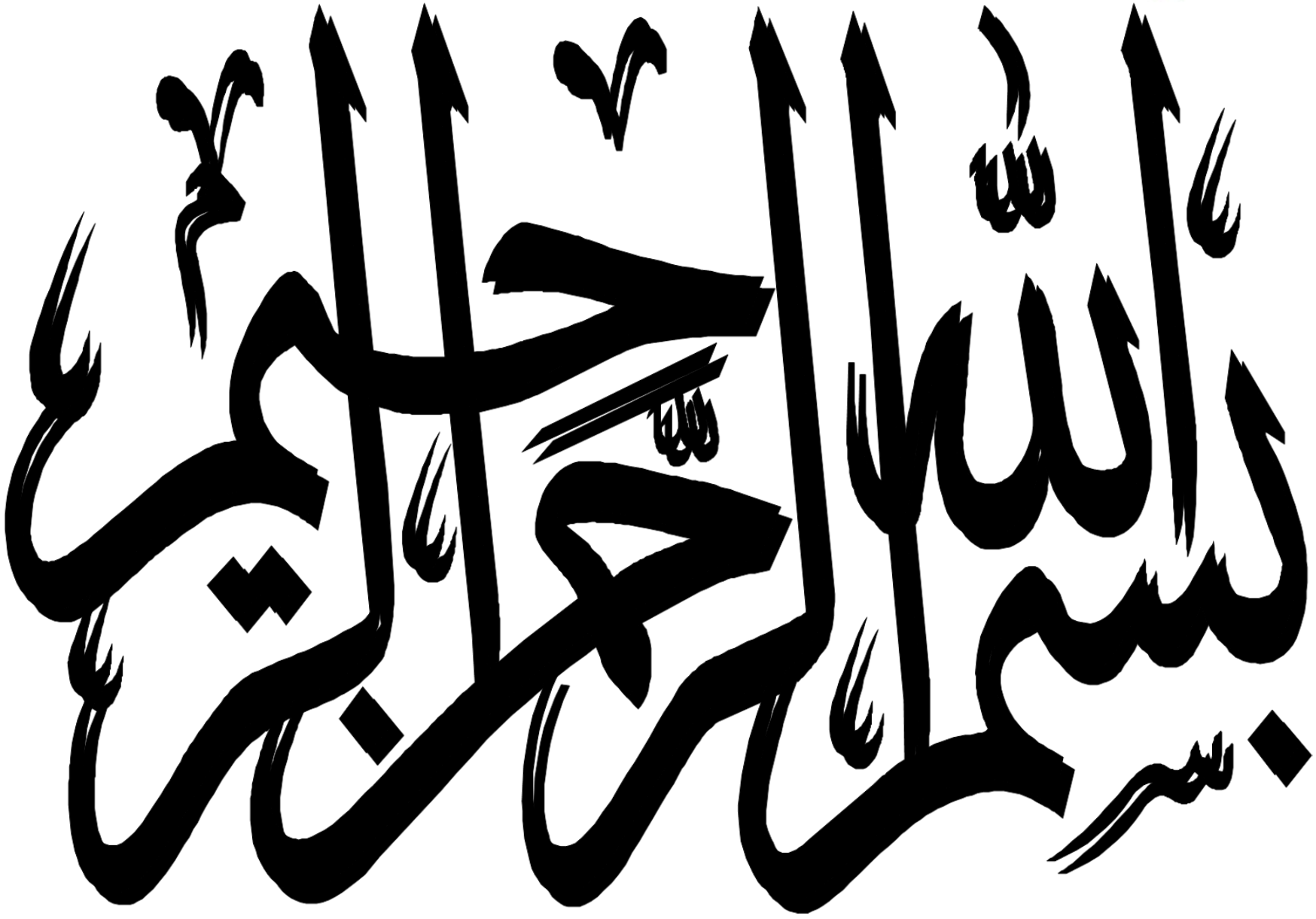

بسم الله الرحمن الرحیم

شناسایی چالشهای امنیتی کارت‌های اعتباری : رویکردی به سوی چالش خدمات نوین الکترونیکی

عبدالنبی کمالی

کارشناس ارشد مدیریت بازرگانی دانشگاه اصفهان

kamalinabi39@gmail.com

بیان مسئله تحقیق

- امروزه فناوری اطلاعات به یکی از مهمترین عناصر محیط استراتژیک سازمان تبدیل شده است طوری که تحولات و تکامل فناوری اطلاعات بیشتر از خود آن، آثار و پیامدهای چشمگیر در سیستم های اقتصادی، اجتماعی و حتی سیاسی دارند .
- از ویژگی های عمومی و جهانی بانکداری الکترونیک می توان به انتقال الکترونیک وجوه، شامل سیستم های پرداخت در سطح خرد و سیستم های مدیریت وجوه نقد مشترک، ماشین های خودپرداز برداشت وجه با قابلیت دسترسی عموم و مدیریت حساب های خرد اشاره کرد .
- افزایش مقبولیت اینترنت در عرصه جهانی به عنوان شیوه انتقال خدمات و محصولات بانکی باعث ایجاد فرصت های تجاری برای بانک ها و برای مشتریان شده است که فعالیتهایی از جمله دسترسی به اطلاعات مالی ودریافت انواع وام ها و ارائه محصولات و خدمات جدید همچون صدور صورتحساب الکترونیک می باشد
- با توجه به مزایای قابل ملاحظه نوآوری های فن آوری و توسعه سریع توانمندی های بانکداری الکترونیک ، روز به روز در حوزه فناوری اطلاعات (در حوزه کارت های اعتباری) تهدیدات و چالش ها فزاینده تر می شود ، لذا شناسایی این گونه چالش ها و مدیریت آنها بر مبنای رویکرد نوین خدمات الکترونیکی بانک ها ضروری است .

هدف تحقیق

- این مقاله به شناسایی آثار ، آسیب ها و چالش های امنیتی کارت های اعتباری در حوزه بانکداری الکترونیک به عنوان مبنایی برای مطالعه برنامه ریزان و رهنمودی برای درک بهتر این آثار می پردازد و به نکات قابل تأمل در مورد امنیت کارت اعتباری در ایران با بهره گیری از مدل پیشنهادی امنیت اطلاعات کارتهای اعتباری اشاره می کند.

اهمیت و ضرورت تحقیق

- ضرورت توجه به سرمایه گذاری آگاهانه و ارزیابی استراتژیک در حوزه بانکداری الکترونیک در کشور با توجه به حجم کلان سرمایه گذاری

- میل بسیار زیاد بانک ها برای صدور این نوع ابزار پرداخت
-
- توجه به نیمه پنهان کارت های اعتباری و مسائل امنیتی و تهدیدات آن برای کشور

طبقه بندی حوزه های اصلی تاثیر پذیر از کارت اعتباری در سازمانهای تجاری

- برخی از آثار به رابطه دولت و شرکتهـــا برمی گردد. این بخش اهمیت نقش دولت در برابر مسایل قانونی و حقوقی بانکداری الکترونیک، مالیات و گمرک و به طورکلی ایجاد فضای سالم کسب و کار را مورد توجه قرار می دهد.

- برخی از آثار شرایط کل افراد جامعه (در سطح کلان) را تحت تاثیر قرار می دهد. این بخش در ادبیات بانکداری الکترونیک مزایا و معایب کلان کارت اعتباری را در جامعه بر می شمارد .

- حوزه هایی که در محیط عمومی سازمانها و فضای کسب و کار برای همه فعالان تجاری و یا شهروندان تاثیر پذیرند و شرایط را برای همه آنان تا حدودی تغییر می دهد.

کارت اعتباری

- پرداخت الکترونیکی در حال حاضر در قالب ابزارهای مختلفی مورد بهره‌برداری قرار می‌گیرد که از آن جمله می‌توان به چک الکترونیکی، پول الکترونیکی، کارت اعتباری، کارت بدهی و غیره اشاره کرد. در این بین با توجه به اهمیتی که کارتهای اعتباری دارد تمرکز خاصی روی این پدیده در بانکداری الکترونیکی خواهد شد.

- کارت اعتباری : کارت اعتباری وسیله‌ای الکترونیکی است که بر اساس اصول فنی خاص و رعایت مسائل ایمنی برای متقاضی صادر می‌شود و دارنده کارت می‌تواند با استفاده از کارت مزبور از طریق ماشینهای خودپرداز و یا نقطه فروش وجوه و یا اعتبار واریز شده به حساب خود را دریافت یا به حساب دیگری منتقل نماید(به نوعی ابزاری برای خرید نسیه است و خریدار با استفاده از این ابزار می تواند کالایی را بدون پرداخت وجه نقد خریداری نماید؛)

انواع کارت های اعتباری

الف) کارت بدهی

ب) کارت هزینه

پ) کارت اعتباری

ت) کارت هوشمند

چالش ها و آسیب شناسی کارت های اعتباری

- از یک منظر یکی از چالش های مهم برای ارائه خدمات مرتبط با کارت های اعتباری ، هزینه دسترسی به منابع مالی است و با توجه به اینکه ارائه این کارت ها می تواند از منابع قرض الحسنه برگرفته باشد ، محدود بودن منابع باعث می شود شبکه بانکی در ارائه این کارت ها با مشکل مواجه شود.

- از منظر دیگر که به طور مفصل توضیح داده خواهد شد ، چالش ها ی کارت اعتباری در قالب حملات نرم افرازی ، سخت افزاری و جانبی نمود پیدا می کند .

چالش ها و آسیب شناسی کارت های اعتباری

کارت های اعتباری بویژه کارت های اعتباری هوشمند با استفاده از روشهای زیر مورد حمله قرار می گیرد

- **الف) اشعه ایکس**
- **ب) میکروسکوپ الکترونی**
- **پ) اغتشاش**
- **ت) کپی برداری**
- **ث) ردیابی**

حملات وارده بر کارت های اعتباری

حملات وارده بر این نوع کارت ها به سه دسته قابل تفکیک است :

- الف) حملات سخت افزاری
- ب) حملات نرم افزاری
- پ) حملات جانبی کانال

حملات سخت افزاری

۱) نوع حملات سخت افزاری

- الف) حملات مخرب
- ب) حملات بد شکل سازی
- پ) حملات غیر هجومی

۲) روش های مشاهده اطلاعات در حملات سخت افزاری

- الف)حلال های شیمیایی
- ب) میکروسکوپ
- پ) استقرار کاوشگر
- ت) حملات نمونه (کاوش فیزیکی رام)

حملات نرم افزاری

- اگر افراد کلاهبردار از مهارت برنامه نویسی برخوردار باشند براحتی خواهند توانست نرم افزار مخربی که می‌تواند در مراحل مختلف حمله نرم افزار استفاده شود طراحی نمایند. بر روی کارت‌های اعتباری هوشمند که توسط جاوا کارت پشتیبانی می‌شود ، این امکان وجود دارد که نرم افزار بارگذاری و اجرا شود

❊ عملکرد مشکل زا

حملات جانبی کانال

- یکی دیگر از حملات کارت اعتباری هوشمند است و زمانی هدایت می‌شود که اطلاعات شروع به پردازش می‌کند. این حملات شامل مشاهده تاثیرات پیش بینی نشده محاسبات است
- چیپ ها برای پردازش برنامه‌ها و یا ارتباط فقط از طریق کانال های مخفیانه طراحی شده اند ولی در محیط های دیگر حساس و آسیب پذیر هستند ؛ این نوع حملات عملکرد چیپ را نسبت به تغییرات فیزیکی بررسی می‌کند .

❊ تاثیر زمان محاسبات

چالش های کارت اعتباری در داخل کشور

کارت های اعتباری بویژه کارت های اعتباری هوشمند با استفاده از روشهای زیر مورد حمله قرار می گیرد

- **الف) چالش کارت اعتباری از منظر بانک ها**
- **ب) چالش کارت اعتباری از منظر اجتماعی**
- **پ) چالش کارت اعتباری از منظر اقتصادی**

مشکلات امنیتی کارت های اعتباری

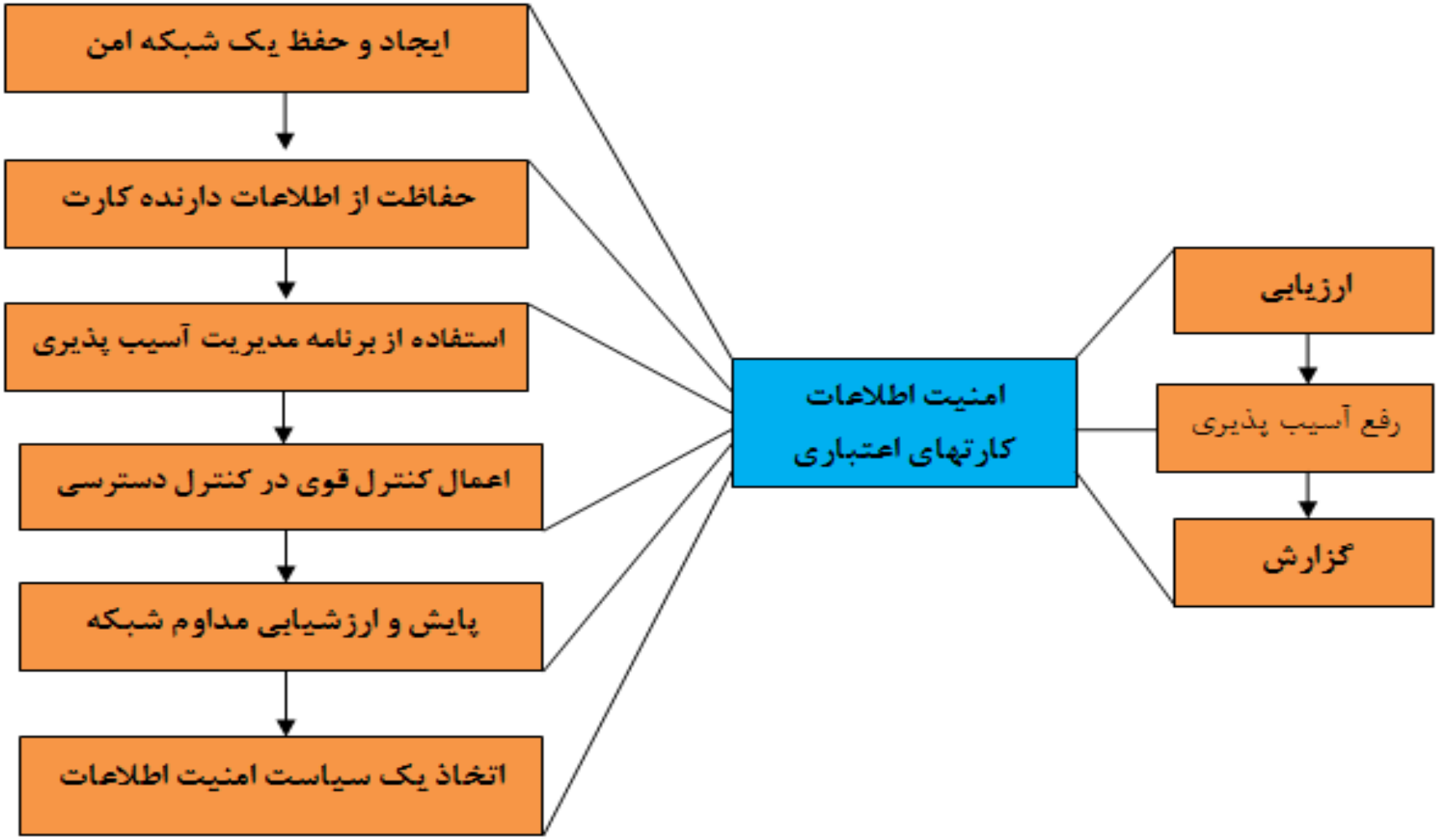
آنچه یک موسسه تجاری در اولین گام امنیتی می بایست مورد توجه قرار دهد بررسی و ارزیابی مسائل امنیتی در شبکه داخلی است . به طور کلی می توان سه مشکل اصلی را از نقطه نظر امنیتی معرفی کرد :

- **الف) کلاهبرداری** : چگونه می توان به مشتری این اطمینان داد که با ورود به سایت و انجام معامله در آن ، شماره رمز کارت اعتباری وی مورد سرقت و جعل قرار نخواهد گرفت ؟
- **ب) استراق سمع کردن** : چگونه می توان به مشتری این اطمینان داد که اطلاعات شماره حساب مشتری زمانی که برای یک معامله امن در وب اقدام می کند قابل دستیابی برای متخلفان نباشد ؟
- **پ) تغییر و تبدیل داده ها** : چگونه می توان اطمینان حاصل نمود که اطلاعات شخصی مشتریان توسط متخلفان قابل تغییر نیست ؟

مدل پیشنهادی تحقیق

- مدل پیشنهادی تحقیق حاضر در چارچوب استاندارد های مربوط به امنیت اطلاعات صنعت کارت های پرداخت قرار می گیرد. این مدل که چارچوبی و مبنای برای امنیت اطلاعات کارتهای اعتباری است که در قالب **۶ اصل و ۱۲ الزام** تفکیک شده است که برای هر کسب و کاری، اعم از فروشندگان، شرکت های ارایه دهنده خدمات کارت و بانک ها که اطلاعات دارندگان کارت های اعتباتری را ذخیره ، پردازش و یا منتقل می کنند، در نظر گرفته است که این ملزومات، یک چارچوب کاری برای محیط امن پرداخت کارتی را تعریف می کند.

مدل پیشنهادی تحقیق



مدل پیشنهادی تحقیق

- بر اساس مدل پیشنهادی تحقیق ، اصل ها و الزامات مدل عبارتند از:

الف) ایجاد و حفظ یک شبکه امن

- الزام ۱ : نصب سیستم های فایروال جهت حفاظت اطلاعات مربوط به دارندگان کارتهای پرداخت الکترونیک
- الزام ۲ : عدم استفاده از تنظیمات پیش فرض انجام شده توسط فروشندگان و سازندگان تجهیزات مانند رمز عبور و دیگر پارمترهای امنیتی

ب) حفاظت از اطلاعات دارنده کارت

- الزام ۳ : محافظت از داده های ذخیره شده مربوط به دارندگان کارت ها
- الزام ۴ : رمز نگاری نقل و انتقال اطلاعات دارندگان کارت ها در شبکه ها

پ) استفاده از برنامه های مدیریت آسیب پذیری

- الزام ۵ : نصب نرم افزار آنتی ویروس و به روز رسانی مداوم آن
- الزام ۶ : توسعه و نگه داری سیستم های ایمن و برنامه های کاربردی امن

مدل پیشنهادی تحقیق

ت) اعمال تمهیدات قوی در کنترل دسترسی ها

- الزام ۷ : محدود کردن دسترسی به اطلاعات دارندگان کارت ها در حداقل احتیاج هر کسب و کار
- الزام ۸ : اختصاص یک شناسه کاربری یکتا به هر یک از کاربران
- الزام ۹ : محدود کردن دسترسی فیزیکی به اطلاعات دارندگان کارت ها

ث) پایش و ارزشیابی مداوم شبکه

- الزام ۱۰ : پایش و ردیابی مداوم هرگونه دسترسی به منابع اطلاعاتی، تجهیزات شبکه و اطلاعات مربوط به دارندگان کارت ها
- الزام ۱۱ : ارزیابی منظم و قاعده مند امنیت سیستم ها و فرآیندهای امنیتی لحاظ شده

ج) اتخاذ یک سیاست امنیت اطلاعات

- الزام ۱۲ : سیاستی اتخاذ شود که خط مشی های امنیت اطلاعات در آن مشخص گردد.

اقدامات اصلی مدل پیشنهادی تحقیق

- **الف) ارزیابی** : فرآیندی که در آن یک فهرست از دارایی های اطلاعاتی و پروسه تجاری مرتبط با فرآیند کارت های اعتباری تهیه شده و از نظر آسیب پذیری هایی که ممکن است اطلاعات شخص دارنده کارت را تحت الشعاع قرار دهد، بررسی می کند.
- **ب) رفع آسیب پذیری** : فرآیند پوشش دهی و رفع آسیب پذیری های امنیتی شناسایی شده در مرحله قبل است که این آسیب پذیری ها ممکن است شامل نقاط ضعف فنی در کد نرم افزار یا اقدامات و رویه های غیر امن پردازش اطلاعات دارنده کارت پرداخت در سازمان باشد
- **پ) گزارش** : جمع بندی سابقه های ثبت شده توسط استاندارد های امنیت اطلاعات کارتهای پرداخت برای کنترل پروسه بازیابی، رفع آسیب پذیری ها و تحویل گزارش های رعایت استاندارد به بانک و شرکت تأمین کننده خدمات کارت پرداخت مورد نظر است که کارهای تجاری با آن انجام می گیرد .

- **این ۱۲ الزام و ۳ اقدام اصلی** ، یک روند مستمر برای انطباق با استاندارد امنیت اطلاعات کارتهای پرداخت است که در نهایت همه آن ها، تضمین کننده امنیت اطلاعات دارنده کارت بوده و به کارگیری این استاندارد می تواند به منزله گام ابتدایی و مهمی باشد که در جهت حفاظت از اطلاعات مشتریان توسط بانک ها، موسسات مالی و سازمان ها برداشته می شود.

نتیجه گیری

- **دستاورد اول :**

با شناخت نقاط ضعف و قوت کارت و نیز شناخت انواع حملات می توان راهکارهای مفیدی برای مقابله با حمله بکارگرفت. یکی از این راه کارهای حفاظت از این کارت‌ها استفاده از رمز نگاری در محتوای اطلاعات ثبت شده روی کارت و یا نمایش آن می‌باشد. برای بالابردن امنیت کارتهای اعتباری ، اولاً مشتریان می توانند در بازده های زمانی مشخص و به صورت دوره ای نسبت به تغییر رمز اول و رمز اینترنتی کارتهای خود اقدام نمایند . ثانیاً مشتریان نباید اطلاعات شخصی کارتهای اعتباری خود را بدون آگاهی از اینکه چه کسی آنها را دریافت می دارد فاش نمایند . ثالثاً افشای اطلاعات شخصی مانند شماره حساب مرتبط با کارت اعتباری کار عاقلانه ای نیست مگر اینکه رمز نگاری شده باشد .

- **دستاورد دوم:**

راهکار یا راه حل دیگر برای جلوگیری از این مشکلات ، استفاده از گواهی دیجیتالی و امضای دیجیتالی درون شبکه ها است که امکان تشخیص صحت و پیوستگی داده ها را فراهم می کند و از الگوی رمز نگاری برای تامین محرمانگی داده ها استفاده می کند .

نکته های ذکر شده در بالا می تواند مشتریان کارت های اعتباری را در مقابل دام ها و حملات سخت افزاری مصون نگه دارد و این اطمینان حاصل کنند که تجربه استفاده از بانکداری الکترونیک برای آنان بسیار امن و لذت بخش تمام شود .

پیشنهادها

- امروزه یکی از سریع ترین و بهترین روش های پرداخت در سراسر جهان ، استفاده از کارت های اعتباری است . در بسیاری کشورها ، کلیه پرداخت های اینترنتی از طریق چند شرکت معتبر که همگان به آن اعتماد دارند و فعالیت شان فقط در زمینه پرداخت های آنلاین می باشد ، انجام می گردد ولی در ایران به دلیل عدم ایجاد امنیت لازم برای این مقوله ، روشی که اغلب مورد استفاده قرار می گیرد ، سفارش کالا به صورت اینترنتی و پرداخت وجه بصورت حضوری به پیک می باشد که مطمئن ترین و ساده ترین روش است . لذا در رابطه می بایست در خصوص استقبال افراد از این کارتهای اعتباری ، امنیت اینترنتی این کارت ها را افزایش داد .

- با توجه به اینکه ممکن است کارت های اعتباری مفقود شود و یا افراد دیگری غیر از دارنده اصلی آن به کارت اعتباری دسترسی داشته باشند ، امکان مسدود نمودن کارت اعتباری و خرید اعتباری از طریق سیستم تلفن بانک و اینترنت بانک در صورت مفقود شدن کارت مهیا شود .

- اگر کارت اعتباری به عنوان یک دغدغه در نهادهای حاکمیتی و نظارتی مطرح باشد ، برای توسعه آن و افزایش ضریب امنیتی دارندگان کارت های اعتباری راهکار پیدا می شود . نقش صاحبنظران و کارشناسان و رسانه ها نیز در توسعه کارت اعتباری مهم است و به موجب آن مردم از این ابزار درستی که می توانند از آن استفاده کنند ، مطلع می شوند و در نتیجه آن را مطالبه می کنند .

پیشنهادها

- فقدان استانداردها و زیرساخت مشترک و همچنین نبود رویکرد استراتژیک برای طراحی نظام اطلاعاتی منسجم بین سازمانی، باعث شده که هر سازمانی تلاش کند سخت افزار و نرم افزار خود را در حوزه از جمله کارت های اعتباری طراحی و اجرا کند. لذا امکان بالقوه ایجاد هماهنگی میان نظامهای مورداستفاده در شرکتها نادیده انگاشته شده است .بنابراین، علاوه بر اینکه بسیاری از سرمایه گذاریها به هدر رفته، هزینه های جدیدی نیز برای ایجاد یکپارچگی مورد نیاز است. این مشکل و ناهماهنگی در بسیاری از موسسات از جمله در بانکها نیز وجود دارد که امر تجارت را با مشکلات جدیدتری مواجه می سازد.

- بانکداری الکترونیک نیازمندیهای فرهنگی خاص خود را می طلبد که اگر این الزامات رعایت نشود ممکن است آسیبهای فرهنگی و اقتصادی به همراه داشته باشد. به عنوان مثال در جامعه ایران هنوز فرهنگ خرید نقدی بسیار پسندیده تر و از لحاظ روحی و روانی مقبول تر از فرهنگ استفاده از کارتهای اعتباری و خرید و فروش به وسیله اینترنت است. به علاوه معمولا خریدار تمایل زیادی به وارسی کردن کالا و آزمایش آن قبل از خرید دارد .لذا آموزشها و قوانین فراوانی باید برای خرید الکترونیک و ایجاد اعتماد برای مشتریان انجام شود.

با تشکر از حُسن توجه شما