APJ. 5(2):16-25, Summer 2024

Arman Process Journal (APJ)

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Investigating Security Dimensions in Electronic Businesses

A. Shokri[*,1]

[1] Department of Computer Engineering, Islamic Azad University, Science and Research Branch, Tehran, Iran

RESEARCH PAPER

Received: 11 April 2024
Accepted: 15 June 2024

KEYWORDS:
E-Business,
E-commerce Security,
Threat Management,
Authentication,

[1] **Corresponding author:**
a.shokri@srbiau.ac.ir

ABSTRACT

The rapid expansion of the Internet and the cost-effective growth of key technologies enable it to revolutionize information technology and create unprecedented opportunities for the development of large-scale distributed applications. At the same time, there is a growing concern about the security of web-based businesses, which are rapidly proliferating on the Internet. Implementing electronic business systems and entering the field of electronic commerce are technical and social solutions to facilitate communication and easy access to information. But the increase of business dependence on information systems has resulted in damages, threats and technical and non-technical measures to violate the principles of business information security, which is the main challenge and problem of organizations and the subject of this article. To achieve dynamic e-businesses, we must implement security in it under fundamental frameworks so that we can use it as a sustainable example of business. A correct understanding of security risks and risks, especially the risks that exist in the executive frameworks of electronic businesses, help a lot in the design and architecture of a safe and efficient infrastructure. In this article, we are going to examine the security aspects of electronic businesses.

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۲، تابستان ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

بررسی ابعاد امنیتی در کسب و کارهای الکترونیک

علیرضا شکری[*،۱]

[۱] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات و تهران و ایران

چکیده

مقاله پژوهشی

گسترش سریع اینترنت و رشد مقرون‌به‌صرفه فن‌آوری‌های کلیدی آن را قادر می‌سازد تا با انقلابی فن‌آوری اطلاعات و ایجاد فرصت‌های بی‌سابقه‌ای برای توسعه برنامه‌های کاربردی در مقیاس بزرگ توزیع‌شده عمل نماید. در همان زمان، نگرانی رو به رشد امنیت برنامه‌های کاربردی مبتنی بر وب، که به‌سرعت در حال گسترش بر روی اینترنت هستند وجود دارد. پیاده سازی سیستم های کسب و کار الکترونیک و ورود به حوزه تجارت الکترونیک، راهکارهای فنی و اجتماعی برای تسهیل ارتباطات و دسترسی آسان به اطلاعات می باشد. اما افزایش وابستگی کسب و کار به سیستم های اطلاعاتی آسیب ها، تهدیدات و اقدامات فنی و غیر فنی برای نقض اصول امنیت اطلاعات کسب و کار را بدنبال داشته است که این چالش ومساله اصلی سازمان ها و موضوع این مقاله می باشد. برای دستیابی به کسب و کارهای الکترونیک پویا باید امنیت را در آن تحت چارچوب های اصولی پیاده سازی نماییم تا بتوانیم از آن به عنوان یک نمونه پایدار از تجارت استفاده کنیم. فهم و درک صحیح از ریسک ها و خطرات امنیتی، به ویژه خطراتی که در چارچوب های اجرایی کسب و کارهای الکترونیک وجود دارد، کمک زیادی درطراحی و معماری یک زیر ساخت امن و کارامد می نمایند. در این مقاله قصد داریم ابعاد امنیتی کسب و کارهای الکترونیک را بررسی نمائیم.

واژگان کلیدی:
کسب و کار الکترونیک،
امنیت،
مدیریت تهدیدات،
تایید هویت،

مقدمه

امروزه تعداد زیادی از سازمان‌های خصوصی و عمومی بر پایه سیستم های مدیریت گردش کاری عمومی هستند و در حال یافتن راه‌هایی برای بهبود خدمات و فرایند تصمیم‌گیری امن می باشند. هیجان ایجاد کسب و کار الکترونیکی جدید و پویا توأم با رقابت بر سر رسیدن (امنیت کسب و کار الکترونیکی) به بازار، بسیاری از شرکت‌ها را به سمت مخاطرات اساسی و جدید سوق می‌دهد. دلیل وجود چنین موردی، سازمانی توسعه یافته است که سیستم ها و داده ها را به روی افراد خارجی باز می‌کند. سیستم های طراحی شده ضعیف با پتانسیل مستعد فنی که در کنار هم قرار داده می شوند غالبا از مخاطرات زیادی که در آن‌جا کمین کرده‌اند غافل هستند. سازمان ها ممکن است به واسطه غفلت و نقض حفظ حریم خصوصی امنیتی متهم شوند. امنیت سیستم بخشی از خط‌مشی گسترده امنیتی است که باید شامل امنیت فیزیکی و امنیت رویه‌ای باشد [۱]. برای بهره‌برداری مؤثر از برنامه های کاربردی وب و تجارت الکترونیک، امنیت یک موضوع کلیدی است. تهدید امنیت تجارت الکترونیک شامل نقض کنترل دسترسی، نقض تمامیت، خرابکاری، تقلب، نقض حریم خصوصی، و همچنین محرومیت از خدمات و زیرساخت‌هاست. تمام این تهدیدات جمعی به‌عنوان جنگ سایبری و یا سایبر تروریسم شناخته شده‌اند.اساساً جنگ سایبری در مورد خراب‌کاری در وب و خراب کردن تمام اجزای آن است به‌طوری‌که دشمن یا نظام مخالف فروریزد. در حال حاضر مقدار زیادی از پول‌هایی که توسط دولت‌های مختلف در آمریکا و غرب اروپا برای انجام تحقیقات در حفاظت از وب و جلوگیری از جنگ سایبری و تروریسم سایبری است وجود دارد [۲]. کسب و کار الکترونیکی در عین حال که دقت و سرعت پردازش را به شکل کاملا محسوسی بالا برده است در معرض خطرات و تهدیدهایی نیز قرار دارد. به دلیل اینکه طبیعت کسب و کار الکترونیکی نیاز به ارسال اطلاعات بین کسب و کار و مشتری دارد می بایست از توجه کافی در رابطه با امنیت و فعالیت‌های برخط به منظور حفاظت از سرمایه کسب و کار، اعتبار و حریم خصوصی کاربر و ارتباط با کاربر اطمینان حاصل نمود. چنین تبادلاتی نیازمند وجود بسترهای ایمن است. خطرات امنیتی زیادی از قبیل سرقت و یا تغییر محتوای پیامها هریک از مراحل فوق را تهدید می کند. بنابراین اطمینان از امنیت در انتقال الکترونیکی داده ها و تراکنشها بسیار مهم است. در این مقاله قصد داریم ابعاد مهم امنیت در کسب و کارهای الکترونیک را بررسی نمائیم.

چالش های امنیتی کسب و کارهای الکترونیک و راه‌حل ها

فناوری اطلاعات و علی الخصوص فضای مجازی نقش بسزایی در زندگی امروز بشریت ایفا میکند و گستره فعالیت مجازی به سمت و سویی رفته که امروزه ما شاهد پیشرفت روز افزون کسب و کارهای الکترونیکی در فضای مجازی می باشیم و رونق هر چه بیشتر این کسب و کارها لزوم بهره برداری از امکانات امنیتی در این فضا را پررنگ تر ساخته است [۳]. امروزه امنیت فضای مجازی یکی از پر چالش ترین بحث ها در دنیای فناوری اطلاعات می باشد. مهم ترین و رایج ترین چالش های این حوزه و نحوه مقابل با آنها در ادامه مقاله توصیف شده است.

امنیت در محیط وب و تجارت الکترونیک

کاربران نهایی هنگام استفاده از مرورگرهای وب در معرض خطرات امنیتی، حفظ حریم خصوصی و آسیب‌پذیری‌های مرورگر ها قرار دارند که این منجر به خطر انداختن امنیت مشتری وب است . اطلاعات کاربر را می‌توان جمع‌آوری کرد و پروفایل کاربر را ساخت و درنتیجه، نگرانی‌های جدی حفظ حریم خصوصی را افزایش داد . کوکی‌ها، داده‌های ذخیره شده بر روی دستگاه مشتری هستند و با جابجایی بین سرویس‌گیرنده و سرویس‌دهنده در هنگام اتصال اطلاعات، به‌منظور جمع‌آوری اطلاعات استفاده شوند . یک منبع آسیب‌پذیر در محل مشتری از استفاده مطالب اجرایی در وب مانند: اپلت های جاوا، کنترل‌های اکتیو ایکس و... وجود می‌آید [۴].

بسیاری از سایت‌ها نیز از تکنولوژی تحمیل برای ارائه محتوای وب به مشتریان استفاده می‌کنند. این فرآیند می‌تواند در نقض امنیت تجارت الکترونیک جدی باشد، به دلیل اینکه ارائه‌دهنده محتوا می‌تواند آسیب‌پذیری مرورگر را با ارسال کدهای اجرایی مخرب و با تحمیل کردن حجم بالایی از اطلاعات در بهره‌برداری، امنیت را نقض کند [۵]. سرورهای شبکه مکان‌هایی هستند که بیشتر خدمات شبکه در آن قرار دارند، مانند وب سرور، سرور ایمیل و غیره. تکنولوژی دیوار آتش به محبوب‌ترین روش دفاعی برای این سرویس‌دهنده‌ها در برابر اینترنت نامطمئن و باز، تبدیل شده است . هرچند فایروال می‌تواند از ترافیک غیرقانونی در اینترنت و شبکه های شرکت ها، جلوگیری کند. اما با درخواست‌های قانونی که از فایروال عبور می‌کند ممکن است برای یک حمله مبتنی بر داده در شبکه و یا در پایانه سیستم استفاده شود. پیکربندی فایروال و سرورهای شبکه، نیازمند توانمندی و مستعد خطا است [۶].

این نیاز به محدود کردن و یا کاهش پیچیدگی در فایروال‌ها و شبکه‌ها و مکمل فایروال با قوه امنیتی مبتنی بر میزبان دارد. در شبکه‌های شرکت‌های بزرگ، حمله خودی امنیت اجتماعی در حال رشد است . بنابراین، یک نیاز قوی درحال‌توسعه به مدل‌های جدید کنترل دسترسی و رسیدگی به نیازمندی‌های امنیتی متنوع در وب برنامه‌های کاربردی هستند.

کنترل دسترسی برای کسب و کارهای الکترونیک

زیرساخت‌های کلید عمومی، یک توسعه مهم برای پرداختن به نگرانی های امنیتی برنامه های کاربردی وب بوده است. این واقعیت که حملات خودی تهدیدی قابل‌توجه هستند، بیشتر تأکید نیاز به قوای امنیتی میزبان، برای احراز هویت و کنترل دسترسی خدمات قابل‌توجهی است، که باید در میزبان مستقر شوند . تهدید حمله خودی یک نیاز قوی برای مدیریت امنیت تجارت الکترونیک و مدیریت کارآمد توابع در یک شرکت را بیشتر نشان می‌دهد . امنیت مبتنی بر میزبان همچنین می‌تواند به سرور شبکه و فایروال برای امنیت اینترانت کمک کند [۷].

مدل امنیتی است که اجازه می‌دهد مدیریت امنیت کارآمد شود و مدیریت بتواند برای محیط های چند دامنه، که در آن تعامل میان حوزه‌ها ناهمگن و فشرده بسط داده شود. نمونه برنامه‌های کاربردی محیط چند دامنه عبارت‌اند از: تجارت الکترونیک، پایگاه داده‌های شرکت‌ها و دولت‌های دیجیتال. چنین برنامه‌های کاربردی نیاز به اتصال و همکاری منطقی کسب‌وکار خود در حال حفاظت از اطلاعات حساس دارند. وب در درجه اول از روش ابرمتن برای اشاعه اطلاعات استفاده می‌کند . با رشد برنامه‌های کاربردی تجارت الکترونیکی، وب به‌سرعت به محیط تبادلی و تراکنشی و فعال فشرده تبدیل شده است . برای وب، مدل‌های دسترسی و مکانیزم باید ساده در تغییرات پویا، محتوا و متن اطلاعات باشند، و امکان اجازه نظارت بر حالت سیستم و تسهیل انجام فعالیت‌های معاملاتی روابط را داشته باشند . مدل‌های دسترسی موجود فاقد این ویژگی‌ها هستند [۸].

در مورد سیاست‌های مختلف نیاز است کاربران تنها به اطلاعات مجاز دسترسی داشته باشند . اگرچه چندین تلاش برای توسعه مدل‌های کنترل دسترسی در محیط‌های پایگاه داده‌های سنتی ساخته شده است، اما محیط تجارت الکترونیک کاملاً متفاوت از محیط‌های پایگاه داده سنتی است که چندین مدل مشخص شده دارند . آنچه باعث تفاوت این سامانه با دیگر سامانه‌های نگهداری فایلی می‌شود قابلیت‌های اوست ازجمله: مخفی کردن سخت‌افزار ذخیره سازی از دید برنامه/بازیابی اطلاعات با کمک پرس‌وجوهای پیشرفته/امنیت، یکپارچگی، تهیه پشتیبان، اصلاح خطا/استفاده هم‌زمان و استفاده از راه دور) ها سنتی است. در محیط‌های پایگاه داده‌های معمولی کنترل دسترسی معمولاً برابر مجموعه‌ای از مجوزهای اعلام شده توسط مأموران امنیتی و یا کاربران با توجه به برخی سیاست‌های امنیتی انجام می‌شود. مجوز به‌طورکلی بر اساس سه پارامتر U>، O، <Pمشخص شده است. این مشخص سه گانه است که کاربران U مجاز است تا با امتیاز Pبه شی o دسترسی داشته باشند . چنین الگویی ساده است و برای یک محیط پویا مانند تجارت الکترونیک نیاز به بازنگری داریم و چنین سه‌تایی‌هایی مناسب نیستند . علاوه بر این، در محیط تجارت الکترونیک منابعی که محافظت می‌شوند تنها داده‌های سنتی نیستند، بلکه دانش و تخصص هم است . چنین ویژگی برای انعطاف‌پذیری بیشتر در تعیین سیاست‌های کنترل دسترسی تغییر ایجاد می‌کند. مکانیزم کنترل دسترسی باید به‌اندازه کافی برای پشتیبانی و حفاظت از طیف گسترده‌ای از اشیاء ناهمگن قابل‌انعطاف باشد. دومین نیاز مرتبط پشتیبانی از کنترل دسترسی مبتنی بر محتوا است [۱۰-۹].

کنترل دسترسی مبتنی بر محتوا اجازه می‌دهد تا به بیان سیاست‌های کنترل دسترسی برای حفاظت از محتوایشی بپردازیم. این یک نیاز مهم است از اغلب اشیاء با توجه به نوع و ساختار محتویات مختلف خود درجه‌ای از حساسیت برای حفاظت داشته باشند . به‌منظور حمایت از کنترل دسترسی مبتنی بر محتوا، سیاست‌های کنترل دسترسی باید اجازه دهد که وضعیت در برابر محتوایشی حمایت شود. نیاز سوم مربوط به ناهمگونی افراد است که نیاز به سیاست‌های کنترل دسترسی بر اساس ویژگی‌های کاربر و مدارک آن بر اساس ویژگی‌های بسیار خاص و منحصربه‌فرد (به‌عنوان‌مثال، شناسه کاربر) مربوط، به هرکس است [۱۱].

یک راه حل ممکن، برای توجه بهتر به پروفایل کاربر، تدوین سیاست‌های کنترل دسترسی برای حمایت از تصور گواهی‌نامه . یک گواهی نامه مجموعه‌ای از ویژگی های در مورد یک کاربر و مربوط به اهداف امنیتی است (در یک سازمان به‌عنوان‌مثال، سن، موقعیت، پروژه‌های در حال کاربر). استفاده از گواهی‌نامه اجازه می‌دهد تا مدیر امنیتی به‌طور مستقیم به بیان سیاست‌های امنیتی مرتبط با آن و نزدیک به ساختار سازمانی بپردازد. به‌عنوان‌مثال، با استفاده از گواهی نامه، می‌توان به‌سادگی سیاست‌هایی مانند "کارکنان دائم فقط می‌توانند به اسناد مربوط درون سیستم دسترسی داشته باشند را" تنظیم کند . ما باور داریم که زبان XML می‌تواند نقش کلیدی را در کنترل دسترسی

به برنامه‌های کاربردی تجارت الکترونیک بازی کند. دلیل این است که XML در حال تبدیل شدن به زبان مشترک بین‌المللی برای تبادل سند در سراسر وب، و نیز تبدیل شدن به زبانی برای تجارت الکترونیک است . بنابراین، نیاز به ساخت XML امن، با ارائه مکانیسم‌های کنترل دسترسی به‌طور خاص به حفاظت از اسناد XML طراحی‌شده وجود دارد [۱۲].

از سوی دیگر، اطلاعات کنترل دسترسی (سیاست‌های کنترل دسترسی و گواهی‌نامه کاربر) را می‌توان با استفاده از XML بیان کرد . سرویس دایرکتوری زبان نشانه‌گذاری متن پایه و اساسی را فراهم می‌کند: یک استاندارد برای برقراری ارتباط با خدمات دایرکتوری که مسئول ارائه / تصدیق هویت اعتبار کاربر خواهد بود . این نوع یکنواخت دارای دو قابلیت حفاظت اشیاء و کنترل دسترسی به اطلاعات دارای مزایای متعددی است . اول، سیاست‌های کنترل دسترسی را می‌توان به سیاست‌ها و اعتبار خود اعمال می‌شود . برای مثال، برخی خواص اعتبارنامه (مانند نام کاربری) ممکن است برای همه قابل‌دسترس ساخته شده باشد، درحالی‌که خواص دیگر ممکن است تنها به یک کلاس از کاربران محدود شود و فقط برای بعضی قابل‌مشاهده است . علاوه بر این، استفاده از یک زبان مبتنی بر XML برای تعیین اعتبار و سیاست‌های کنترل دسترسی ثبت اطلاعات کاربری امن و با استفاده از سیاست‌های کنترل دسترسی را تسهیل می‌کند [۱۳].

عناصر امنیتی در کسب و کارهای الکترونیک

استراتژی‌های امنیت تجارت الکترونیک با دو موضوع در ارتباطند: حفاظت از یکپارچگی شبکه کسب‌وکار و سیستم‌های داخلی آن، و ایجاد امنیت در تراکنشات بین مشتری و کسب‌وکار . ابزار اصلی استفاده برای حفاظت از شبکه داخلی کسب‌وکار فایروال است . فایروال یک سخت‌افزار و نرم‌افزار است که اجازه می‌دهد تنها کاربران با ویژگی خاص برای دسترسی به یک شبکه محافظت شده ورود کنند . فایروال در حال حاضر به نقطه اصلی دفاع در معماری امنیت کسب‌وکار تبدیل شده است . بااین‌حال، فایروال باید بخش کوچکی از زیرساخت‌های امنیتی کسب‌وکار باشد . ابزارهای هکری نیز مانند SMTPTUNNEL و ICMPTUNNELوجود دارد که به هکرها اجازه می‌دهند که اطلاعات را از طریق پورت‌های مجاز انتقال دهند [۱۴].

کرم‌های کد قرمز و نیمدا نیز از طریق فایروال وارد می‌شدند چراکه آن‌ها از طریق پورت‌های استاندارد وب سرور به سیستم دسترسی داشتند. امنیت تراکنش برای جذب اعتماد مشتریان در یک سایت تجارت الکترونیک خاص حیاتی است . امنیت تراکنش بستگی به توانایی سازمان برای تضمین حریم خصوصی، تشخیص هویت، جامعیت، در دسترس بودن و جلوگیری از درخواست‌های ناخواسته است . حریم خصوصی تراکنش می‌تواند توسط نرم‌افزارهای نظارت شبکه به‌طور نامشخص مانند برنامه‌های اسنیفر مورد تهدید واقع شود . این برنامه‌ها عموماً در نقطه نهایی ارتباط شبکه یافت می‌شوند. انواع مختلفی از دفاع در مقابل این حملات ازجمله رمزنگاری و توپولوژی‌های چرخشی شبکه وجود دارد . اعتماد و اطمینان تراکنش نیازمند حذف هرگونه مسیریابی تراکنش‌های واقعی و داده‌ها از بین وب‌سایت‌هاست . ضبط پیام‌ها نیز یک بحث مجزاست و نیازمند شناسایی تراکنش واقعی انجام شده است . گره‌های میانی که وظیفه کنترل داده‌های تراکنش را بر عهده دارند نباید داده‌ها را به‌غیراز زمان تراکنش مورداستفاده قرار دهند. رمزنگاری یکی از مطمئن‌ترین روش‌های ایجاد امنیت است. جامعیت تراکنش نیز نیازمند روش‌هایی است که از تغییر تراکنش در هنگام ارسال و دریافت از کاربر جلوگیری می‌کند [۱۵].

کدهای کنترل خطا نیز روشی برای جلوگیری از تغییر تراکنش هستند . روش‌های رمزنگاری مانند کلید مخفی، کلید عمومی و امضای دیجیتال از معمول‌ترین روش‌های حفظ حریم خصوصی تراکنش هستند . از معمول‌ترین ضعف این روش‌ها این است که این‌ها به امنیت نقاط نهایی سیستمها برای حفاظت از تغییر دادن کلیدها وابسته‌اند. همچنین حملات اخیر هکرها هجوم مستقیم به سرور است زیرا آنجا مکان ذخیره داده‌هاست . هرچه مدیران یک سرور باتجربه‌تر و بهتر باشند امکان نفوذ هکرها در آن کمتر است پس هکرها توجه خود را به نفوذ در شبکه و تزریق به شبکه جلب کرده‌اند. آن‌ها قادر به ادامه براندازی سرورها با متوقف کردن جریان ترافیک متن در داخل و خارج از سرور بودند. ترافیک رمزنگاری شبکه، تبدیل شبکه به یک توپولوژی تغییریافته و فیلتر کردن دسترسی ناشناخته برخی از اقدامات متقابل به این حمله اسنیف بود. در پاسخ به این، هکرها به‌سادگی به سمت سرویس‌گیرنده منتقل شدند و این زمانی بود که بسیاری از معماری‌های امنیت شبکه شکست خوردند [۱۶].

ویروس‌ها یک تهدید مزاحم در امنیت تجارت الکترونیک جهان هستند . آن‌ها فقط به خراب کردن عملیات تجارت الکترونیک می‌انجامند و باید به‌عنوان یک ابزار منع سرویس (DOS) نامیده شوند . اسب‌های تروجان برنامه‌های کنترل از راه دور و معادل تجاری آن‌ها نیز از جدی‌ترین خطرات برای تجارت الکترونیک هستند . برنامه‌های اسب تروآ امکان حمله به تمامیت داده‌ها و دست‌کاری سیستم مشتری با نشان دادن خود به‌صورت به‌ظاهر

معتبر را می‌دهند و حل‌وفصل مشکلات ایجاد شده توسط آن‌ها بسیار دشوار است . یک هکر می‌تواند دستورات جعلی را به سیستم یک قربانی و سرور تجارت الکترونیک بدهد که مشخص نباشد جعلی یا واقعی‌اند . حفاظت از رمز عبور، رمزگذاری ارتباطات کلاینت سرور، طرح‌های رمزگذاری کلید عمومی و خصوصی و همه این روش‌ها با یک واقعیت ساده بی‌اثر می‌شوند که برنامه اسب تروجان هکر می‌تواند تمام متن را قبل از رمزگذاری مشاهده کنند. شخص تنها زمانی که هک می‌شود می‌تواند خطر را درک کند . دستورات جعلی یا غیر معتبر به‌حساب به‌عنوان یک‌ششم از همه خرید اقدام در اینترنت است . تهدیدات امنیتی نه‌تنها شامل شکست و اختلال در تکنولوژی هستند، بلکه وسیله، جعل هویت نیز هستند [۱۷].

تهدیدات امنیتی در تجارت الکترونیک و نیازمندی‌ها

نیازمندی‌های امنیتی تجارت الکترونیکی را می‌توان با بررسی روند کلی، شروع از فعالیت‌های مصرف‌کننده تا سرور تجارت موردمطالعه قرار داد . با توجه به هر یک از لینک‌های منطقی در زنجیره تجارت، دارایی که باید از آن محافظت شود اطمینان حاصل کردن از تجارت الکترونیک امن که شامل کامپیوتر سرویس‌گیرنده، پیام کانال‌های ارتباطی، وب و سرورهای تجارت ازجمله هر سخت‌افزار متصل به سرور است . درحالی‌که ارتباطات از راه دور قطعاً یکی از دارایی‌های عمده است که باید محافظت شود، ارتباطات مخابراتی تنها نگرانی در کامپیوتر و تجارت الکترونیک و امنیت نیستند . به‌عنوان‌مثال، اگر ارتباط مخابراتی امن ساخته شد. اما هیچ اقدامات امنیتی برای هر مشتری به اجرا در نیامد کامپیوتر و یا تجارت و سرویس‌دهنده‌های وب، پس‌ازآن هیچ امنیت ارتباطاتی وجود ندارد [۱۸].

تهدیدات سرویس گیرنده

در محتوای ابتدایی وب اجرایی، صفحات وب به‌طور عمده ثابت بود . در HTML کد زده می‌شدند، و صفحات استاتیک می‌توانند قسمت کوچکی از محتوای صفحه‌نمایش را نشان دهد و لینک مرتبط به صفحات با اطلاعات اضافی را ارائه دهد . بااین‌حال، امروزه استفاده گسترده از محتوا تغییر کرده است و به‌صورت فعال درآمده است.

- **محتوای فعال :**محتوای فعال به برنامه‌هایی اطلاق می‌شود که به‌صورت شفاف در صفحات وب تعبیه‌شده‌اند . محتوای فعال می‌تواند گرافیک در حال حرکت، دانلود و بازی صوتی، و یا اجرای برنامه‌های گسترده مبتنی بر وب باشد. محتوای فعال در تجارت الکترونیک برای علاقه‌مندی‌ها و افزودن کالای خرید به یک سبد خرید و محاسبه مقدار فاکتور کل، ازجمله مالیات بر فروش، حمل‌ونقل، و هزینه‌های حمل‌ونقل مورداستفاده قرار می‌گیرد . بهترین و شناخته‌شده‌ترین اشکال محتوای فعال اپلت های جاوا، کنترل‌های اکتیو ایکس، جاوا اسکریپت، و VBScript هستند. ازآنجاکه ماژول محتوای فعال در صفحات وب تعبیه‌شده، می‌توان آن‌ها را به‌طور کامل برای هرکسی که در حال مشاهده یک صفحه حاوی آن‌هاست شفاف باشند . هرکسی می‌تواند محتوای فعال مخرب جاسازی‌شده در صفحات وب را ببیند . کدهای جاسازی‌شده در محتوای فعال صفحات وب که در تجارت الکترونیک هستند خطرات امنیتی را به دنبال دارند . برنامه‌های مخرب بی سروصدا از طریق صفحات وب می‌توانند شماره کارت اعتباری را نشان دهند، نام‌های کاربری، کلمه عبور که غالباً در کوکی‌ها ذخیره‌شده است را نیز نشان دهند . زیرا اینترنت بی‌حدومرز است و نمی‌تواند پاسخ یک نمایش صفحه وب خود را به دیگری به یاد داشته باشد . کوکی‌ها به حل مشکل، به خاطر سپردن اطلاعات مشتری، سفارش و یا نام کاربری و یا کلمه عبور کمک می‌کنند . محتوای فعال خرابکار با استفاده از کوکی‌ها می‌تواند مطالب را از سمت سرویس‌گیرنده و فایل‌ها را نشان دهد یا حتی می‌تواند فایل های ذخیره‌شده بر روی کامپیوتر سرویس‌گیرنده را از بین ببرد [۱۹].

- **کدهای مخرب :**ویروس‌های کامپیوتری، کرم‌ها و اسب‌های تروجان نمونه‌هایی از کدهای مخرب می‌باشد. اسب تروجان برنامه‌ای است که یک تابع مفید است، اما انجام یک اقدام غیرمنتظره است . ویروس یک قطعه کد است که با اتصال به نسخه اجرایی موجود است. یک کرم یک برنامه است که خود را تکرار می‌کند و باعث اجرای نسخه جدید می‌شود. این می‌تواند خطرات را در سمت سرویس‌گیرنده ایجاد کنید.

-**حمله تغییر هویت سمت سرور :**حمله گرهای تغییر قیافه یک قربانی را به باور این‌که نهادی که با آن در ارتباط است یک نهاد متفاوت است وامی‌دارد [۱۹].

تهدید کانال ارتباطی

اینترنت به‌عنوان زنجیره الکترونیکی ارتباط یک مصرف‌کننده (مشتری) به تجارت الکترونیک در خدمت منابع (سرور) است. پیام در اینترنت طی یک مسیر تصادفی از یک گره منبع به گره مقصد می‌رود . پیام از طریق تعدادی از رایانه‌های متوسط در شبکه قبل از رسیدن به مقصد نهایی عبور می‌کند. تضمین این‌که هر کامپیوتر در اینترنت که از طریق آن پیام امن و غیر خصمانه است غیرممکن است.

- **تهدیدات محرمانگی :** محرمانگی جلوگیری از افشای اطلاعات به‌صورت غیرمجاز است. نفوذ در محرمانگی در وب بسیار دشوار است.

- **تهدیدات جامعیت :** وقتی‌که یک حزب غیرمجاز می‌تواند یک جریان پیام از اطلاعات را تغییر دهد تهدید جامعیت نام دارد. معاملات بانکی محافظت نشده در معرض نقض جامعیت هستند . به‌عنوان‌مثال خرابکاری سایبری از نقض جامعیت است. خرابکاری سایبری محو کردن الکترونیکی صفحه وب‌سایت موجود است . تغییر ظاهر و یا spoofing تظاهر به نمایندگی از یک وب‌سایت به‌عنوان وب ا صلی و یا زمانی که آن وب واقعاً جعلی ا ست، یکی از راه‌های ایجاد خرابی در وب‌سایت است . با استفاده از یک حفره امنیتی در سرور نام دامنه(DNS) ، عاملان می‌توانند آدرس وب‌سایت خود را در محل یکی از وب‌سایت‌های واقعی برای بازدیدکنندگان وب‌سایت و کلاه‌برداری جایگزین کنند . تهدید جامعیت می‌تواند مالی، حیاتی، پزشکی، و یا اطلاعات نظامی را تغییر دهد. این می‌تواند عواقب بسیار جدی برای کسب‌وکار و مردم داشته باشد.

-**تهدید در د سترس بودن :** هدف از تهدید در د سترس بودن، انکار و یا تأخیر سرویس و مختل شدن پردازش معمولی کامپیوتر و یا انکار پردازش به‌طور کامل است.

تهدیدات سرور

سرور لینک سوم در سه‌تایی مشتری، اینترنت و سرور ا ست که م سیر تجارت الکترونیک بین کاربر و سرور تجارت ا ست. سرور آ سیب‌پذیر می‌تواند مورد سوءاستفاده توسط هرکسی قرار بگیرد و به‌طور غیرقانونی اطلاعات را به دست آورد.

- **تهدیدات وب سرور :** نرم‌افزار وب سرور برای ارائه صفحات وب با پاسخ به درخواست‌های HTTP طراحی‌شده است. درحالی‌که نرم‌افزار وب سرور ذاتاً در معرض خطر نیست، این با وب‌سرویس به‌عنوان هدف اصلی و طرح اصلی طراحی‌شده است . هرچه نرم‌افزار پیچیده‌تر باشد، احتمال آن‌که شامل خطاهای برنامه‌نویسی، باگ‌ها، حفره‌های امنیتی و نقاط ضعف امنیتی، بالاتر است .

-**تهدید سرور تجارت :** سرور تجارت، همراه با وب سرور، به درخواست از مرورگرهای وب از طریق پروتکل HTTP و اسکریپت CGI پاسخ می‌دهد . چند قطعه نرم‌افزار شامل مجموعه نرم‌افزار سرورهای تجارت، ازجمله سرورFTP ، پست الکترونیکی، سرور ورود از راه دور و سیستم‌عامل بر روی ماشین میزبان وجود دارند. هر یک از این نرم‌افزارها می‌توانند حفره‌های امنیتی و اشکالاتی را داشته باشد.

- **تهدیدات پایگاه داده :** سیستم‌های تجارت الکترونیک داده های کاربر را ذخیره کرده و اطلاعات تولیدی را از پایگاه داده‌های متصل به وب سرور بازیابی می‌کنند . علاوه بر اطلاعات مربوط به محصول، پایگاه داده متصل به وب حاوی اطلاعات ارزشمند و خصوصی است که اگر فاش شد و یا تغییر کرد می‌تواند جبران‌ناپذیر باشد.برخی از بانک اطلاعاتی ذخیره‌شده نام کاربری/رمز عبور غیر امن هستند. اگر کسی اطلاعات احراز هویت کاربران را به دست آورد، و سپس از آن‌ها برای جعل هویت به‌عنوان یک کاربر پایگاه داده مشروع استفاده کرد، فاش شدن اطلاعات خصوصی و پرهزینه است.

- **خطر های رایج دروازه رابط :** رابط دروازه عمومی (CGI) ادوات انتقال اطلاعات از یک وب سرور به یک برنامه دیگر، مانند یک برنامه پایگاه داده را فراهم می‌کند و برنامه‌های انتقال داده‌ها ارائه محتوای فعال به صفحات وب است . ازآنجاکه CGIها برنامه هستند، آن‌ها در حال حاضر یک تهدید امنیتی هستند اگر مورد سوءاستفاده قرار گیرند. درست مثل سرویس‌دهنده‌های وب، اسکریپت‌های CGI می‌توانند مجموعه‌ای اجرا شوند . با امتیازات CGIهای مخرب با دسترسی آزاد به منابع سیستم قادر به غیرفعال کردن سیستم، هستند. برنامه‌های سیستم ممکن است به حذف فایل‌ها، و یا مشاهده اطلاعات مالی و حساس مربوط به مشتری، ازجمله نام‌های کاربری و کلمه عبور اجازه دهند.

- **هک پسورد :** ساده‌ترین حمله به یک سیستم مبتنی بر رمز عبور، حدس زدن کلمه عبور است . حدس زدن کلمه عبور مستلزم آن است که دسترسی به، توابع مکمل و توابع احراز هویت به‌دست‌آمده با شد . اگر هیچ‌یک از این‌ها برای مدت‌زمانی تغییر نکند رمز عبور حدس زده شده است، پس‌ازآن مهاجم می‌تواند رمز عبور را برای دسترسی به سیستم استفاده کند .

Phishing

متداول‌ترین نوع حملات اینترنتی و سرقت هویت در فضای مجازی phishing است که تعداد و پیچیدگی آن ها هم روزبه‌روز در حال افزایش ا ست . آنان می‌گویند که به علت وجود نقص‌های امنیت تجارت الکترونیک در بسیاری از پروتکل‌های email، امکان طرح‌ریزی این حملات به‌سادگی امکان پذیر است . در این نوع حملات، شخص کلاه‌بردار با ارسال نامه‌هایی با سربرگ و ظاهری مشابه با مؤ سسات مالی و اعتباری مشهور از مشترکان خدمات آن‌ها می‌خواهد تا با کلیک کردن روی لینکی

که در نامه موجود است، اطلاعات مربوط به حساب‌های بانکی خود را در بخش‌های مختلف آن وارد کنند [۲۰].

Pharming

در حملات pharming معمولاً کاربران به‌طور ناآگاهانه و بدون آن‌که خودشان بفهمند به‌سوی سایت‌های آلوده هدایت می‌شوند. در این نوع از حمله برخلافphishing ، قربانیان نباید روی لینک موجود در email کلیک کنند تا حمله آغاز شود . قربانیان pharmingحتی متوجه نمی‌شوند که مرورگر آن‌ها در حال باز کردن یک URL غلط ولی مشابه URL واقعی شرکت‌های مالی و اعتباری است . حمله pharmingدر صورتی موفقیت‌آمیز خواهد بود که مهاجمان بتوانند به درون دامنه نام سرور یا DNS نفوذ کنند و آن را تحت کنترل بگیرند DNS .اعدادی را که معادل با آدرس وب‌سایت است، در خود ذخیره می‌کند [۲۱].

حملات محتمل به سیستم های رایانه ای

اتفاقات بدی که در مورد سیستم‌های رایانه‌ای و یا اطلاعات یک سازمان پیش می‌آید و باعث زیان دیدن سازمان می‌گردد (فارغ از عمدی و یا تصادفی بودن اتفاق) حمله نامیده می‌شود. چهار گروه اصلی حمله وجود دارد:

- **حملات دستیابی :**یک حمله دستیابی، نوعی تلاش برای دستیابی مهاجم به اطلاعاتی است که مجاز به دیدن آن‌ها نیست. این حمله در هرجایی که اطلاعات قرار داشته باشد و یا در حال انتقال باشد ممکن است رخ دهد. این نوع حمله، حمله‌ای علیه اعتبار و محرمانه بودن اطلاعات است.

-**حملات ایجاد تغییر :**این نوع حمله، تلاشی برای تغییر اطلاعات است که مهاجم مجاز به انجام نیست. این نوع حمله می‌تواند اطلاعات حساس یا عمومی را مورد هدف قرار دهد.

-**حملات انکار سرویس :**حملات انکار سرویس(DOS) ، حملاتی هستند که کاربران قانونی را از دسترسی به منابع سیستم، اطلاعات یا توانایی‌ها محروم می سازند . حملات DOS معمولاً به مهاجم اجازه دستیابی یا تغییر اطلاعات در سیستم رایانه‌ای یا در دنیای فیزیکی را نمی‌دهد. حملات DOS چیزی جز خرابکاری نیستند.

- **حملات انکاری :**یک حمله انکاری، حمله‌ای علیه جوابگویی سیستم می‌باشد. به‌عبارت‌دیگر، تلاشی برای ارائه دادن اطلاعات غلط می‌باشد .

تغییر قیافه: تغییر قیافه تلاشی برای جا زدن خود به‌جای فردی دیگر یا سیستمی دیگر می‌باشد. این حمله می‌تواند در ارتباطات بین افراد یا در معاملات و یا در ارتباط بین دو سیستم واقع شود.

حریم خصوصی مشتری

سوءاستفاده از حریم خصوصی مشتریان در حال تبدیل شدن به یک نگرانی در سطح مشتری، کسب‌وکار و دولت است . یک مقاومت برای شرکت در انواع خاص معاملات و تراکنش های تجارت الکترونیکی وجود خواهد داشت اگر اطمینان از حفظ حریم خصوصی کم باشد و یا وجود نداشته باشد [۲۲].

سایر خطرات امنیتی و حفظ حریم خصوصی

علاوه بر مواجه با تهدیدات امنیت تجارت الکترونیک و اینترنت در برنامه‌های آنلاین، دستگاه‌های بی‌سیم به معرفی خطرات جدید و خاصی در محیط تحرک و ارتباطاتی خود می‌پردازد .

در نظر بگیرید که دستگاه‌های بی سیم می‌توانند شبکه‌های ad hocرا فرم دهند که در آن مجموعه‌ای از گره‌های تلفن همراه نظیر به نظیر با یکدیگر ارتباط برقرار می‌کنند بدون کمک زیر ساخت و با یک زیربنای ثابت. یکی از معانی شبکه‌های Ad hoc این است که تصمیم‌گیری شبکه غیرمتمرکز است. درنتیجه، پروتکل های شبکه تمایل به همکاری میان تمام گره‌های شرکت‌کننده دارند . دشمن می‌تواند از این اعتماد فرض به سازش کند و از گره بهره‌برداری کند .

اگر ارتباط از دست یک دامنه به بعدی برود، تنها با خراب شدن یک دامنه، دامنه به‌طور بالقوه می‌تواند دستگاه‌های بی سیم را از طریق دریافت مخرب و اطلاعات غلط یا انکار ساده سرویس به خطر بیندازد. اهداف می‌توانند به مهاجمان در شبکه‌های بی‌سیم به‌سادگی با رومینگ از طریق منطقه مهاجم بیایند .

دستگاه‌های بی‌سیم به‌طور بالقوه از شبکه‌های غیرقابل‌اعتماد مختلف که مشتق شده است و خدمات داده‌ای مبادله شده است عبور کنند . بیشتر واسطهای پیاده‌سازی لایه امن سوکت (SSL) و یا همتای بی‌سیم خود (WTLS) انجام احراز هویت اصولی دوباره و یا مجدداً گواهی یک بار اتصال را بررسی نمی‌کنند. مهاجم می‌تواند از این آسیب‌پذیری به نفع خود در شبکه‌های بی‌سیم استفاده کند . هکرهای مضر می‌توانند از اتصالات بی‌سیم سازش حتی بدون بهره‌برداری موقت شبکه‌های همکار در لایه انتقال سوءاستفاده کنند [۲۳].

به‌عنوان یک نتیجه، به‌احتمال‌زیاد حملات از دستگاه‌های بی‌سیم برای حمله به شبکه‌های ثابت راه‌اندازی می‌شوند، به‌ویژه هرچه

توانایی این دستگاه‌های بی‌سیم رشد می‌کند و افزایش می‌یابد خطرات آن‌ها بیشتر می‌شوند.

بدون امنیت تجارت الکترونیک محیط فیزیکی ارائه‌شده توسط ساختمان‌ها، قفل‌ها و نگهبانان د ستگاه‌های محا سبات همراه در معرض خطر سرقت و از دست رفتن هستند، به‌ویژه با توجه به‌اندازه کوچک خود آن‌ها . با استفاده از دستگاه‌های بی‌سیم برای تجارت موبایل آسیب‌پذیری‌های جدید به وجود آمده و به‌طور بالقوه نشان‌دهنده یک پیوند جدید و ضعیف در تجارت الکترونیک ازنظر امنیت است . ازآنجا که حمله تما یل به بهره‌برداری از ضعیف‌ترین حلقه در زنجیره دارد، خطرات امنیتی از دستگاه‌های بی‌سیم نیز باید به‌دقت تجزیه‌وتحلیل شوند.

نتیجه‌گیری

صنعت تجارت الکترونیک در حال توجه به مسائل امنیتی در شبکه اینترنت ا ست .راهنمایی‌هایی برای دا شتن سی ستم‌ها و شبکه‌های امن برای اجرا در سیستم‌های تجارت الکترونیک وجود دارد. کابران عموما در مورد ایمنی و محرمانه بودن اطلاعات خود نگران هستند . برای یک کسب‌وکار مبتنی بر وب برای زنده ماندن و تلاش، باید اطمینان حاصل شود که از حریم خصوصی و امنیت مشتریان محافظت می‌شود. این مانع امنیت تجارت الکترونیک باید تو سط همه احزاب ازجمله دولت، فرو شندگان، و سازمان موردتوجه قرار گیرد. در این مقاله ابعاد امنیتی ک سب و کارهای الکترونیک را بررسی نموده و برخی راهکارهای کلیدی را درجهت بهبود چارچوب های امنیتی سازمان ها و کاربران توصیه نمودیم.

تعارض منافع

هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است.

منابع و مآخذ

[1] Smith J, Carter E. Security Challenges in E-commerce Transactions: Safeguarding the Digital Marketplace. EasyChair; 2024 Jan 3.

[2] Chaudhry RS, Chandhok A. Online Reviews-An effective way to reduce perceived consumer risks of online shopping. In2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) 2024 Feb 24 (pp. 1-6). IEEE.

[3] Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J, Abbas S. Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology. 2022 Oct 19;13:927398.

[4] Kalkha H, Khiat A, Bahnasse A, Ouajji H. The rising trends of smart e-commerce logistics. IEEE Access. 2023 Mar 6;11:33839-57.

[5] Jamra RK, Anggorojati B, Sensuse DI, Suryono RR. Systematic Review of Issues and Solutions for Security in E-commerce. In2020 International Conference on Electrical Engineering and Informatics (ICELTICs) 2020 Oct 27 (pp. 1-5). IEEE.

[6] Mohamad MB, Kanaan AG, Aseh K, Alawi NA, Amayreh KT, Al Moaiad Y, Al-hodiany ZM, Pathmanathan PR, El-Ebiary YA. Enterprise Problems and Proposed Solutions Using the Concept of E-Commerce. In2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) 2021 Jun 15 (pp. 186-192). IEEE.

[7] Taher G. E-commerce: advantages and limitations. International Journal of Academic Research in Accounting Finance and Management Sciences. 2021 Feb;11(1):153-65.

[8] He Y, Hu W. [Retracted] E-Commerce Data Access Control and Encrypted Storage Based on Internet of Things. Mathematical Problems in Engineering. 2022;2022(1):4547002.

[9] Penelova M. Access control models. Cybernetics and Information Technologies. 2021 Dec 1;21(4):77-104.

[10] Omotunde H, Ahmed M. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. Mesopotamian Journal of CyberSecurity. 2023 Aug 7;2023:115-33.

[11] Ravi NC, Muppalaneni NB, Sridevi R, Kamakshi Prasad V, Govardhan A, Padma J. Advanced Access Control Mechanism For Cloud Based E-Wallet. InProceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2018) 2020 (pp. 392-399). Springer International Publishing.

[18] Lyngdoh SW, Chhering M. Cybersecurity Threats and Legal Responsibilities in E-Business: An Indian Perspective. InBusiness Transformation in the Era of Digital Disruption 2025 (pp. 259-292). IGI Global.

[19] Mishra A, Alzoubi YI, Gill AQ, Anwar MJ. Cybersecurity enterprises policies: A comparative study. Sensors. 2022 Jan 11;22(2):538.

[20] Kayumbe A, Michael L. Cyber threats: Can small businesses in tanzania outsmart cybercriminals. International Research Journal of Advanced Engineering and Science. 2021;6(1):141-4.

[21] Jiang B. Computer security vulnerabilities and preventive measures. InApplication of Intelligent Systems in Multi-modal Information Analytics: Proceedings of the 2020 International Conference on Multi-model Information Analytics (MMIA2020), Volume 1 2021 (pp. 752-759). Springer International Publishing.

[22] Yasmeen G, Afaq SA. The critical analysis of E-Commerce web application vulnerabilities. InAdvances in Cyberology and the Advent of the Next-Gen Information Revolution 2023 (pp. 22-37). IGI Global.

[23] Girimurugan B, Dilip D, Bhuvaneswari G, Vegunta D, Swetha Y. Executive Strategies for Implementing Advanced E-Commerce Security Technologies. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 205-228). IGI Global.

[12] LONE SA, MIR A. User Authentication Mechanism for Access Control Management: A Comprehensive Study. International Journal of communication and computer Technologies. 2022;10(2):54-63.

[13] Lian J. Application of Computer Network Security Technology in Electronic Commerce. In2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) 2021 Oct 15 (pp. 691-694). IEEE.

[14] Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J, Abbas S. Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology. 2022 Oct 19;13:927398.

[15] Praveenadevi D, Sathyasundari S, Dakshinamurthy T, Syamala M, Gundapaneni M, Pattnaik M. Cybersecurity Strategies for E-Commerce: Best Practices and Case Studies. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 137-158). IGI Global.

[16] Marta AF, Florescu MS, Coroban L. Risks and Vulnerabilities in Online Commerce. Revista de Management Comparat International. 2023 May 1;24(2):210-27.

[17] Duong PH, Mai DV, Nga VT, Toan TD. A Survey of attacking methods, techniques, and tools on E-commerce systems and recent solutions.