فناوریهای تامین امنیت سیستمهای اطلاعاتی، بازاریابی و میزان بکارگیری

فاطمه ثقفی
مربی پژوهشی مرکز تحقیقات مخابرات ایران
دکتر علیرضا علی احمدی
دانشیار دانشگاه علم و صنعت ایران
دکتر محمد فتحیان
استادیار دانشگاه علم و صنعت ایران

چکیده

ظهور تکنولوژی ارتباطات و اینترنت امکان اشتراک اطلاعات و تبادل آسان اطلاعات بین سیستم‌های کامپیوتری را به وجود آورده است. این فناوری‌های نوین بستری مناسب را برای خدمات الکترونیکی از جمله انجام مبادلات تجاری، ارائه خدمات برخط مانند بانکداری و تجارت الکترونیکی ایجاد کرده‌اند. توجه امنیت به اطلاعات به اندازه توسعه و همه‌گیر بودن فناوری اطلاعات اهمیت دارد. لذا امنیت اطلاعات هر کشور یکی از مهمترین عوامل موفقیت در تجارت الکترونیک و به تبع آن بازاریابی الکترونیکی است و تامین آن بطور منطقی بر عهده همان کشور است. نتایج حاصل از یک پژوهش میدانی در مجله امنیت اطلاعات امریکا، نشان می دهد بازار محصولات و خدمات امنیت اطلاعات از سال ۲۰۰۵ با نرخ رشد سالیانه ۲۵٪ مواجه است. با وجود گذشت بیش از یک دهه از تحقیقات امنیت اطلاعات در دنیا، این موضوع در ایران همچنان بکر باقی مانده است. عدم درک و شناخت کافی مسوولین و کاربران از اهمیت و جایگاه مقوله بازار امنیت اطلاعات، رکود بی سابقه بازار شرکت های داخلی فعال در این حوزه را سبب شده است. این مقاله پس از معرفی بازار محصولات امنیتی به بررسی نقش امنیت در اکوسیستم اقتصاد دیجیتال می پردازد. سپس فناورهای امنیتی معرفی و طبقه بندی می شوند. در ادامه بازارهای محصولات و خدمات امنیت اطلاعات در چند کشور نمونه بررسی و تحلیل شده و فروشندگان برتر این محصولات در دنیا، معرفی می شوند. در آخر بازار این محصولات در کشور معرفی و وضعیت بازار امنیت اطلاعات در کشور در مقایسه با دیگران ارائه می شود. با استفاده از نتایج فوق در انتها پیشنهاداتی برای بازار این محصولات در ایران و راهکارهایی برای تحقیقات بازار در این حوزه ارائه خواهد شد.

کلید واژه:

بازاریابی الکترونیکی، امنیت اطلاعات، سهم بازار، محصولات و خدمات امنیت اطلاعات

مقدمه

تا اوایل دهه هفتاد، فعالیت‌های مربوط به دسترسی و محافظت از اطلاعات در سازمانها و شرکت‌ها محدود به محل‌های نگهداری این اطلاعات شامل آرشیو اسناد و شبکه‌های محلی کامپیوتری بود. در چنین محیط‌هایی، روشهای حفاظت فیزیکی امنیت سیستم‌ها و اطلاعات را تا حد بسیار بالایی تأمین می‌کرد. اگرچه مزایای فضای تبادل اطلاعات غیر قابل انکار است، ولی اتصال سیستم‌های داخلی به شبکه‌های خارجی و بین المللی و ارائه خدمات و مبادله اطلاعات از طریق این شبکه‌ها خطرات و تهدیدات جدیدی را ایجاد کرده‌است. مهمترین نگرانی‌های امنیتی مرتبط با سیستم های اطلاعاتی شامل دستیابی نفوذگران به سیستم‌های اطلاعاتی و سرقت اطلاعات آنها، ایجاد وقفه و اختلال در ارائه سرویس‌های حیاتی و تغییر یا تخریب اطلاعات می‌باشند. بدیهی است که در این شرایط روشهای حفاظت فیزیکی به تنهایی قادر به تامین امنیت نخواهند بود. لذا سازمانها ناچار از بکارگرفتن روش‌های جدید حفاظت اطلاعات و کنترل دسترسی‌ها به منابع سازمان شده‌اند. در یک کار پیمایشی که از ۱۱۳۸ متخصص حرفه ای در زمینه امنیت اطلاعات در زمینه محصولات امنیت در سال ۲۰۰۳ انجام شده[۱]، نشان می دهد تا سال ۲۰۰۵ آنتی ویروس، فایروال و VPN در ۹۵٪ سازمانها بکار گرفته شده و مدیریت هویت و جلوگیری از نفوذ، در میان محصولات امنیت از نرخ رشد سالانه ترکیبی (CAGR) معادل ۴۵ و ۴۳ درصد برخوردار خواهند بود. در حالی که در سال ۲۰۰۱ تنها ۷٪ از سازمانها از ابزار تحلیل آسیب پذیری استفاده کرده اند در سال ۲۰۰۵ این نرخ به ۶۰٪ رسیده است. ضمنا بازار خدمات امنیت اطلاعات از نرخ رشد سالانه ترکیبی ۲۵٪ برخوردار خواهد بود. مطالعات میدانی نشان داده که رشد محصولات امنیت در دوسال ۲۰۰۳-۲۰۰۵ دو برابر دوسال قبل آن بوده است. تشخیص نفوذ و روشهای پیشگیری؛ موضوع تازه روز بوده و در سالهای ۲۰۰۱ ال ۲۰۰۵ با نرخ رشد سالانه ترکیبی متجاوز از ۴۰٪ روبرو بوده است. هدف از این مقاله، تبیین جایگاه امنیت اطلاعات؛ بررسی فناوریهای امنیت سیستمهای اطلاعاتی و میزان بکار گیری آنها در کشورهای مختلف جهان است.

۱. اهمیت بررسی بازار امنیت در اکو سیستم اقتصاد دیجیتال

دراقتصاد دیجیتال ارتباط بین تولیدکنندگان و مصرف‌کنندگان بیشتر و فاصله بین آنها کمتر میشود. مشتری‌گرایی بیشتر و محصولات وخدمات کاملا سفارشی و مبتنی بر سلایق مشتریان ارائه می‌شود. لذا امنیت اطلاعات و ریسک حاصل از آن در این جامعه از اهمیت بالایی برخوردار بوده و هر کشوری باید بتواند مدیریت آن را عهده دار شود. در دست گرفتن بازار در این حوزه باعث تفوق شبکه ای و اعمال نفوذهای مختلف سیاسی در کشورها خواهد شد. پاسخ اغلب سازمان‌ها در مواجهه با تهدیدات امنیتی، خرید محصولات امنیتی مانند فایروال و برنامه‌های ضدویروس، و بکارگیری آنها در سیستم‌های کامپیوتری، استفاده از سیستمهای مدیریت امنیت اطلاعات (ISMS) است. اما استفاده از گرانقیمت‌ترین محصولات امنیتی بدون شناخت و تحلیل دقیق نیازهای امنیتی ،استفاده از روالهای استاندارد در بکارگیری و کنترل سیستم های امنیتی و بروز رسانی مداوم این سیستم‌ها به تنهائی کارساز نخواهند بود. این سیستم به مدیران امکان می دهد تا بتوانند امنیت سیستم های خود را با به حداقل رساندن ریسک‌های تجاری کنترل کنند. یک سیستم جامع امنیتی بر سه پایه بنا می‌شود:

سیاستها و دستورالعملهای امنیتی : طرحها و برنامه‌های مرتبط برای نحوه محافظت از سیستم‌های اطلاعاتی و داده‌های آنها در این قسمت مورد توجه قرار می گیرد. استراتژی امنیتی در دو بخش غیرفنی و فنی ارائه می شود. بخش غیرفنی شامل تعیین سطوح امنیتی مطلوب و انتخاب استانداردهای امنیتی و بخش فنی شامل تهیه دستورالعملهای لازم برای بکارگیری و نظارت بر اجزای سیستم امنیتی جهت نیل به اهداف استراتژیک می‌باشد .

تکنولوژی و محصولات امنیتی: این قسمت شامل تمام ابزارهای مورد استفاده در بخش‌های مختلف امنیتی برای اعمال دستورالعملها، کنترل و نظارت می‌باشد. ابزارهای محافظتی و نظارت بر شبکه، سیستم‌های کنترل دسترسی و راهکارهای ضدویروس در این بخش مطرح می شوند.

عوامل اجرایی: افراد مرتبط با مدیریت و اجرای سیستم امنیتی شامل مدیران سیستم‌ها و شبکه‌ها، پرسنل و کاربران عادی در این قسمت جای دارند. این عوامل از تکنولوژی و ابزارها در جهت اجرای سیاستها و دستورالعملهای امنیتی استفاده می‌کنند.

ملاحظه می شود با توجه به نفوذ غیر قابل انکار شبکه های ICT در زندگی مردم، مقوله امنیت اطلاعات زیر بنای آینده اقتصادی یک جامعه محسوب می شود. لذا در ادامه حوزه های امنیتی، محصولات، خدمات و بازارها و فروشندگان عمده یا به عبارتی رقبای جهانی ایران در این زمینه بررسی خواهد شد.

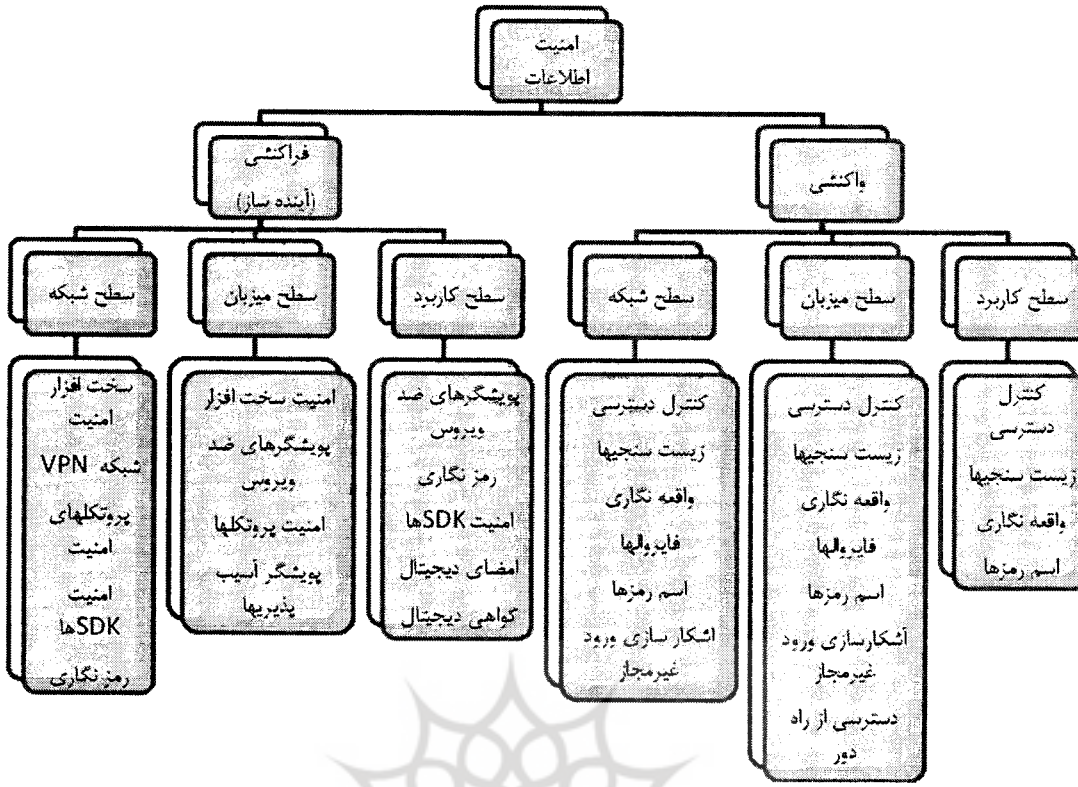
۲. طبقه بندي فناوري‌هاي حوزه امنيت اطلاعات

امنیت اطلاعات[1] به حفاظت از اطلاعات[۲] و به حداقل‌رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد.[۳] امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است.[۴] با توجه به تعاریف ارائه شده، امنیت به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی اطلاق می‌شود. فن آوری به کاربرد علم، خصوصاً برای اهداف صنعتی و تجاری[۵] یا به دانش و روش‌های مورد استفاده برای تولید یک محصول گفته می‌شود. بنابراین فناوری امنیت اطلاعات به بهره‌گیری مناسب از تمام فناوری‌های امنیتی پیشرفته برای حفاظت از تمام اطلاعات احتمالی روی اینترنت اشاره دارد.[۶]

برای شناخت این حوزه مطابق شکل(۱) یک طبقه بندی از فناوری‌های امنیت اطلاعات با دو ویژگی زیر ارائه می شود:

۱) براساس مرحله خاصی از زمان: بدین معنا که در زمان تعامل فن آوری با اطلاعات، عکس العمل لازم در برابر یک مشکل امنیتی می تواند فراکنشی یا پیش دستانه[2] یا واکنشی[3] باشد.[۷] منظور از فراکنشی ، انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی و منظور از واکنشی انجام عکس‌العمل لازم پس از وقوع یک مشکل خاص امنیتی است.

۲) براساس سطوح پیاده‌سازی نظام های امنیتی در یک محیط رایانه‌ای: فناوری امنیت اطلاعات را، خواه از نوع فراکنشی باشد یا واکنشی، می‌توان در سه سطح، سطح شبکه[4]، سطح میزبان[5] و سطح برنامه کاربردی[6] پیاده‌سازی کرد. بدین منظور می‌توان نظام امنیتی را نیز در همان سه سطح پیاده کرد.



شکل(۱)طبقه بندی فناوریهای امنیت اطلاعات

۲ . ۱ . فناوري‌هاي امنيت اطلاعات فراكنشي يا پيش دستانه

۲ . ۱ . ۱ . رمزنگاري[۷]

رمزنگاری به معنای نوشتن پنهان، و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌ها است[۱۱]. این علم شامل اعمال رمزگذاری، رمزگشایی و تحلیل رمز است. رمزنگاری با تمام جوانب پیام‌رسانی امن، تعیین اعتبار، امضاهای دیجیتال، پول الکترونیکی و نرم افزارهای کاربردی دیگر ارتباط دارد. رمزنگاری یک فناوری امنیت اطلاعات از نوع فراکنشی است، زیرا اطلاعات را قبل از آن که یک تهدید بالقوه بتواند اعمال خرابکارانه انجام دهد، از طریق رمزگذاری داده‌ها ایمن می‌سازند. به علاوه، رمزنگاری در سطوح برنامه‌های کاربردی و در سطوح شبکه قابل پیاده‌سازی است.

۲ . ۱ . ۲ . امضاهاي ديجيتال[۸]

امضاهای دیجیتال، معادل امضای دست‌نوشت و مبتنی بر همان هدف هستند: نشانه منحصر به فرد یک شخص، با یک بدنه متنی[۹]. است و نباید قابل جعل باشد. این فناوری که با استفاده از الگوریتم رمزنگاری ایجاد می‌شود، تصدیق رمزگذاری‌شده‌ای است که معمولاً به یک پیام پست الکترونیکی یا یک گواهی‌نامه ضمیمه می‌شود تا هویت واقعی تولیدکننده پیام را تأیید کند. امضای دیجیتال یک فناوری امنیت اطلاعات از نوع فراکنشی است، زیرا قبل از وقوع هر تهدیدی، می‌توان با استفاده از آن فرستنده اصلی پیام و صاحب امضا را شناسایی کرد. به علاوه این فناوری در سطح یک برنامه کاربردی قابل پیاده‌سازی است.

۲. ۱. ۳. گواهی‌های دیجیتال[۹]

گواهی‌های دیجیتال به حل مسئله اطمینان در اینترنت کمک می‌کنند. گواهی‌های دیجیتال به متصدی‌های گواهی اشاره دارند. متصدی‌های گواهی، مؤسسات تجاری هستند که هویت افراد یا سازمان‌ها را در وب تأیید، و تأییدیه‌هایی مبنی بر درستی این هویت‌ها صادر می‌کنند. این گواهی‌ها حاوی نام فرد، شماره سریال، تاریخ انقضا، یک نسخه از گواهی نگاهدارنده کلید عمومی هستند[۱۲]. گواهی‌های دیجیتال، فناوری امنیت اطلاعات از نوع فراکنشی هستند، زیرا از این فناوری برای توزیع کلید عمومی از یک گروه ارتباطی به گروه ارتباطی دیگر استفاده می‌شود.

۲. ۱. ٤. شبکه‌های مجازی خصوصی[۱۰]

فناوری شبکه‌های مجازی خصوصی، عبور و مرور شبکه را رمزگذاری می‌کند. بنابراین این فناوری برای تضمین صحت و امنیت داده‌ها، به رمزنگاری وابسته است. این شبکه بسیار امن، برای انتقال داده‌های حساس (از جمله اطلاعات تجاری الکترونیکی) از اینترنت به عنوان رسانه انتقال بهره می‌گیرد. شبکه‌های مجازی خصوصی، فناوری امنیت اطلاعات از نوع فراکنشی هستند، زیرا داده‌ها قبل از آن که در شبکه عمومی منتشر شوند، با رمزگذاری محافظت می‌شوند و این باعث می‌شود که تنها افراد مجاز قادر به خواندن اطلاعات باشند.

۲. ۱. ٥. نرم‌افزارهای آسیب شناسی[۱۱]

نرم‌افزارهای آسیب شناسی برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا سیستم یا سایت و به عبارتی یک نمونه خاص از نظام آشکارساز نفوذی از فناوری امنیت اطلاعات هستند[۱۴]. این نرم‌افزارها میزبان‌های روی شبکه را در فواصل خاص و نه بطور پیوسته، پویش می‌کنند. به مجرد این که یک نرم‌افزار آسیب‌شناسی بررسی یک میزبان را خاتمه داد، داده‌ها در درون یک گزارش، نمونه‌برداری می‌شوند، که به یک عکس فوری (**snapshot**) شباهت دارد (مثل: **cisco secure scanner**). نرم‌افزارهای آسیب شناسی، فناوری امنیت اطلاعات از نوع فراکنشی هستند و از آن‌ها برای کشف عامل‌های نفوذی قبل از آن که بتوانند با عملیات‌های خرابکارانه از اطلاعات سوء استفاده کنند، استفاده می‌شود.

۲. ۱. ٦. پویشگرهای ضد ویروس[۱۲]

در دهه‌های گذشته ویروس‌های رایانه‌ای باعث تخریب عظیمی در اینترنت شده‌اند. ویروس رایانه‌ای یک قطعه مخرب نرم‌افزاری است که توانایی تکثیر خودش را در سراسر اینترنت، با یک بار فعال‌شدن، دارد[۱۷]. اعمالی که پویشگرهای ضد ویروس انجام می‌دهند عبارت‌اند از: ۱) ممانعت از فعالیت ویروس، ۲) حذف ویروس، ۳) تعمیر آسیبی که ویروس عامل آن بوده است، و ۴) گرفتن ویروس در زمان کنترل و بعد از فعال‌شدن آن پویشگر ضدویروس، یک فناوری امنیت اطلاعات از نوع فراکنشی است. این پویشگرها در سطح برنامه‌های کاربردی و در سطح میزبان، قابل پیاده‌سازی هستند.

۲. ۱. ۷. پروتکل‌های امنیتی[۱۳]

پروتکل‌ها فناوری‌هایی هستند که از یک روش استاندارد برای انتقال منظم داده‌ها بین رایانه‌ها استفاده می‌کنند، یا مجموعه‌ای از مقررات یا قراردادها هستند که تبادل اطلاعات را میان نظام‌های رایانه‌ای، کنترل و هدایت می‌کنند. پروتکل‌های امنیتی، یک فناوری امنیت اطلاعات از نوع فراکنشی هستند، زیرا برای حفاظت از اطلاعات حساس از یک پروتکل خاص امنیتی، قبل از آن که اطلاعات به وسیله خرابکاران به دست آید، استفاده می‌کنند. این فناوری در سطوح مختلف؛ سطح برنامه کاربردی و سطح شبکه قابل پیاده‌سازی است.

۲. ۱. ۸. سخت افزارهای امنیتی[۱٤]

سخت افزار امنیتی به ابزارهای فیزیکی که کاربرد امنیتی دارند، اشاره می‌کند؛ مانند معیارهای رمزگذاری سخت‌افزاری یا مسیریاب‌های سخت‌افزاری. ابزارهای امنیت فیزیکی شامل امنیت سرورها، امنیت کابل‌ها، سیستم‌های هشداردهنده امنیتی در زمان دسترسی غیرمجاز یا ذخیره فایل‌ها بعد از استفاده یا گرفتن فایل پشتیبان هستند. این فناوری یک فناوری امنیت اطلاعات از نوع فراکنشی است، زیرا داده‌ها را قبل از آن که تهدید بالقوه‌ای بتواند تحقق یابد، حفاظت می‌کنند.

۲. ۱. ۹. جعبه‌های توسعه نرم‌افزار امنیتی[۱۵]

جعبه‌های توسعه نرم‌افزار امنیتی، ابزارهای برنامه‌نویسی هستند که در ایجاد برنامه‌های امنیتی مورد استفاده قرار می‌گیرند. Microsoft.net SDKs نمونهٔ نرم‌افزار ساخت برنامه‌های کاربردی امنیتی (مانند برنامه‌های تعیین اعتبار مبتنی بر وب) است. این جعبه‌ها شامل سازنده صفحه تصویری، یک ویراستار، یک مترجم، یک پیونددهنده، و امکانات دیگر هستند. جعبه‌های توسعه نرم‌افزار امنیتی، فناوری امنیت اطلاعات از نوع فراکنشی هستند، زیرا از آن‌ها در توسعه نرم افزارهای متنوع برنامه‌های کاربردی امنیتی (که داده‌ها را قبل از آن که تهدید بالقوه تحقق یابد، حفاظت می‌کنند) استفاده می‌شوند.

۲. ۲. فناوری‌های امنیت اطلاعات واکنشی

۲. ۲. ۱. دیوار آتش[۱۶]

دیوار آتش در اینترنت یک ابزار نرم‌افزاری، خصوصاً روی یک رایانه پیکربندی‌شده می‌باشد که به عنوان مانع، فیلتر یا گلوگاه بین یک سازمان داخلی یا شبکه امین و شبکه غیرامین یا اینترنت، نصب می‌شود[۱۸]. هدف از دیوار آتش جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکه داخلی سازمان یا میزبان است[۱۹]. دیوار آتش به عنوان اولین خط دفاعی در تلاش برای راندن عامل مزاحم، مورد توجه قرار می‌گیرد. دیوار آتش بین نظام‌های سازمان و اینترنت قرار می‌گیرد. دیوار آتش یک فناوری امنیت اطلاعات از نوع واکنشی است و مهم‌ترین ابزار امنیتی مورد استفاده برای کنترل ارتباطات شبکه‌ای بین دو سازمان که به یکدیگر اعتماد ندارند، می‌باشد.

۲. ۲. ۲. کنترل دسترسی[۱۷]

کنترل دسترسی به مجموعه سیاست‌ها و اقدامات مربوط به دادن اجازه یا ندادن اجازه برای دسترسی یک کاربر خاص به منابع، یا محدودکردن دسترسی به منابع نظام‌های اطلاعاتی برای کاربران، برنامه‌ها، پردازه‌ها یا دیگر سیستم‌های مجاز اطلاق می‌شود. هدف از این فناوری، حصول اطمینان است از این که کاربر نوعی، حقوق کافی برای انجام عملیات‌های خاص روی سیستم را دارد[۲۰]. کنترل دسترسی از نوع واکنشی است، زیرا دسترسی به یک نظام را به محض این که یک درخواست دسترسی صورت گیرد، مجاز یا غیرمجاز می شمارد.

۲. ۲. ۳. اسم رمز عبور[۱۸]

اسم رمز یا کلمه عبور، یک کلمه، عبارت یا حروف متوالی رمزی است که فرد برای به‌دست آوردن جواز دسترسی به اطلاعات باید وارد نماید. این کلمه برای شناسایی و برای اهداف امنیتی در یک نظام رایانه‌ای به کار می‌رود. کلمه عبور، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به‌منظور گرفتن مجوز و دسترسی به نظام، به محض این که یک فرد یا فرایند بخواهد به یک برنامه کاربردی، میزبان یا شبکه متصل شود، به کار می‌رود.

۲. ۲. ۴. زیست‌سنجی[۱۹]

زیست‌سنجی، علم و فناوری سنجش و تحلیل‌داده‌های زیستی است. در فناوری اطلاعات، زیست‌سنجی معمولاً به فناوری‌هایی برای سنجش و تحلیل ویژگی‌های بدن انسان (مانند اثر انگشت، قرنیه و شبکیه چشم، الگوهای صدا، الگوهای چهره، و اندازه‌های دست) خصوصاً به‌منظور تعیین اعتبار اشاره دارد. زیست‌سنجی فناوری امنیت اطلاعات از نوع واکنشی است، زیرا از آن می‌توان با استفاده از ویژگیهای بخشی از بدن کاربر برای گرفتن مجوز استفاده نمود.

۲. ۲. ۵. نظام‌های آشکارساز نفوذی[۲۰]

نظام‌های آشکارساز نفوذی، یک نظام تدافعی است که فعالیت‌های خصمانه را در یک شبکه تشخیص و از ادامه آنها ممانعت بعمل آورد.این ابزارها می‌توانند بین تهاجم‌های داخلی از داخل سازمان (کارمندان یا مشتریان) و تهاجم‌های خارجی (حملاتی که توسط هکرها انجام می‌شود) تمایز قایل شوند (مثل Cisco IDS). این فناوری از نوع واکنشی است، زیرا از آن برای کنترل میزبان‌های روی شبکه، آشکارسازی، ثبت گزارش، و متوقف ساختن هر نوع حمله و استفاده غیرقانونی استفاده می‌شود.

۲. ۲. ۶. واقعه‌نگاری[۲۱]

واقعه‌نگاری به ثبت اعمال یا تراکنش‌های انجام‌شده توسط کاربر یا یک برنامه، تولید سابقه، و ثبت نظام‌مند رویدادهای مشخص به ترتیب وقوع آن‌ها برای فراهم‌کردن امکان تعقیب و پیگیری داده‌ها در تحلیل‌های آتی اطلاق می‌شود. واقعه‌نگاری، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به علت‌جویی حوادث امنیتی بعد از وقوع می‌پردازد. این فناوری در سطوح برنامه کاربردی، میزبان و شبکه قابل پیاده‌سازی است.

۲. ۲. ۷. دسترسی از راه دور[۲۲]

دسترسی از راه دور به دسترسی به یک سیستم یا برنامه، بدون نیاز به حضور فیزیکی در محل توجه دارد. با این حال معمولاً دسترسی به خدمات از راه دور، کنترل‌شده نیستند، زیرا ممکن است دسترسی به یک خدمت از راه دور به طور ناشناس صورت بگیرد که در این مورد دسترسی به خدمت، خطر جعل هویت را به همراه دارد. دسترسی از راه دور، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا یک فرد یا فرایند برای اتصال از راه دور، قادر به دستیابی بر طبق امتیازات دسترسی می‌باشد.

۳. بررسی بازار امنیت اطلاعات در کشورهای نمونه (امریکا، تایوان و کره) و معرفی فروشندگان جهانی

۳. ۱. بازار امنیت اطلاعات امریکا [۱۵]

بازار خدمات و محصولات امنیت اطلاعات امریکا هر ساله ۱۹٪ تا سال ۲۰۰۸ رشد خواهد کرد و درسال ۲۰۰۸ به ۲۰ میلیارد دلار خواهد رسید. افزایش رشد بلند مدت در اثر تلاشهای سازمانی برای ایجاد سکوهای[۲۳] امنیت اطلاعات یکپارچه در سراسر سازمان بوجود خواهد آمد. این تلاشها دو هدف زیر را توامان دنبال خواهد کرد:

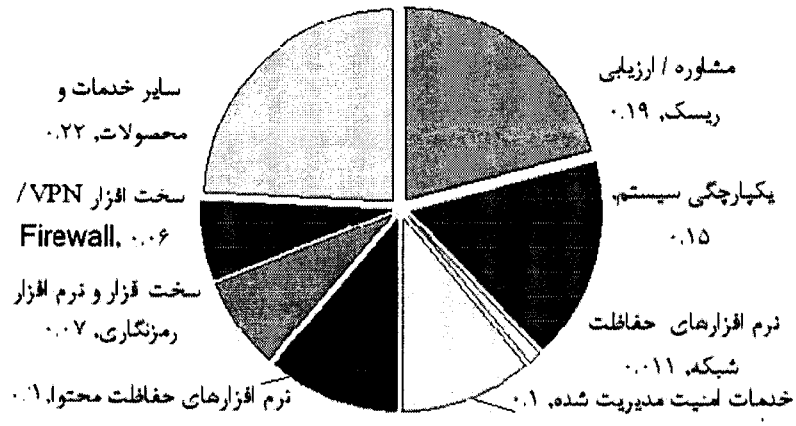
- افزایش حفاظت
- ساده سازی عملکرد و مدیریت عملکرد امنیت در این راستا

در تمام بخشهای عمده از جمله سخت افزار، نرم افزار و خدمات رشد زیادی مورد انتظار است. در این میان محصولات و خدمات سطح بالا که در آن کیفیت بدون توجه به قیمت آن حرف اول را می زند، مانند خدمات امنیت مدیریت شده و ارزیابی ریسک، رشد بسیار زیادی خواهد داشت. در سایر حوزه ها مانند: سخت افزار رمزنگاری(کارتهای شتابدهنده سرور، اسمارت کارتها و ...)، کنترلهای دسترسی بیومتریک، نرم افزارهای حفاظت از محتوا(مخصوصا ابزارهای فیلتر کردن اسپم)، نرم افزار و سخت افزار VPN و نرم افزار مدیریت امنیت از رشد بالقوه متوسطی برخوردار خواهد بود. مهار تهدیدات امنیتی با ریسک بالا به عنوان نقطه بلوغ صنعت در نظر گرفته می شود. لازم به ذکر است؛ بازار امنیت اطلاعات به عنوان یک بخش، رشد اصلی خود را از نیمه دوم دهه ۱۹۹۰م، وقتی که سازمانها به ایجاد حفاظتهای امنیتی قوی برای اینترانت های داخلی و سیستمهای تجارت الکترونیک خود روی آورده بودند، آغاز کرد. بدیهی است سرمایه گذاری در آینده بر تهدیدات با ریسک بالا متمرکز خواهد شد.

صنعت امنیت اطلاعات در دهه ۲۰۰۰ برای تغییر ساختار و یکپارچه سازی، هزینه زیادی را صرف کرده است. به عنوان مثال شرکتهای بزرگی مانند VeriSign و Symantec برای تصاحب بیشتر سهم بازار و تبدیل شدن به فروشندگان رتبه اول بازار و تامین نظر فروشندگان در سال ۲۰۰۲ تا ۲۰۰۳ دست به تجدید ساختار زدند در شکل(۲) پیش بینی بازار خدمات و محصولات امنیت اطلاعات امریکا در سال ۲۰۰۸ ملاحظه می شود. حجم مالی این بازار ۲۰/۵ میلیارد دلار برآورد شده است.

طبقه بندی محصولات و خدمات امنیت اطلاعات امریکا به شرح زیر است:

محصولات مبتنی بر سخت افزار	نرم افزار رمز نگاری(زیر ساخت کلید عمومی(PKI) و سایر)
سخت افزار VPN و فایروال	نرم افزار حفاظت از اسم رمز
کنترلهای دسترسی(مبتنی بر کارت- بیومتریک و سایر)	نرم افزار امنیت ارتباطات
سخت افزار رمز نگاری(کارتهای شتابدهنده سرور[۲۴] و سایر)	نرم افزار مدیریت امنیت
تجهیزات امنیت تلفن	خدمات امنیت اطلاعات
سایر سخت افزارها	مشاوره (ارزیابی ریسک / یکپارچگی سیستم /ارزش
نرم افزارهای حفاظت شبکه(فایروالها_ شبکه های خصوصی مجازی VPN- سایر)	افزوده)
نرم افزارهای حفاظت از محتوا(آنتی ویروس/ فیلتر اسپم و...)	دوباره فروشی
	خدمات امنیت مدیریت شده
	سایر خدمات



شکل(۳) بازار خدمات و محصولات امنیت اطلاعات امریکا در سال ۲۰۰۸

۳ .۲. بازار امنیت اطلاعات کره

طبقه بندی محصولات کره بر اساس نظر دفتر نمایندگی دولت و شرکتهای عمومی کره بیان شده است. سپس مروری بر محصولات و خدمات، درجه رضایت از آنها و سطح سرمایه گذاری برای سیستمها و محصولات امنیتی انجام شده است. منظور از این مطالعه کشف وضعیت کنونی صنعت امنیت اطلاعات در کره و استراتژیهای حمایت از توسعه آنها برای جهانی شدن از سوی دولت است. امنیت اطلاعات معنایی مدیریتی و فنی دارد. امنیت اطلاعات از خطرات، نوسان و طغیان اطلاعات در حال جمع آوری، پروسه ذخیره سازی، جستجو و انتقال دریافت اطلاعات به دیگری، جلوگیری می کند. صنعت امنیت اطلاعات محصولات سخت افزاریH/W یا نرم افزاریS/W و خدمات امنیت اطلاعات را توسعه می دهد. در این مطالعه، سطح نفوذ این محصولات و خدمات در کره تعیین می شود. برای انجام این مطالعه ۱۷۸ نهاد از ۵ آوریل ۲۰۰۳ تا ۳۰ می ۲۰۰۳ مطالعه شده اند. در این پیمایش شرکتهای دولتی، بانکها، موسسات مالی و شرکتهای عمومی بررسی شده است[۱۶].

جدول (۱) طبقه بندی محصولات و خدمات امنیت در کره

کلاس		تعریف / عملکرد
محصولات	آنتی ویروس	خواندن ویروسهای کامپیوتر و جبران مشکلات ناشی از وجود ویروس درپاک کردن کامپیوتر
	فایروال	مسدود کردن نفوذ غیرقانونی از شبکه بیرونی S/W یا H/W
	IDS	تشخیص برخط نفوذ غیرمجاز از شبکه بیرونی یا استفاده غیرقانونی در اینترانت
	تصدیق هویت	تعیین صحت گواهی کاربر S/W: رمز عبور و امضای الکترونیک H/W : بیومتریک و کارت IC
	رمزنگاری	رمز نگاری محتواهای فایلها در برابر استفاده از آنها در اینترانت
	VPN	شبکه خصوصی مجازی: ایجاد عملکرد خط خصوصی با ایجاد تونلی در شبکه عمومی
	PKI	چارچوب تصدیق هویتی که صحت، امنیت و عدم انکار مستند الکترونیکی را در شبکه بازی مانند اینترنت تضمین کند
	OS امن	کرنل امنیتی که دسترسی به ضعفهای حفاظتی OS را تنظیم می کند در سطحی که کرنل نفوذ غیر مجاز به شبکه را مانع شده و مسدود می نماید.
	امنیت محتواها	تعیین محتواها ی در برگرفته پست الکترونیکی و ترافیک WEB و حفاظت از محتواها و کدهای بداندیش[۲۵]
	مدیریت امنیت	تحلیل نقاط ضعیف سیستمهای امنیتی بااستفاده از نظارت بر بسته ها و بازرسی ضعفها با ابزار تحلیل ریسک، ابزار تحلیل ضعفها، تحلیلگر بسته (packet)، اسکنر
خدمات	مشاوره	مشاوره و پشتیبانی فنی مدیریت و کاربرد سیستمهای امن
	تصدیق هویت	خدماتی برای تعیین تصدیق هویت واقعی کاربر به عنوان موسسه تصدیق کننده هویت
	کنترل	برونسپاری کارهای مرتبط با امنیت به یک شرکت امنیتی

مختصری از پیمایش: محصولات و خدمات متنوعی که برای کاهش خطرات توسعه داده شده اند می توانند در سه دسته بندی زیر قرار گیرند:

فاز اول حفاظت(فاز حفاظتی): آنتی ویروس و فایروال

فاز حفاظت از جریان اطلاعات (فاز جریان محور): زیرساخت کلید عمومی(PKI)، شبکه خصوصی مجازی(VPN).

فاز سوم(فاز تطبیقی): وقتی رخنه ای در فازهای قبلی ایجاد می شود شامل سیستم تشخیص نفوذ (IDS)، امنیت محتواها و مدیریت امنیت و ...

محصولات و خدمات امنیت اطلاعات کره در جدول(۱) طبقه بندی شده اند. بر اساس این طبقه بندی مطالعه پیمایشی از ماه جولای تا سپتامبر برای ۴۰۰ نهاد و شرکت انجام شد. قبل از انجام پیمایش، شرکتها و نهادها به ۵ گروه ۱- نمایندگیهای دولتی ۲- شرکتهای عمومی ۳- موسسات مالی و بانکها ۴- شرکتهای خصوصی که بصورت برخط کار می کنند ۵- شرکتهای خصوصی عادی تقسیم شدند. از ۴۰۰ نمونه فوق، تعداد ۱۷۸ مرکز به سوالات پاسخ دادند که تعداد و فراوانی در جدول(۲) نوشته شده است.

بازار امنیت اطلاعات کره از سال ۲۰۰۰ تا سال ۲۰۰۷ معادل ۱۹/۵٪ رشد خواهد کرد و حجم بازار آن از ۴۰۰۰ bnwon به ۷۰۰۰ bnwon خواهد رسید. بزرگترین بازار سال ۲۰۰۲ به فایروال و سیستمهای تشخیص نفوذ اختصاص داشت. بازار فایروال ۶/۷٪ و بازار IDS ۲۲/۱٪ رشد خواهد کرد.

جدول(۲) تعداد پاسخهای جمع آوری شده در پیمایش از مراکز مختلف

نهادها	تعداد/ سهم
نمایندگیهای دولتی GA[۲۶]	۳۲(٪۱۸)
شرکتهای عمومی PC[۲۷]	۳۱(٪۱۷/۴)
موسسات مالی و بانکها BFC[۲۸]	۳۰(٪۱۶/۹)
شرکتهای خصوصی که بصورت برخط کار می کنند. PCBO[۲۹]	۳۰(٪۱۶/۹)
شرکتهای خصوصی عادی GPC[۳۰]	۵۵(٪۳۰/۹)

جدول(۳) نفوذ محصولات و خدمات در هر بخش

	GA(۳۲)		PC(۳۱)		BFC(۳۰)		PCBO(۳۰)		GPC(۵۵)		کل(۱۷۸)	
	استفاده	تعداد	استفاده	تعداد	استفاده	تعداد	استفاده	تعداد	استفاده	تعداد	استفاده	تعداد
ضد ویروس	۳۲	۰	۳۱	۰	۳۰	۰	۲۴	۶	۵۲	۳	۱۶۹	۹
فایروال	۳۱	۱	۲۵	۶	۲۸	۲	۲۲	۸	۲۲	۳۳	۱۲۸	۵۰
IDS	۱۹	۱۳	۱۳	۱۸	۲۴	۶	۷	۲۳	۸	۴۷	۷۱	۱۰۷
تصدیق هویت	۸	۲۴	۹	۲۲	۱	۱۴	۷	۲۳	۱۱	۴۴	۵۱	۱۲۷
رمز نگاری	۸	۲۴	۴	۲۷	۱۹	۱۱	۸	۲۲	۷	۴۸	۴۶	۱۳۲
VPN	۱۱	۲۱	۱۱	۲۱	۴۸	۲۲	۶	۲۴	۱۳	۴۲	۴۹	۱۲۹
PKI	۵	۲۷	۴	۲۷	۱۳	۱۷	۱	۲۹	۲	۵۳	۲۵	۱۵۳۴
Secure OS	۱۱	۲۱	۱۰	۲۱	۱۴	۱۶	۴	۲۶	۷	۴۸	۴۶	۱۳۲
محتوای امنیت	۱	۳۱	۱	۳۰	۱	۲۹	۰	۳۰	۰	۵۵	۳	۱۷۵
مدیریت امنیت	۹	۲۳	۱	۳۰	۱۲	۱۸	۰	۳۰	۰	۵۵	۲۲	۱۵۶
مشاوره	۹	۲۳	۵	۲۶	۱۳	۱۷	۴	۲۶	۱	۵۴	۳۲	۱۴۶
تصدیق	۵	۲۷	۶	۲۵	۷	۲۳	۱۴	۱۶	۶	۴۹	۳۸	۱۴۰
کنترل	۲	۳۰	۰	۳۱	۴	۲۶	۷	۲۳	۰	۵۵	۱۳	۱۶۵

نفوذ و رضایت از محصولات و خدمات امنیت در کره: جدول (۳) خلاصه ای از نفوذ محصولات و خدمات در هر بخش را نشان می دهد.۹۴/۹٪ از نهادها از آنتی ویروس استفاده کرده اند. بعد از آنتی ویروس، فایروال با ۷۱/۹٪ بالاترین رتبه نفوذ در بازار را به خود اختصاص داده است. به جز دو محصول بالا سایر محصولات نفوذ زیادی در بازار ندارند. بخصوص امنیت محتواها و خدمات کنترل امنیت بندرت استفاده می‌شوند و بترتیب از ۱/۷٪ و ۷/۳٪ نفوذ برخوردارند. این مسئله بیان می کند که اغلب نهادها علاقمند به حفاظت امنیت فاز ۱ هستند.

همانطور که در جدول دیده می شود، شرکتهای مالی بانکی روی تعداد محصولات بیشتری نسبت به سایرین سرمایه گذاری کرده‌اند. از ۱۳ محصول و خدمت معرفی شده، ۵ مورد بالای ۵۰٪ هستند. در بخش شرکتهای خصوصی، صرفنظر از نوع کار، آنتی ویروس تنها موردی است که بیش از ۵۰٪ شرکتها بکار برده اند. این نهادها علاقمندی بیشتری نسبت به تامین امنیت فاز ۱ نشان داده اند. لذا می توان استنتاج کرد که فعال سازی یک کسب و کار امن هزینه و زمان زیادی را می طلبد.

نسبت هزینه مدیریت سیستم شبکه

جدول (۴) خلاصه ای از هزینه های مدیریت سیستم شبکه را نشان می دهند. جواب ۰ تا ۵٪ در مجموع ۴۱/۶٪ است و این نتیجه بیان می کند که هزینه مدیریت سیستم شبکه بطور غیر مستقیم پایین است. ضمنا جواب بیش از ۴۰٪ نیز صفر است.

جدول(۴)نسبت هزینه مدیریت سیستم شبکه

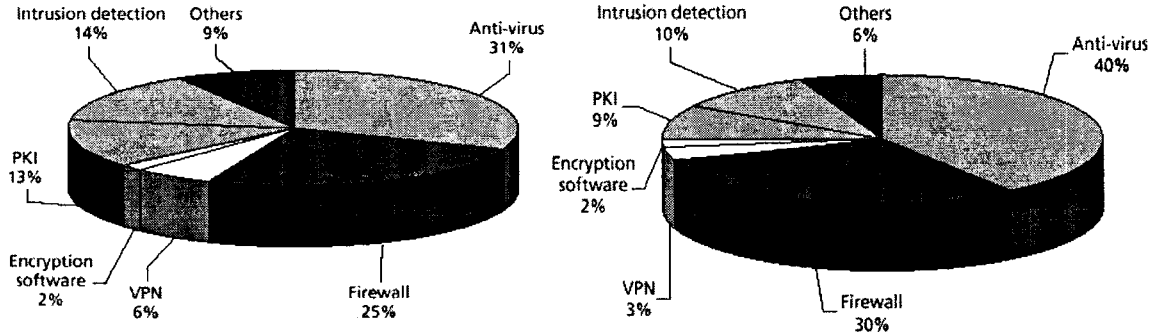
	٪۵	٪۱۰-٪۵	٪۲۰-٪۱۰	٪۳۰-٪۲۰	٪۴۰-٪۳۰	جمع
GA	۱۱,۸	۳,۹	۰	۲,۲	۰	۱۸
PC	۱۱,۸	۲,۸	۰,۶	۲,۲	۱,۸۲	۱۷,۴
BFC	۱,۷	۳,۹	۶,۷	۴,۵	۰	۱۶,۹
PCBO	۲,۲	۳,۹	۲۰,۲	۳,۴	۵,۱	۱۶,۹
CPC	۱۴	۱۱,۸	۲,۸	۲,۲	۰	۳۰,۹
جمع کل	۴۱,۶	۲۶,۴	۱۲,۴	۱۳,۵	۶,۲	۱۰۰

درسهای برگرفته از کره و راه هدف گذاری سازمانی : همه تولید کننده گان راه حل در بازار IT، فهمیده اند که بهترین راه برای ماکزیمم کردن فروش محصولاتشان، آن است که هر چه سریعتر از رقبا، به درکی عمیق از نیازهای مشتریان دست یابند. در حالی که بیشتر فروشندگان احساس می کنند بیشترین تاثیر پیامدهای امنیتی همه سازمانها و فروشندگان راه حلهای امنیتی، یک پیامد افقی است، دیدگاه خدمات حرفه ای همیشه به سازمانها در اولویت بندی ریسکها و حفاظت از حوزه های سرمایه گذاری IT که ماموریتی بحرانی دارند کمک کرده است. یکی از این روشها، ازمون محیط بازار در جایی که یک سازمان کار می کند، است. شرکتهای نمونه در یک بازار عمودی معین، فرایندهای داخلی مشابهی داشته و خواهان رویارویی با فناوریها و فشارهای رقابتی هستند. با درک نیازهای کاری این شرکتها و اینکه کدام فناوری بیشتر بکار برده می شود، یک ارائه دهنده راه حل امنیتی (بازاریاب مدرن این رشته)باید از درک یک مشتری بالقوه نسبت به راه حل امنیتی که از ایجاد بحران برای سرمایه ای که روی محصول گذاشته حفاظت کند مطمئن شود. امروزه فروشندگان کمی می توانند این سطح را برای پشتیبانی از مشتری خود پیشنهاد کنند. فروشندگان عمدتا تواناییهای خود را برای سازگاری بیشتر با نیازهای مشتریانشان با توسعه استراتژی عمودی شده، افزایش می دهند. سازمانها با یک بازار عمودی معین از ریسکهای مشابهی رنج می برند. ضمنا اهداف مشابهی داشته و نیازمند راه حلهای IT مشابهی برای فعالیتهای خود هستند. بازارهای محصولات امنیت سازمانی با توجه به روند افزایشی آگاهی سازمانهای بزرگ و کوچک برای بهبود امنیت سیستمهای IT توجه زیادی را به خود جلب کرده است. در کره، ۵٪ کل بودجه به هزینه استقرار و مدیریت سیستم شبکه کامپیوتر تخصیص یافته است. ۸۲/۵٪ از سازمانها، در زمینه امنیت اطلاعات سرمایه گذاری کرده اند.

۳ . ۳.بازار امنیت اطلاعات تایوان

بر اساس مطالعه انجام شده[۱۷] در سال ۲۰۰۱، بعد از چند سال برنامه ریزی، تایوان در زمینه امنیت اطلاعات، تجربه و مهارت قابل ملاحظه ای بدست آورده است. با توجه به پیوستن روزمره افراد به استفادکنندگان از اینترنتی، دولت و کمپانیهای تجاری سرمایه گذاری بیشتری در زمینه نیروی انسانی و سایر منابع خود را به این بخش اختصاص می دهند. هدف آنها اطمینان از پیشی گرفتن تایوان در استفاده از IT و تولید کننده محصولات و خدمات IT از رقبا است. بعنوان یک تولید کننده و مصرف کننده محصولات و خدمات امنیت اطلاعات ، تایوان جایگاه در حال رشدی در اقتصاد جهانی دارد. سرمایه گذاری بیشتر در سایر نواحی زمینه های اطلاعات و گسترش انواع و تعداد محصولات تولیدی و مصرفی از آرزوهای تایوان است.

کاربردهای صنعتی و حجم بازار : در سال سال ۲۰۰۳ بازار امنیت اطلاعات در تایوان در حدود ۷/۵ میلیارد دلار تایوان و معادل ۰/۲۱ میلیارد دلار امریکا بود. در بخش فروش خانگی طبق برآورد مرکز هوشمند بازار صنعت اطلاعات تایوان(MIC) انجام شده، در سال گذشته ۲۵٪ افزایش داشته است[۱۸]. در همین زمان محصولات امنیت اطلاعات ۳۰٪ رشد داشته و خدمات نیز ۳۹٪ رشد داشته است. MIC در کل پیش بینی می کند بازار امنیت اطلاعات سالانه ۲۵٪ رشد داشته و در سال ۲۰۰۴ به ۱۰ میلیارد دلار تایوان رسیده است. در سال ۲۰۰۵ خدمات ۴۵٪ از بازار کل را به خود اختصاص داده است. در سال ۲۰۰۱ محصولات خاص مانند نرم افزارهای آنتی ویروس و فایروال بر بازار امنیت اطلاعات تایوان چیره شدند(شکل ۳ سمت راست). گرچه بازار فایروال و آنتی ویروس کماکان در سال ۲۰۰۴ نیز به عنوان بازار غالب بوده، سایر محصولات امنیت اطلاعات نیز به رشد خود در بازار ادامه داده اند.(شکل ۳ سمت چپ)



شکل (۳ سمت راست) انواع محصولات عرضه شده توسط فروشندگان محصولات اطلاعات تایوانی در سال ۲۰۰۱ و سمت چپ بازار محصولات اطلاعات تایوانی در سال ۲۰۰۴ [۱۹]

توسعه زیر ساخت کلید عمومی(PKI) از نظر تعیین اینکه آیا تایوان می تواند دسترسی اینترنتی قابل اطمینان، امن و گسترده ای را در سالهای اتی ایجاد کند بسیار مهم خواهد بود لذا دولت ۳۰/۵ میلیارد دلار تایوانی روی پروژه دیجیتال تایوان سرمایه گذاری نمود[۲۰]. هدف پروژه آن است که ۳۰۰ میلیون گواهی شخصی طبیعی[۳۱] یا نوعی ID کارت اینترنتی را منتشر کند و ارتباط بین المللی بین تایوان و دیگر کشور های آسیایی، اروپاو شمال و جنوب امریکا را برقرار سازد. اگر تایوانیها یک مدل مناسب تجاری بر اساس مشخصات محصولات و مزیتهای آنها را توسعه دهند؛ زیرساخت کلید عمومی وابسته به صنایع در تایوان بطور فزاینده ای باعث ترقی محبوبیت تجارت الکترونیکی خواهد شد. در تایوان شرکتهای خصوصی و خریداران؛ بجای تمرکز بر مارک تجاری، تمایل دارند بر تواناییهای کاربردی PKI -که اکنون رهبر مشخصی نیز ندارد- تاکید کنند. به این ترتیب صنایع PKI در تایوان منابع بیشتری را برای توسعه محصولات سرمایه گذاری خوا هد کرد.

محصولات امنیت اطلاعات : از بین محصولات متنوع امنیت اطلاعات، فایروالها بیشترین سرمایه گذاری را جذب کرده اند و تنها اندکی از کمپانیهای تایوانی چنین نرم افزاری را توسعه داده اند. بررسی درصد سهم از کل بازار نشان می دهد، سهم بازار فایروالهای نرم افزاری از ۵۷٪ در سال ۲۰۰۰ به ۴۴٪ در سال ۲۰۰۱ کاهش یافته است. در صورتی که در مقام مقایسه، سهم بازار فایروالهای سخت افزاری از ۴۳٪ در سال ۲۰۰۰ به ۵۶٪ در سال ۲۰۰۱ افزایش یافته است. در مجموع، بازار فایروال در سال ۲۰۰۱ در تایوان حدود ۹۱۰ میلیون دلار تایوانی بوده است. بخاطر گسترش جهانی ویروسها، اشخاص و صنایع بر توسعه نرم افزارهای ضد ویروس تاکید دارند(به عنوان مثال پیوستن Trend Micro به Chunghwa Telecom.[۲۱]). توسعه نرم افزارهای ضد ویروس در تایوان بر توسعه محصولات برای کامپیوترهای رومیزی و اینترفیس بین گیت وی ها و سرورها تاکید دارد.

برای انعطاف پذیری و ملاحظات قیمت، IP_VPN یک راه حل مرجح برای محرمانگی اطلاعات صنایع،مخصوصا صنعت مخابرات است. بودجه برای خرید محصولات VPN محور برای پشتیبانی از محرمانگی اطلاعات افزایش داشته است. هرچند با توجه به جدول(۵)، نرخ رشد متوسط است. این امر ناشی از تاثیر قابل قبول محرمانگی و کسادی اقتصاد است.

تشخیص نفوذ، بویژه محصولات نظارت ۲۴ ساعته آن، برای کسب و کارهایی که تصدیق می کنند بدون اجازه وارد شبکه آنها شدن ریسک زیادی دارد، بسیار جذاب است. لازم است حساسیت و دقت محصولاتی که در حال حاضر توسط فروشندگان تایوانی در بازار عرضه می شوند بهبود یابد. اکنون بازار نرم افزار رمزنگاری در حدود ۷۰ میلیون دلار تایوان است. هر چند این بازار در آینده کاهش خواهد یافت زیرا شرکتها تمایل دارند بجای اینکه یک رمز نگاری را بصورت یک محصول مستقل[۳۲] در دست داشته باشند آن را نیز در کنار سایر قابلیتهای کاربردی محصول خود ایجاد نمایند.

جدول(۵) بازار محصولات امنیت تایوان[۲۲]

نوع محصولات	بازار ۲۰۰۱(برحسب میلیون NT)	بازار ۲۰۰۲(برحسب میلیون NT)	درصد رشد
فایروالها	۹۱۰	۱۱۰۷	۲۲,۹
آنتی ویروس	۱۱۸۰	۱۴۳۹	۲۲
VPN	۹۷	۱۳۵	۳۹,۲
رمزنگاری	۶۱	۷۲	۱۸
زیرساخت کلید عمومی	۱۶۲	۲۰۸	۲۸,۴
آشکار سازی نفوذ غیرمجاز	۳۱۰	۵۱۶	۶۶,۵
تخمین امنیت	۹۵	۱۷۵	۸۴,۲

خدمات امنیت اطلاعات : در مارس ۲۰۰۳،MIC گزارشی در زمینه روند مدیریت امنیت اطلاعات منتشر نمود. این گزارش پیش بینی نموده که صنعت مالی بزرگترین تقاضا را برای امنیت اطلاعات خواهد داشت و میلیاردها دلار در سال ۲۰۰۳ در این زمینه خرج خواهد کرد. خدمات امنیت اطلاعات : صدور گواهی،مشاوره، یکپارچگی سیستم و تخمین امنیت را شامل می شوند. جدول(۶) بازار خدمات امنیت را نشان می دهد. همچنین مقدار سهم فروش به شرکتها و افراد را که نشان دهنده سهم توسعه یافتگی هر بازار در تایوان است را جداگانه نشان می دهد.

جدول(۶) بازار خدمات امنیت تایوان

خدمات	بازار ۲۰۰۱(برحسب میلیون NT)	بازار ۲۰۰۲(برحسب میلیون NT)	درصد رشد
صدور گواهی	۹۱	۱۲۹	۴۱,۸
مشاوره	۲۴۳	۴۲۳	۷۴,۱
یکپارچه سازی سیستمها	۱,۱۸۹	۱,۵۶۷	۳۱,۸

رمز نگاری کلید عمومی که نیازمند به شخص ثالث معتمد دارد و مرجع گواهی۳۳ نامیده می شود؛ برای تعیین ارتباط صحیح بین نام و کلید عمومی است. تاسیس یک مرجع گواهی اصلی دولتی به عنوان نقطه عطفی در توسعه این خدمات در تایوان است. نمونه ای از مراجع گواهی دهنده خصوصی در تایوان عبارتند از[۲۳، ۲۴، ۲۵] : سایر نمایندگیهای دولتی؛به عنوان نمایندگان امنیت اطلاعات حمایت شده دولتی تایوان، شرکتها را در تشخیص نفوذ یاری می‌دهند. برای کاربرانی که محصولات تخمین امنیت را برای تعیین وجود رخنه در سیستم خود بکار می برند، نرم افزار کار چک‌آپ سلامت سیستم را انجام می دهد. تخمین امنیت برای هر چند دفعه که نفوذ رخ می دهد نباید استفاده شود. این نرم افزار در سطح جزئیات کار می کند. چون این محصول در زمره محصولات جدید است، صنایع آن را به عنوان یک خدمت در نظر گرفته و سعی می کنند استفاده از ان را به تدریج افزایش دهند. محصولات و خدمات تخمین امنیت در حال حاضر سهم بازار یکسانی دارند. بسیاری از شرکتها خدمات یکپارچگی سیستم را برای یکپارچه سازی کاربردها یا شبکه ها استفاده می کنند. خدمات یکپارچه سازی کاربردها از رواج بیشتری برخوردار بوده و ۷۳٪ از سهم بازار ۱,۴ میلیارد دلاری(دلار تایوان) را در سال ۲۰۰۱ در تایوان به خود اختصاص داده است. یکپارچه سازی تدریجی شبکه امنیت روی این بازار اثر خواهد گذاشت. علاوه بر این، انگیزه اولیه برای هزینه های یکپارچگی سیستم به کاربری محصولات امنیتی وابسته به کلید عمومی مرتبط است. توضیحات فوق کمک می کند که دلیل اینکه چرا محصولات PKI تنها ۱۰٪ درامد بازار محصولات و خدمات مرتبط با کلید عمومی را علیرغم وجود پتانسیل لازم در این بازار، به خود تخصیص داده را بخوبی بیان نماید. این درصد پایین از این واقعیت ناشی می شود که صنایع PKI وابسته به یکپارچگی کاربردها نیازمند هزینه های سنگینی برای یکپارچه کردن سیستم هستند.

اساسا شرکتها در پرداخت هزینه های سنگین برای خرید سخت افزار(یکپارچه سازی شبکه) به کندی عمل می کنند ولی در پرداخت هزینه های کم(یکپارچه سازی کاربردها) راحتتر هزینه می کنند. در تایوان PKI بزرگترین محرک یکپارچگی کاربردها است. به عنوان بخشی از پروژه دیجیتال تایوان، تایوان تلاش میکند که بیش از ۶ میلیون کاربر اتصال اینترنتی باند پهن، برای دیجیتالی کردن دولت، صنعت و کنترل ترافیک داشته باشد موسسه صنایع اطلاعاتی تخمین می زند که این پروژه بازار امنیت اطلاعات تایوان را از ۵,۰۷ میلیارد دلار تایوانی در سال ۲۰۰۱ به ۲۴/۲ میلیارد دلار در سال ۲۰۰۷ خواهد رساند. لذا نرخ رشد ترکیبی ۲۹/۸ درصد در سال خواهد بود. این بهره تجاری بزرگ باعث ورود فعال بسیاری از صنایع در این عرصه خواهد شد و اطلاعات کارآمدی برای پشتیبانی از امنیت اطلاعات و خدمات امنیت اطلاعات یکپارچه بوجود خواهد آورد. بیشترشدن راه‌حلهای امنیت اطلاعات دولت باعث تقاضای بیشتر امنیت اطلاعات شخصی می شود. این پدیده

باعث تشویق دانشگاهها به ارائه درسهای مرتبط شده و اساتید بیشتری خود را وقف این کار خواهند کرد.لذا بطور غیر مستقیم باعث افزایش کیفیت پرسنل و قدرت تایوان در گسترش امنیت اطلاعات می شود. با توجه به این اوضاع ناگوار شرکتهای IT، یکپارچگی صنایع در عرصه امنیت اطلاعات یکی از چند داستان موفقیت خواهد بود.

۳. ٤. وضعیت فروشندگان جهانی امنیت

جدول(۷) فروشندگان برتر جهانی محصولات امنیت اطلاعات را به همراه سهم بازار و امتیاز کیفی آنها معرفی کرده است.

جدول۷ نرخ کیفیت و سهم بازار محصول بر ای عرضه کنندگان اصلی محصولات امنیت اطلاعات جهان

محصول	نام شرکت برتر دنیا	درصد سهم بازار جهانی	امتیاز کیفیت (۱ تا ۵)
سیستمهای تشخیص نفوذ	Tripwire inc.	۱۶	۳,۹۴
سیستمهای جلوگیری از نفوذ	Stormwatch,OKENA	۶	۴,۶۳
فایروال	Software Technologies	۲۳	۴,۲۳
فایروال	Norton AV, Symantac	۳۸	۴,۲۴
VPN	Nokia	۷	۴,۱۸
مدیریت امنیت شبکه	Intellitactics	۹	۴,۶۴
مدیریت موجودیت	Clear Trust, RSA Security	۱۴	۴,۱۶
ارزیابی آسیب پذیری و نظارت بر امنیت	Retina, EEye Digital Security	۱۱	۴,۰۶
تصدیق هویت / نوع نرم افزار	SSH Secure Shell, SSH Communications	۲۶	۴,۱۷
تصدیق هویت/ نوع سخت افزار	Secure, RSA Security	۶۱	۴,۲۸

٤. بررسی وضعیت بازار امنیت اطلاعات در ایران

در عصر حاضر جامعه اطلاعاتی در جایگاه مهمترین بخش جامعه قرار خواهد داشت لذا زیرساختها و کاربردهای فناوری اطلاعات قابل اطمینان، مهمترین عامل برای رشد اقتصادی پایدار محسوب می شوند. زیر ساختهای بحرانی در جامعه با زیرساختهای محیط سایبر بهم پیوسته اند. کامپیوتر، مخابرات، منابع ذخیره جهانی در حال رشد هستند ولی متاسفانه به موازات آن حوادث امنیت کامپیوتر نیز الگوی رشدی مشابهی دارد. با این توصیف دیدگاه کنونی به امنیت اطلاعات ناکافی به نظر می‌رسد و فرمول خط مشی، چالشها و احتمالات مختلفی را دربرمی‌گیرد.

مطالعات انجام شده برای این مقاله حاکی از آن است که در حال حاضر حدود ۵۰ شرکت خصوصی و دولتی در زمینه امنیت اطلاعات در کشور فعالند ولی تقریبا هیچکدام در بازار جهانی سهمی ندارند. خوشبختانه تمام این شرکتها به اینترنت دسترسی داشته و دارای سایت هستند. از میان این ۵۰ شرکت تقریب ۴۱ شرکت در زمینه امنیت شبکه و سخت افزارهای آن و نرم افزارهای ضد ویروس کار می کنند و ۷ شرکت در زمینه مشاوره و آموزش سیستمهای مدیریت امنیت اطلاعات (ISMS) مشغول به کارند. با وجود اهمیت بسیار بالای وجود سیستم مدیریت امنیت اطلاعات برای سازمانها؛ هنوز پیاده سازی آن در ایران انجام نشده است. یکی از شرکتها نیز در زمینه امنیت فیزیکی و تجهیزات مربوط به ان فعال است. (جدول ۷ در پیوست آمده است).

در گزارش روزنامه ابرار اقتصادی در تاریخ ۵ اردیبهشت ۸۶، فرهنگ سازی در حوزه امنیت اطلاعات مهمترین اولویت کاری کمیسیون افتای کشور در سال ۸۶ تعیین شد و ۷ محور اصلی به عنوان برنامه کاری کمیسیون افتا در سال جاری مطرح شد که عبارتند از: شفاف سازی فعالیت های دولت در حوزه فناوری اطلاعات، تقویت کمی و کیفی تقاضا در بازار، تقویت بنیه اعضای سازمان نظام صنفی رایانه ای، اصلاح مقررات و شرایط حاکم بر بازار، افزایش توان سازمان سازمان مذکور، اطلاع رسانی و تلاش برای حفظ و ارتقاء جایگاه صنف امنیت. طبق گزارش ابرار اقتصادی ، به گفته دبیر کمیسیون افتا در سازمان نظام صنفی رایانه ای استان تهران در خصوص وضعیت پروژه های در دست اجرا شرکت ها ؛ متاسفانه در این مدت کارهای بسیار محدودی به بخش خصوصی واگذار شده است و علی رغم همه وعده های مسوولین مربوطه دولتی، نه تنها امنیت اطلاعات در کشور از جایگاه و ارزش مشخصی برخوردار نشده بلکه برخی از شرکت ها نیز با ارایه خدمات و سرویس هایی نامناسب، بازار این حوزه را به شدت تحت تاثیر عملکرد نامناسب خود قرارداده اند. ضمنا ایشان با توجه به ضرورت تحقق اجرای اصل ۴۴ قانون اساسی و سیاست های کلی نظام در خصوص توسعه و تقویت بنگاه های کوچک اقتصادی، خواستار توجه جدی متولیان امر به فرهنگ توسعه و به کارگیری فناوری اطلاعات و لحاظ نمودن امنیت اطلاعات در کشور شد.

نتیجه گیری

در این مقاله اهمیت امنیت اطلاعات در شبکه های ارتباطات جهانی و به تبع آن در تجارت و بازاریابی اینترنتی مورد بررسی قرار گرفته و مولفه ها و محصولات و خدمات امنیت اطلاعات معرفی شد . از آنجا که مبحث امنیت اطلاعات بعد از ظهور شبکه‌های جهانی و ارتباطات مبتنی بر آن در ادبیات علمی بطور مشخص مطرح شد و کشور ما هنوز از نبود یک شبکه و پرتال واحد دولت الکترونیک رنج می برد، مبحث امنیت این حوزه نیز از قدمت چندانی برخوردار نیست. تعداد شرکتهایی که در ایران با خدمات امنیت اطلاعات آشنا هستند بسیار محدود بوده و تعداد شرکتهایی که استانداردهای امنیت اطلاعات را آن هم در سطوح پایین پیاده سازی کرده‌اند در کشور ما از شمار انگشتان یک دست تجاوز نمی کند. از طرفی بررسیهای کشورهای مختلف در مقاله حاضر حاکی از آن است که دیگران گوی سبقت را در بازار جهانی امنیت اطلاعات از ما ربوده اند. لذا با توجه به اینکه پیاده سازی امنیت اطلاعات توسط دیگران در یک کشور از ریسک بالایی برخوردار است، پیشنهادات زیر برای ادامه تحقیقات در جهت فعال سازی بازار امنیت اطلاعات در ایران ارائه می شود:

۱. انجام تحقیقاتی عمیق در خصوص

الف)بررسی روند و نرخ بکارگیری محصولات و خدمات امنیت اطلاعات در سازمانهای ایرانی

ب) تعیین درصد سازمانهایی که به نظر می رسد نیاز به محصولات و خدمات امنیت دارند ولی تا پایان برنامه پنج ساله آینده برنامه‌ای برای استفاده از این محصولات ندارند به تفکیک محصول.

ج)درصد سازمانهایی که بطور شتابنده ای درصد بکارگیری محصولات و خدمات امنیت اطلاعات را در سازمانشان افزایش می دهند.

د) نرخ رشد ترکیبی سالانه محصولات و خدمات امنیت اطلاعات در ایران

ه)تهیه بانک اطلاعاتی فروشندگان محصولات امنیت اطلاعات در ایران و اولویت بندی آنها بر مبنای کیفیت و ارزش کاری از دیدگاه مشتری.

و) ملاحظات محصول: بررسی محصولات امنیتی تولید شده در ایران و تهیه بانک اطلاعاتی مربوطه و مقایسه با محصولات خارجی. از بررسی روند بودجه های امنیتی مدیریت شده در سازمانها به تفکیک اندازه سازمان در سالهای مختلف(خصوصی و دولتی)

ح)روند درصد بودجه امنیت اطلاعات نسبت به بودجه فناوری اطلاعات در سازمانها به تفکیک اندازه سازمان در سالهای مختلف

ط)روند خدمات امنیت (نرخ بکارگیری آنها، سازمانهایی که قصد بکارگیری آنها را ندارند و نرخ رشد سالانه آنها)

۲. انجام موارد بند ۱ در خصوص شرکتهای داخلی و مقایسه با رقبای خارجی.

۳. تجمیع و تنقیح قوانین و مقررات حوزه امنیت اطلاعات برای تعیین و پرکردن خلاء های قانونی توسط دولت.

۴. تسریع در فعالیتهای پیاده سازی دولت الکترونیک و به تبع آن سایر کاربردهای الکترونیکی.

۵. فرهنگ سازی در خصوص فعالیتهای شبکه محور .

۶. بررسی نفوذ امنیت اطلاعات در حوزه بازرگانی و بازاریابی محصول و ارائه درسهای مرتبط با این حوزه در دانشگاههای کشور.

منابع

Information Security Magazine, May ۲۰۰۳, PP. ۲۸-٤١ , www.Infosecuritymag.Com.

King, C. M., Dalton, C. E., & Osmanoglu, T.E., Security Architecture: Design, Deployment and Operations. London: Mcgraw-Hill, ۲۰۰۲.

Conway, s., & Sliger, C. , Building Taxonomies. In unlocking knowledge assets, Washington: Microsoft press, ۲۰۰۲, pp. ۱۰٥-۱۲٤.

هاشمیان، وحید. روش های رمزنگاری اطلاعات. رایانه شریف ۵(۸)، سال ۱۳۷۹،ص ۱۸-۲۱.

Lexico publishing group,LLC, ۲۰۰۲.
Information Security & Prevention of Computer Related Crime (Infosec), ۲۰۰۲.
Venter, h. S., & Eloff, j. H. P., Taxonomy for Information Security Technologies[Electronic version in Elsevier Database]. Computers & Security, vol. ۲۲(٤), ۲۰۰۳, *p.* ۲۹۹-۳۰۷.
Comer, D. E., Computer Networks and Intranets: With Internet Applications. New york: Prentice-Hall, ۲۰۰۲.
Encyclopedia and Learning Center., Techtarget Network: What is.Com. Retrieved June ۲۰۰٤, *from* http://whatis.Techarget.Com/definitionscategory./
Bace, r. G., Intrusion Detection. Indianapolis, in: Macmillan Technical Publishing, ۲۰۰۰.
*Mcclure, S., Scambray, J., & Kurtz, G., Hacking Exposed. (*۳*rd Ed.). London: Mcgraw-hill,* ۲۰۰۲.
Tiwana, A.,Web Security, Boston: Digital Press, ۱۹۹۹.
Oppliger, R., Internet & Intranet security. Boston: Artech House, ۱۹۹۸.
جعفری، م. ، مبانی امنیت فضای رایانه ای، نشر علوم پایه، تابستان ۸۵
Us Information Security Market by Product/Service, Freedonia, Feb ۲۰۰٤.
Sung_uk, P. and Hyun-woo, L.,The Study of Korean Information Security Applied Market, Internet Economy Research Team, Etri, www.Etri.Re.Kr ۲۰۰٤.
Chang Ch. and Lee, W., Taiwan: Focus on The Information Security Market, IEEE Computer Society, Sep./Oct. ۲۰۰۳.
Http://mic.Iii.Org.Tw.
W.R.JI, Outlook for information security, Last Chapter , CNET Business, http://taiwan.Cnet.Com/enterprise/trend/story/۰۰۲۰۰۰۰٤۰٤۷٤،۲۰۰۳٦۱٤۹-۲۰۰۰.Htm .
Http://www.Taipei.Org/official/۱۰۱۰۲۰۰۲/۱۰۱۰-۱.Htm.
Http://www.Trendmicro.Com.
The Institute For Information Industry MIC Rreport, Jan. ۲۰۰۳, *see at:* http://mic.Iii.Org.Tw/intelligence.
Http://www.Hitrust.Com.Tw/hitrustexe/frontend/default_tw.Asp.
Http://www.Taica.Com.Tw.
Http://www.Entrust.Net.Tw.

پي نـوشت

[۱] *Information security*
[۲] *Proactive*
[۳] *Reactive*
[٤] *Network Level*
[٥] *Host Level*
[٦] *Application Level*
[۷] *Cryptography:*
[۸] *Digital signatures:*
[۹] *Digital certificates:(*
[۱۰] *Virtual private networks*
[۱۱] *Vulnerability scanners*
[۱۲] *Anti- virus scanner*
[۱۳] *Security protocols*
[۱٤] *Security hardware*
[۱٥] *Security software development kits (SDKs:)*
[۱٦] *Firewalls*
[۱۷] *Access control:*
[۱۸] *Passwords:*
[۱۹] *Biometrics:*
[۲۰] *IntrusionDetection systems (IDS)*
[۲۱] *) Logging:(*
[۲۲] *) Remote Accessing*
[۲۳] *Platform*
[۲٤] *Server Accelerator Cards*
[۲٥] *Malicious*
[۲٦] *Government Agency*
[۲۷] *Public Corporation*
[۲۸] *Bank/ FinancialCcompanies*
[۲۹] *Private Companies doing business via online*
[۳۰] *General Private Comapines*
[۳۱] *Natural person Certificate*
[۳۲] *Stand-alone*
[۳۳] *Certificate authority*