

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

سمینار

عنوان

مطالعه و ارزیابی امنیت در تجارت الکترونیک

توسط:

چکیده

به دلیل اینکه تجارت الکترونیک در فضای مجازی انجام می شود و عملیات 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 است که توسعه تجارت الکترونیکی را تضمین می کند. شبکه‌های عمومی نظیر اینترنت دارای ضعف امنیتی زیادی می باشد، 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 می پردازد. و آخر روش‌های افزایش امنیت در تجارت الکترونیک را مورد مطالعه و ارزیابی قرار می دهیم. خطرات امنیتی ناشی از عملکرد نامطلوب افراد، نرم افزارها و سخت افزارهایی است که در حوزه‌ی ایجاد و بهره برداری از تجارت الکترونیکی فعالیت دارند. اینگونه تهدیدات که منشاء ایجاد ناامنی در شبکه‌های کامپیوتری محسوب می شود می تواند به شیوه‌های مختلفی از جمله: 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

صفحه

عنوان

۱	چکیده
۷	فصل اول: مقدمه
۸	۱-۱- مقدمه
۱۰	فصل دوم: مروری بر امنیت در تجارت الکترونیک
۱۱	۱-۲- مقدمه
۱۲	۲-۲- تعریف امنیت
۱۲	۳-۲- تجارت الکترونیک
۱۳	۴-۲- بکارگیری امنیت در تجارت الکترونیکی
۱۳	۱-۴-۲- سیکل زندگی مهندسی امنیت
۱۳	۲-۴-۲-۱-۱- خصوصیات مورد نیاز امنیت و آنالیز ریسک
۱۳	۲-۴-۲-۱-۲- خصوصیات سیاست امنیتی
۱۳	۲-۴-۲-۱-۳- خصوصیات زیرساختهای امنیتی
۱۳	۲-۴-۲-۱-۴- بکارگیری زیرساختهای امنیتی
۱۴	۲-۴-۲-۵-۱- تست امنیت
۱۴	۲-۴-۲-۶-۱- ارزیابی نیازمندیها
۱۴	۲-۴-۲-۲- نیازهای امنیتی
۱۴	۲-۴-۲-۱-۲- تعیین اعتبار
۱۴	۲-۴-۲-۲-۲- پنهانی
۱۴	۲-۴-۲-۳-۲- تمامیت
۱۵	۲-۴-۲-۴-۲- عدم انکار
۱۵	۲-۴-۲-۳- سیاستهای امنیتی
۱۵	۲-۴-۲-۴- زیرساختهای امنیتی
۱۵	۲-۴-۲-۵- تست امنیت (بررسی تطابق)
۱۶	۲-۵- حملات امنیتی
۱۷	۲-۶- بررسی ریسکها و تهدیدهای موجود در تجارت الکترونیک

۱۸	۱-۶-۲- ریسک‌های موجود.....
۱۸	۱-۱-۶-۲- ریسک‌های حوزه حریم خصوصی و امنیت.....
۱۸	۲-۱-۶-۲- ریسک‌های حوزه خدمات مشتری.....
۱۹	۳-۱-۶-۲- ریسک‌های حوزه فروشنده.....
۱۹	۴-۱-۶-۲- ریسک‌های حوزه محصول.....
۱۹	۲-۶-۲- تهدیدهای موجود.....
۱۹	۱-۲-۶-۲- بدافزار.....
۱۹	۲-۲-۶-۲- DOS.....
۱۹	۳-۲-۶-۲- Defacement.....
۲۰	۴-۲-۶-۲- Datastreaming.....
۲۰	۵-۲-۶-۲- Phishing.....
۲۰	۶-۲-۶-۲- سیستم‌های درست پیکربندی نشده.....
۲۰	۷-۲- اعتماد و امنیت در تجارت الکترونیک.....
۲۲	۸-۲- جمع‌بندی.....

۲۳	فصل سوم: مطالعه و بررسی روش‌های افزایش امنیت در تجارت الکترونیک
۲۴	۱-۳- مقدمه.....
۲۵	۲-۳- خدمات و مکانیزم‌های امنیتی.....
۲۵	۱-۲-۳- خدمات امنیتی.....
۲۵	۲-۲-۳- مکانیزم‌های امنیتی.....
۲۶	۳-۳- مشکلات امنیت در تجارت الکترونیکی.....
۲۶	۴-۳- روش‌های افزایش امنیت.....
۲۶	۱-۴-۳- الگوریتم‌های رمزنگاری.....
۲۷	۱-۱-۴-۳- فناوری رمزنگاری داده‌ها.....
۲۷	۲-۱-۴-۳- الگوریتم رمزنگاری کلید عمومی.....
۲۷	۳-۱-۴-۳- فناوری رمزنگاری ترکیبی.....
۲۸	۴-۱-۴-۳- الگوریتم‌های متقارن.....

- ۳-۴-۱-۵- الگوریتم‌های نامتقارن ۲۹
- ۳-۴-۱-۶- الگوریتم‌های هش ۳۰
- ۳-۴-۲- امضا دیجیتال ۳۰
- ۳-۴-۱-۱- امضا بوسیله الگوریتم کلید عمومی ۳۱
- ۳-۴-۲-۲- امضا با تابع درهم‌سازی یک طرفه ۳۱
- ۳-۴-۳- گواهی دیجیتال ۳۲
- ۳-۵-۵- بررسی فناوری‌های امنیتی ۳۳
- ۳-۵-۱- زیرساخت کلید عمومی ۳۳
- ۳-۵-۲- سرویس رمزنگاری PGP ۳۴
- ۳-۵-۳- طراحی سه لایه ی وب ۳۴
- ۳-۵-۴- EbXml ۳۵
- ۳-۵-۵- فناوری تشخیص هویت ۳۵
- ۳-۵-۵-۱- فناوری تشخیص هویت دیجیتال ۳۶
- ۳-۵-۵-۲- فناوری تشخیص هویت بیولوژیکی ۳۶
- ۳-۵-۵-۱-۲- تشخیص هویت با اثر انگشت ۳۶
- ۳-۵-۵-۲-۲- تشخیص هویت با عنبیه ۳۶
- ۳-۵-۵-۳-۲- تشخیص هویت با صورت ۳۷
- ۳-۵-۵-۴- تشخیص هویت با شکل دست ۳۷
- ۳-۵-۵-۵-۲- تشخیص هویت با کف دست ۳۷
- ۳-۵-۵-۶-۲- تشخیص هویت با راه رفتن ۳۷
- ۳-۵-۵-۷-۲- تشخیص هویت با امضای دستی ۳۷
- ۳-۵-۵-۸-۲- تشخیص هویت با صدا ۳۸
- ۳-۵-۶- فناوری پرداخت ایمن ۳۸
- ۳-۵-۶-۱- پروتکل SSL ۳۸
- ۳-۵-۶-۲- پروتکل SET ۳۸
- ۳-۵-۷- فناوری دیواره آتش ۳۹
- ۳-۵-۷-۱- دسته‌بندی دیواره آتش ۴۰
- ۳-۵-۷-۱-۱- دیواره آتش غربال کننده میزبان ۴۰
- ۳-۵-۷-۱-۲- دیواره آتش غربال کننده زیر شبکه ۴۰

۳-۵-۸- فناوری تشخیص نفوذ..... ۴۰

۳-۴- جمع بندی ۴۲

فصل چهارم: نتیجه گیری و پیشنهادات ۴۳

۴-۱- نتیجه گیری و پیشنهادات ۴۴

مراجع ۴۵

فهرست اشکال

- شکل ۱-۲- ارسال صحیح داده از مبدا به مقصد..... ۱۶
- شکل ۲-۲- حمله قطع..... ۱۶
- شکل ۳-۲- حمله استراق سمع..... ۱۶
- شکل ۴-۲- حمله دستکاری..... ۱۷
- شکل ۵-۲- حمله جعل..... ۱۷
- شکل ۱-۳- رمزنگاری و رمزگشایی در الگوریتم متقارن..... ۲۸
- شکل ۲-۳- رمزنگاری و رمزگشایی در الگوریتم نامتقارن..... ۲۹
- شکل ۳-۳- الگوریتم هش..... ۳۰
- شکل ۴-۳- امضای الکترونیکی بر روی کارت هوشمند..... ۳۲
- شکل ۵-۳- زیرساخت کلید عمومی PKI..... ۳۳
- شکل ۶-۳- معماری سه لایه وب..... ۳۴

فصل اول

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 می‌نمایند. 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 شکننده 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. متأسفانه، 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 کاملاً 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 هماهنگی با آخرین فناوری‌ها و فنون مدیریت، باید آن را بطور مداوم مورد ارزیابی و سنجش قرار داد.