاعات و منابع روی شبکه بسیارند، لذا مشخص نمی‌باشد اطلاعات مذکور کجا می‌روند و چه اشخاصی از آنها بهره‌برداری می‌نمیایند. بدین ترتیب حفظ امنیت اطلاعات از مباحث مهم تجارت الکترونیک محسوب می‌شوند. هر چند امنیت مطلق وجود ندارد اما لااقل برخورداری از یک وضعیت غیر شکنده می‌یابد هزینه‌های را صرف نمود. هر ساله سازمان‌های بسیاری هدف جرائم مرتبط با امنیت اطلاعات، از جمله ویروسی گرفته تا کلاه‌برداری‌های تجاری از قبیل سرقت اطلاعات حساس تجاری و اطلاعات محرمانه کارت‌های اعتباری، قرار می‌گیرند. چنین حملات امنیتی موجب میلیون‌ها دلار ضرر و اخلال در فعالیت شرکت‌ها می‌شوند. این واقعیت است که با افزایش کاربران سیستم‌های اطلاعاتی، دسترسی آسان به اطلاعات و رشد فزاینده کاربران مطلع می‌توان به راحتی فرض کرد که تعداد این سوء استفاده‌ها از فناوری و تهدیدهای امنیتی نیز به همین نسبت افزایش یابد. متاسفانه، از آنجا که بسیاری از شرکت‌ها دوست ندارند نفوذ به سیستم‌شان را تایید و اطلاعاتشان در مورد این نفوذها و وسعت آنها را با دیگران به اشتراک بگذارند، میزان دقیق خساراتی که شرکت‌ها از جرائم مرتبط با امنیت متحمل شده‌اند، را نمی‌توان بدست آورد. بی‌میل به ارائه اطلاعات مربوط به نقائص امنیتی، از این ترس معمول ناشی می‌شود که اطلاع عموم از چنین نقائصی باعث بی‌اعتمادی مشتریان نسبت به توانایی شرکت در حفظ دارایی‌های خود می‌شود و شرکت با این کار مشتریان خود و در نتیجه سوددهی اش را از دست خواهد. از آنجایی که مصرف‌کنندگان امروزی نسبت به ارائه آنلاین اطلاعات مالی بی‌اعتماداند، شرکت‌ها با تایید داوطلبانه این واقعیت که قربانی جرائم مرتبط با امنیت شده‌اند، چیزی بدست نمی‌آورند. با هیجانات رسانه‌ای که امروزه دور و بر اینترنت و قابلیت‌های آن وجود دارد، حفظ یک تصویر مثبت از امنیت تجارت الکترونیک در اذهان، دغدغه شماره یک بسیاری از شرکت‌ها است و برای بقاء و باقی ماندن در رقابت کاملا ضروری است. نبود اطلاعات دست اول از موارد واقعی برنامه‌ریزی و مقابله با تهدیدهای امنیتی را بسیار مشکل‌تر کرده است اما با این وجود هم فناوری‌ها و روش‌های امنیت اطلاعات و فنون کلی مدیریتی در برنامه‌ریزی و حفاظت از منابع فناوری اطلاعات سازمان، در یک دهه گذشته پیشرفت قابل توجهی داشته‌اند. اکنون خبرگانی هستند که در حوزه امنیت سایبر تخصص پیدا کرده‌اند و راهکارهای زیادی برای حفاظت از فناوری‌های تجارت الکترونیک از مجرمین بالقوه فضای سایبر دارند. بسیاری از شرکت‌ها دریافته‌اند که برای موفقیت در تجارت الکترونیک، علاوه بر روش‌های امنیتی که برای حفاظت از منابع فناوری اطلاعات طراحی شده‌اند، نیازمند سرمایه‌گذاری و برنامه‌ریزی برای ایجاد یک برنامه جامع امنیت هستند تا بدان طریق از دارایی‌هایشان در اینترنت محافظت و از نفوذ مجرمین به سیستم‌هایشان که موجب خسارت دیدن فعالیت‌های تجارت الکترونیک آنها می‌شود جلوگیری کنند. برنامه جامع امنیت تجارت الکترونیک شامل برنامه‌های حفاظتی که از فناوری‌های موجود، افراد، برنامه‌ریزی راهبردی استفاده می‌کنند و برنامه‌های مدیریتی که برای حفاظت از منابع و عملیات تجارت الکترونیک شرکت طراحی و اجرا می‌شوند، است. چنین برنامه‌ای برای بقاء کلی فعالیت‌های تجارت الکترونیک شرکت حیاتی است و سازمان باید آنرا به عنوان

مولفه‌ای اساسی در راهبرد تجارت الکترونیک موفق به حساب آورد[1]. موفقیت چنین برنامه‌هایی به حملات کامل مدیران رده بالا و مشارکت کامل بخش فناوری اطلاعات و مدیریت در جهت درک تاثیرگذاری و محدودیت‌های برنامه است. علاوه بر این برای اطمینان از بروز بودن این برنامه و ابزارهای آن و هماهنگ با آخرین فناوری‌ها و فنون مدیریت، باید آن را بطور مداوم مورد ارزیابی و سنجش قرار داد.