شهر الکترونیک، امنیت اطلاعات و شهروندان

زهره فولادبند
fouladband@yahoo.com

۱- مقدمه

پیشرفت های تکنولوژیک در زمینه فناوری اطلاعات و ارتباطات، موجب خلق فضای مجازی شده اند. در این فضای مجازی و با استفاده از امکانات جدیدی که به دنیا ارائه شده، بسیاری از فعالیت های اقتصادی، اجتماعی، فرهنگی و حتی سیاسی شکل جدیدی به خود گرفته است. در حقیقت کاربردهای فناوری اطلاعات و ارتباطات در دگرگونی بخش های مختلف زندگی افراد و ارتباطات آنها مؤثر بوده است. با رشد روز افزون تکنولوژی ها و کارکردهای جدیدی که ارائه می شود و نیز با در نظر گرفتن نفوذ آن در دنیا، گریزی در استفاده از آن ها نیست. آنچه اهمیت دارد شناخت صحیح فرصت های جدیدی است که فناوری اطلاعات و ارتباطات در اختیار ما قرار داده و البته چالش ها و ریسک هایی که از فرصت ها جدایی ناپذیرند. یکی از ریسک ها و مخاطرات انکارناپذیر دنیای مجازی، موضوع امنیت اطلاعات است. از دست دادن امنیت اطلاعات و یا به خطر افتادن آن ممکن است به قدری خسارت بار باشد که اساس استفاده از مزایای فناوری اطلاعات و ارتباطات را به چالش بکشد.

شهر الکترونیک از دستاوردهای دنیای مجازی است و فرصت های جدیدی برای تعاملات اقتصادی و اجتماعی به شهروندان، کسب و کارها و دولت ارائه می دهد. همانطور که اشاره کردیم این فرصت ها همراه با ریسک ها و مخاطراتی است از جمله کلاهبرداری های مالی و از بین رفتن محرمانگی داده ها. نگرانی از این مخاطرات نباید مانع بکارگیری امکانات شهر الکترونیک شود بلکه باید برای آن اقدام کرد. نقش شهروندان در تامین امنیت اطلاعات قابل توجه است. شهروند الکترونیک با استفاده از دانش و مهارت کافی در زمینه مقابله با آسیب پذیری های امنیتی، بخوبی می تواند از امکانات شهر الکترونیک استفاده کند.

۲- گسترش شهرهای الکترونیک

امروزه بسیاری از شهرها، شهر الکترونیک شده اند و تعاملات از طریق شبکه ها صورت می گیرند، مثل بسیاری فعالیت های تجاری، بهداشتی، آموزشی و خدماتی که با امکانات الکترونیکی موجود انجام می شوند. مزایای الکترونیکی شدن از جمله سرعت و دقت بالاتر و کاهش هزینه های سربار باعث گسترش شهرهای الکترونیک شده است. اینترنت بعنوان یکی از مهمترین فاکتورهای رشد شهرهای الکترونیک، در حال گسترش و نفوذ در زندگی مردم عادی است. برای نشان دادن نرخ رشد سریع اینترنت و کاربردهای مبتنی بر آن کافی است نگاهی به آمارها داشته باشیم:

- اینترنت هر ده الی دوازده ماه از نظر حجم دو برابر می شود و تعداد ارتباطات خانگی و دفترهای کوچک کاری در حال افزایش است.
- رشد اینترنت در دنیا روندی صعودی دارد. البته شیب این رشد در مناطق مختلف دنیا متفاوت است. آفریقا و آسیا در حال حاضر بیشترین شیب را دارند.
- یک فاکتور مهم در ارزیابی میزان استفاده از اینترنت در کشورها، ضریب نفوذ است. ضریب نفوذ اینترنت در دنیا در حال حاضر ۱۵.۷ در صد و در کشور ما حدود ۱۱ در صد است. این ضریب در آمریکای شمالی ۶۸.۶ درصد و در اروپا ۳۶ در صد است.
- آمار رشد تجارت الکترونیک در سال ۲۰۰۴ نشان می دهد آمریکا با ۴۷ در صد، بیشترین سهم تجارت الکترونیک را در دنیا دارد. پس از آن ژاپن با ۱۳ در صد و آلمان با ۵.۷ در صد قرار دارند.

از آنجایی که بسیاری از فرایندها در دنیا از طریق شبکه ها و بخصوص شبکه اینترنت انجام می شوند(مثل پست الکترونیک یا وب سایت ها) ، حتی اگر شهری رسماً بصورت الکترونیکی اداره نشود، شهروندان آن به سمت الکترونیکی شدن خواهند رفت. بنابر این بهتر است برای کنترل چنین روندهایی و نیز کاهش اثرات منفی استفاده از کاربردهای جدید دنیای فناوری اطلاعات و ارتباطات، مشکلات را شناسایی کرد و با تحلیل و بررسی های همه جانبه، تهدیدات را کاهش داد. ضمن اینکه برای استفاده بیشتر از تکنولوژی های موجود برنامه ریزی نمود. امنیت اطلاعات یکی از موضوعات چالش برانگیز شهر الکترونیک است.

آمار مشکلات امنیت اطلاعات نیز مثل رشد کاربردهای آن روندی صعودی دارد و حتی هر روز شکل جدیدی از آسیب ها به وجود می آید. خسارات مالی ایجاد شده نیز قابل توجه هستند. حوزه حفاظت سیستم های اطلاعاتی همگام با رشد سریع فناوری اطلاعات و ارتباطات حرکت نکرده است و با سرعت زیاد بکارگیری تکنولوژی های اطلاعات در سازمان ها همگام نبوده.

در گذشته امنیت اطلاعات با اعمال سیستم های نظارتی و حضور فیزیکی تأمین می شد ولی امروزه از ابزارهای خودکار و مکانیزم های هوشمند برای حفاظت داده ها استفاده می شود. امروزه ابزارهای حمله فراوان شده و گاهی استفاده از آنها نیز ساده تر گشته است.

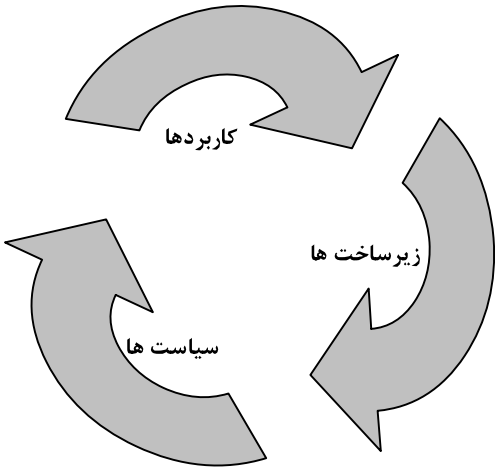
یکی از مهمترین عوامل که باعث خسارت به سیستم های اطلاعاتی می شود، اشتباهات انسانی هستند. نبود آموزش های مناسب و به روز نبودن اطلاعات شهروندان و گاهی سهل انگاری و بی توجهی آنان می تواند باعث به خطر افتادن امنیت اطلاعات در شهرهای الکترونیک باشد.

۳- چالش های امنیت اطلاعات در شهر الکترونیک

شهر الکترونیک بخش مهمی از ساختار دولت الکترونیک است و به معنی شهری است که از سرویس های الکترونیکی برای فعالیت ها و ارائه خدمات بهره می برد.

به خاطر وجودسیستم های اطلاعاتی مختلف، کاربرد دسترسی های از راه دور اطلاعات، اشتراک اطلاعات و وجود داده های محرمانه و حساس شهروندان و کسب و کارها در شهر الکترونیک، موضوع امنیت اطلاعات را نمی توان ساده گرفت. شهر الکترونیک باید دسترسی امن به اطلاعات، کاربردها و سرویس ها را برای تمام کاربران ایجاد نماید. برای رعایت امنیت اطلاعات در شهر الکترونیک نیاز به ترکیبی مناسب از مسائل حقوقی، اجتماعی و فنی است.

بلوک های اصلی شهر الکترونیک عبارتند از: زیر ساخت ها، کاربردها و سیاست ها(شکل یک). دستیابی به امنیت اطلاعات در شهر الکترونیک، با اجرای برنامه های امنیتی در بلوک های اصلی امکان پذیر است. مشکلات امنیتی موجود در این بلوک ها، آسیب های امنیت اطلاعات را ایجاد می کنند. مسئولیت بخش عمده ای از زیرساخت ها و سیاست ها در شهر الکترونیک، وابسته به دولت ها است و بررسی مسائل امنیتی در این بخش، از برنامه های دولت ها محسوب می شود.



شکل یک

۳-۱ - امنیت اطلاعات

امنیت اطلاعات به معنی محافظت از سیستم های اطلاعاتی در مقابل تلاش های افراد غیر مجاز برای دسترسی به اطلاعات یا دستکاری اطلاعات می باشد. طبق تعریف استاندارد ISO 17799 امنیت اطلاعات به معنی حفاظت و نگهداری از محرمانگی (Confidentiality)، جامعیت (Integrity) و در دسترس بودن (Availability) اطلاعات است. محرمانگی یعنی اطلاعات فقط برای کاربران مجاز قابل دسترسی است. جامعیت یعنی اطلاعات فقط توسط کاربرانی که مجازند و به روش های مجاز قابل دستکاری و تغییر است. و قابلیت دسترسی یعنی استفاده از سیستم برای کاربران مجاز هیچگاه قابل منع نیست.

امروزه اطلاعات بعنوان یک سرمایه مهم باید نسبت به حملات محافظت شود. میزان تلاش هر سازمان برای این محافظت وابسته به ارزش سرمایه های آن سازمان و تهدیداتی است که ممکن است اتفاق بیفتد.

منظور از تهدیدات، مشکلات بالقوه موجود در زیر بنای امنیتی یک سیستم است. تهدیدات امنیتی را می توان به چهار دسته تقسیم کرد:

۱. قطع یا وقفه (Interruption) : اختلال در شبکه و سرویس
۲. دزدی یا شنود (Interception) : استراق سمع ارتباطات شخصی یا محرمانه
۳. دستکاری داده ها (Modification) : تغییر غیر مجاز داده های سیستم و یا شبکه
۴. جعل داده ها (Fabrication) : ارسال داده توسط کاربران غیر مجاز با نام کاربران مجاز

منظور از حمله‌ها عملیاتی است که برای اعمال تهدیدات انجام می پذیرد. حمله های امنیتی به دو گروه فعال و غیر فعال تقسیم می شوند.

حمله های فعال عبارتند از :

۱. جعل هویت
۲. تکرار پاسخ
۳. تغییر محتوای پیام
۴. اختلال در سرویس

حمله های غیر فعال عبارتند از:

۱. انتشار محتوای پیام
۲. تحلیل ترافیک

۳-۲ - جرایم الکترونیکی

برخی افراد با نیت خرابکاری یا سوء استفاده مثلاً سوء استفاده مالی اقدام به اجرای حمله های امنیتی می کنند. به این اقدامات جرایم الکترونیکی می گوییم. هدف ایجاد امنیت اطلاعات در شهر الکترونیک جلوگیری از وقوع این جرایم و کاهش اثرات منفی آنها است. سابقه جرایم الکترونیک به سابقه استفاده از کامپیوترها بر می گردد. آنچه تازگی دارد گسترش وسیع تجهیزاتی است که توان محاسباتی و ارتباطی بالایی دارند و در انواع فعالیت های اجتماعی و اقتصادی در شهرهای جدید، بصورت یک رکن اصلی مورد استفاده قرار می گیرند. امروزه حجم وسیعی از اطلاعات مهم در شبکه ها جریان دارند و تعداد بسیار زیادی کاربران مختلف که عمدتاً هیچ آموزشی در زمینه امنیت ندیده اند. هر شهروند در شهر الکترونیک مجاز

است از زیر ساخت های اطلاعاتی بعنوان یک امکان عمومی استفاده نماید و همین واقعیت است که منجر به بروز جرایم الکترونیکی در شهرهای الکترونیک می شود.

شایع ترین جرایم در زمینه امنیت اطلاعات در شهرهای الکترونیک عبارتند از: حملات ویروس ها، دسترسی غیرمجاز، دزدی اطلاعات محرمانه و خصوصی افراد و مسائل مربوط به کامپیوترهای قابل حمل.

۴- برقراری امنیت اطلاعات در شهر الکترونیک

برای ایجاد سیستم های امن باید نیازمندیها و مشخصات امنیتی سیستم شناسایی و تعریف شود. با بررسی دقیق جنبه های امنیتی سیستم و نقاط ضعف و آسیب پذیری های امنیتی، می توان تحلیل ریسک را انجام داد و بعد با برآورد هزینه و اولویت بندی، یک سیاست امنیتی طرح کرد. برای اجرای سیاست امنیتی طرح شده احتیاج به تهیه راه حل امنیتی داریم. با انتخاب مکانیزم ها و تکنولوژی های امنیتی که با نیازهای امنیتی ما متناسب هستند، راه حل را پیاده سازی می کنیم. بخش مهم دیگر سیاست امنیتی دستورالعمل ها و کنترل های مربوط به کارکنان و کاربران است. همچنین باید برای تست، ارزیابی و برآورد امنیت سیستم، معیارهایی داشته باشیم و فرایند ارزیابی امنیت را در بازه های زمانی مناسب تکرار کنیم.

بطور کلی می توان گفت برای پیاده سازی و اعمال امنیت اطلاعات در شهر الکترونیک مثل هر سیستم دیگری وابسته به سه عامل اصلی هستیم:

۱- افراد و عوامل اجرایی ۲- سیاست ها و روال ها ۳- تکنولوژی ها

۱. افراد و عوامل اجرایی

خطاهای انسانی منشأ بسیاری از آسیب پذیری های امنیتی هستند. افرادی که آموزش کافی در زمینه امنیت اطلاعات داشته باشند، می توانند در موقعیت های حساس عکس العمل مناسب نشان دهند. همچنین با آموزش می توان از ابزارهای امنیتی موجود بهتر استفاده کرد. البته افراد و عوامل اجرایی در شهر الکترونیک دارای نقش های متفاوت هستند. بنابراین قدرتمندی و آگاهی و آموزش آنها نیز در زمینه امنیت اطلاعات متفاوت است. بسیاری از کشورهای پیشرفته دنیا برای آموزش و آگاهسازی کاربران وکارکنان برنامه های دقیق تنظیم می کنند. امروزه در سازمان ها برای آموزش های امنیتی سرمایه گذاری می شود.

۲. سیاست ها و روال ها

برای مواجهه با آسیب پذیری های امنیتی در شهر الکترونیک باید قوانین و مقررات امنیتی تنظیم گردد طوری که متناسب با نیازها و ویژگی های جدید شهرهای الکترونیک باشد. این قوانین و مقررات از سوی دولت در بخش های مختلف اقتصادی و اجتماعی قابل بررسی است. قوانین مربوط به جرائم الکترونیکی، حقوق مصرف کنندگان و قوانین تجارت الکترونیک از مهم ترین آنها هستند. همچنین سازمان ها و کسب و کارهای خصوصی که از شبکه ها و سیستم های اطلاعاتی استفاده می کنند دارای سیاست امنیتی هستند. اجرای سیستم های مدیریت امنیت اطلاعات و پیاده سازی استانداردهای مربوطه مثل ISO17799 برای سازمان ها ضروری است. حتی خانواده ها و شهروندان الکترونیک نیز برای کاهش آسیب های امنیت اطلاعات، برای خود و خانواده سیاست ها و روال های امنیتی در نظر می گیرند مثل کنترل های والدین روی استفاده کودکان از کامپیوتر و اینترنت.

۳. تکنولوژی ها

تکنولوژی های امنیتی هر روز جدیدتر می شوند. استفاده از آخرین تکنولوژی های ارائه شده به معنی بالا بردن ضریب امنیت سیستم نیست بلکه انتخاب درست و استفاده مناسب از تکنولوژی ها است که با کمک متخصصان و کارشناسان این حوزه، امنیت سیستم را بالا می برد. در تکنولوژی های امنیتی از مکانیزم های امنیتی مختلف استفاده می شود. منظور از مکانیزم امنیتی، مکانیزمی است که برای کشف، جلوگیری و رفع و بازسازی یک حمله امنیتی طراحی شده است مثل مکانیزم های رمزنگاری، تصدیق اصالت و کنترل دسترسی. علاوه بر تکنولوژی های امنیتی، به منظور تضمین کارایی وضعیت امنیت سیستم از تکنیک هایی برای ارزیابی کارایی امنیت استفاده می شود مثل سیستم های تشخیص نفوذ و نرم افزارهای مانیتورینگ.

شهر الکترونیک بخش های مختلفی دارد: بخش های دولتی، کسب و کارهای خصوصی و شهروندان عادی. رعایت امنیت در شهر الکترونیک باید در تمام بخش ها وارد شود.

بخش های دولتی مثل شهرداری سرویس های مورد نیاز شهروندان و کسب و کارها را ارائه می دهند و حجم وسیعی از جریان داده ها در شبکه ها از همین سرویس ها و کاربردها ایجاد می شود. بنابراین هنگام طراحی شبکه ها و سرویس های بخش های دولتی، امنیت فاکتور مهمی است. بکارگیری کارشناسان و متخصصان امنیت اطلاعات، انتخاب و استفاده از تکنولوژی های امنیتی روز، تدوین دستورالعمل ها و روال های امنیت اطلاعات در بخش های مختلف از سوی مدیریت و انجام ممیزی و بازبینی امنیتی بصورت دوره ای، برای بهبود وضعیت امنیت اطلاعات در سازمان ها، گام های اصلی هستند.

کسب و کارهای خصوصی نیز در حوزه امنیت اطلاعات مشابه بخش های دولتی اما در مقیاسی متفاوت فعالیت دارند. امن ماندن اطلاعات کسب و کار و اعتماد مشتریان یک مزیت مهم رقابتی است.

از سوی دیگر شهروندان بعنوان یکی از مهم ترین بخش های شهر الکترونیک با آگاهی و دانش خود و استفاده از ابزارهای امنیتی موجود می توانند سهم خود را در امنیت اطلاعات شهر الکترونیک حفظ کنند.

۵- شهروند الکترونیک و امنیت اطلاعات

"به زودی اگر یک شهروند الکترونیک نباشید، اساساً شهروند به حساب نمی آیید."

این عبارت، پیام استاندارد آموزشی "شهروند الکترونیک" است که توسط بنیاد بین المللی ICDL ارائه شده. شهروند الکترونیک کسی است که توانایی لازم برای کار با یک کامپیوتر را داشته باشد و بتواند از اینترنت برای انجام سریع تر و مؤثرتر کارهای زندگی روزمره از قبیل برقراری ارتباط با دیگران، خرید و فروش، تعاملات بانکی، استخدام، مسافرت، تفریح، سرگرمی، پزشکی و ... استفاده کند. در بسیاری کشورهای پیشرفته، شهروندان الکترونیکی شده اند.

شهروندان نقش بسیار مهمی در توسعه شهرهای الکترونیک دارند. پیشرفت شهر الکترونیک مبتنی بر اعتماد و اطمینانی است که شهروندان نسبت به کاربردهای الکترونیکی شهر الکترونیک دارند. در صورتی که اطمینان به سیستم ها و روش ها داشته باشند و نیز آموزش و آگاهی کافی نسبت به روال ها و فرایندهای مربوط به شهر الکترونیک داشته باشند، بصورتی فعال و مؤثر یک شهروند الکترونیک می شوند. از طرفی امنیت یک شهر الکترونیک وابسته به مشارکت و همکاری تمام شهروندان است. به همین خاطر باید شهروندان قدرتمند شوند تا بعنوان یک بخش فعال در شهر الکترونیک، به حفظ امنیت اطلاعات کمک کنند.

بنیاد بین المللی ICDL با تدوین استاندارد "شهروند الکترونیک"، یک برنامه آموزشی برای قدرتمند کردن شهروندان عادی برای حضور در شهرهای الکترونیک ارائه کرده است. این برنامه در سه بخش تهیه شده و بطور کلی دارای ده فصل می باشد. بخش اول: مهارت های پایه فناوری اطلاعات و ارتباطات، بخش دوم: جستجوی اطلاعات و ایمن سازی در وب و بخش سوم: مشارکت الکترونیکی/شهروند الکترونیکی در عرصه عمل. عنوان فصل هفتم که در بخش دوم ارائه شده، هشدارهای امنیتی است. در این فصل با معرفی برخی آسیب پذیری ها و مشکلات امنیت اطلاعات که پیش روی یک شهروند الکترونیک است، سعی شده راهکارهایی برای کاهش این مشکلات بطور اجمالی بیان شود.

شهروند الکترونیک پس از گذراندن این بخش از آموزش باید نسبت به این موارد توانمند شده باشد:

۱. درک مشکلات و خطرات ایمیل های ناخواسته و قدرت انجام اقدامات پیش گیرانه

دریافت ایمیل های ناخواسته به تعداد زیاد، موجب صرف وقت هنگام بررسی پیام ها می شود و نیز به دلیل احتمال آلوده بودن آنها به ویروس های کامپیوتری، ایجاد مشکل و دردسر می نماید. گرچه پیشگیری کامل و صد در صد ایمیل های ناخواسته ناممکن است اما روش هایی برای کاهش آن وجود دارد. اغلب این روش ها شامل بکاربستن توصیه ها است و البته استفاده از سیستم های نرم افزارهای.

۲. درک مشکلات و خطرات ویروس ها و قدرت انجام اقدامات پیش گیرانه

ویروس ها برنامه های کامپیوتری کوچکی هستند که امکان انتشار دارند و روی سیستمهای کامپیوتری اثرات مخرب دارند. از آنجا که اینترنت امکان دسترسی به فایل ها و اطلاعات را از هر جایی امکان پذیر می کند، احتمال آلودگی به ویروس نیز بیشتر می شود. با استفاده از نرم افزارهای آنتی ویروس، می توان ویروس ها را کنترل و حذف نمود. نکته مهم اینکه نرم افزارهای آنتی ویروس باید مرتبا به روز شوند.

۳. درک نیاز به دسترسی امن به اینترنت و شناخت برخی تکنیک های پیاده سازی امنیت

اینترنت به خاطر ماهیت باز بودن آن و نداشتن مرجع مشخصی برای کنترل و پاسخگویی محتوا، ذاتا محیط امنی نیست. بنابراین برای کاهش خطرات و آسیب ها بخصوص در مورد سازمان ها و شرکت ها از تکنیک هایی استفاده می شود. دیوارآتش ابزاری برای مقابله نرم افزاری و سخت افزاری در برابر تهاجمات اینترنتی است. بعد از نصب دیوارآتش، هر ارتباطی با اینترنت بطور خودکار از طریق آن انجام می شود.

۴. درک خطر امنیتی ارائه اطلاعات محرمانه و شخصی در اینترنت و قدرت انجام اقدامات پیش گیرانه

ارائه اطلاعات شخصی و محرمانه مثل آدرس یا جزئیات مربوط به کارت اعتباری به سایت های نامطمئن، منجر به بروز مشکلات مختلف از جمله خسارات مالی می شود. همچنین به دلیل ماهیت مجازی اینترنت، ممکن است افراد آنچه ادعا می کنند نباشند، بنابر این در اتاق های گپ زنی باید هوشیار بود.

۵. شناخت حقوق مصرف کنندگان و قوانین حفاظتی برای خریدهای اینترنتی

تجارت از طریق اینترنت علاوه بر مزایای آن همراه با پیامدهای منفی نیز می باشد. اثبات ادعای فروشندگان و تصدیق اصالت آنها موضوع مهمی است. همچنین باید اطلاعاتی در مورد تسهیلات همراه با خریدها، قوانین حقوق مصرف کننده (که ممکن است در هر کشوری متفاوت باشد) و درستی تبلیغات و ضمانت های فروشندگان داشت تا بتوان درست تصمیم گرفت.

۶. درک ماهیت غیر رسمی و غیر معتبر وب سایت ها و خطرات ناشی از اطلاعات گمراه کننده و غیر قابل اطمینان

سایت ایمن سایتی است که بتوان بدون نگرانی با آن ارتباط برقرار کرد و تبادل اطلاعات نمود. امنیت وب سایت ها با استفاده از مکانیزم ها و تکنیک های پیچیده امنیتی مثل رمزنگاری و ... حاصل می شود اما یک شهروند الکترونیک لازم نیست این تکنیک ها را بشناسد بلکه برای بررسی رسمیت یک وب سایت نکات و توصیه هایی وجود دارد که با بکاربستن آن ها می توان خطرات را کاهش داد.

۷. درک مشکلات و خطرات دسترسی کنترل نشده کودکان به اینترنت و قدرت اعمال کنترل های مناسب برای دسترسی به وب.

بسیاری از اطلاعات موجود در اینترنت برای کودکان نامناسب هستند مثل موضوعات مربوط به مسائل جنسی و خشونت. با بکاربستن توصیه ها و دستورالعمل های کارشناسان و نیز شناخت و استفاده مناسب از ابزارهای نرم افزاری موجود می توان مشکلات را کم کرد تا کودکان نیز بتوانند بصورتی امن از امکانات دنیای مجازی استفاده نمایند.

اهمیت این بخش بخصوص در کشورهایی مثل کشور ما بدلیل دارا بودن ویژگی های خاص فرهنگی و مذهبی، بیشتر است و البته اندکی متفاوت خواهد بود.

۶- نتیجه گیری

برای بهره بردن از امکانات شهرالکترونیک، تا حد امکان باید آسیب ها را کاهش دهیم. امنیت اطلاعات از مهمترین آسیب پذیری های هر سیستمی است. تکنولوژی ها و روال های امنیت اطلاعات متناسب با رشد سریع کاربردهای اطلاعاتی و ارتباطاتی، پیشرفت نکرده اند و بسیاری از کاربردها و سرویس ها بدون در نظر گرفتن امنیت طراحی شده و توسعه یافته اند. شهر الکترونیک بعنوان یک کاربرد وسیع و گسترده که سرویس های مهمی به شهروندان، دولت و کسب و کارها ارائه می دهد و داده های محرمانه و مهمی را در حجم زیاد پردازش کرده و انتقال می دهد، بدون رعایت امنیت اطلاعات اساساً غیر مفید و حتی زیان بار خواهد بود. عوامل اجرایی، سیاست ها و تکنولوژی ها پایه های اصلی ایجاد امنیت در شهر الکترونیک هستند. شهروندان که بخش عمده عوامل اجرایی هستند نقش قابل توجهی در حفظ امنیت اطلاعات دارند. سرمایه گذاری و برنامه ریزی برای ایجاد آگاهی و دانش کافی و تسلط به ابزارهای امنیتی برای شهروندان الکترونیک گام بزرگی برای دستیابی به امنیت اطلاعات شهر الکترونیک است.

مراجع

[1] David R. Wilkinson, “Protection and Security of Citizens in the Information Society”, Institute for the Protection and Security of the Citizen,2001, www.itas.fzk.de .
[2] T.M.RAO, “Network and Information Security Standards in e-Governance”, eGov Standards workshop Hyderabd, 2006.
[3]Poh-Chuan, “e-Goveranancee Boosts Productivity & Wealth of Asia Nations”, 2007, www.sda-asia.com.
[4] Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson, ”CSI/FBI COMPUTER CRIME AND SECURITY SURVEY”, Computer Security Institute. 2006.
[5]Farhad Foroughi, “eCity as an eGonernment Approach”, 2005, www.negarmedia.com/papers/e-goverment.
[6] Narasimha Reddy,Riccardo Bettati,Andreas Klappenecker,” Topics in Network Security”,2006, www.ece.tamu.edu
[7] “e-Citizen Syllabus Version 1.0”,The European Computer Driving Licence Foundation Ltd.,2004
[8] “INTERNET USAGE STATISTICS”,www.internetworldstats.com,2006
[۷] متواضع، مرتضی، “شهروند الکترونیکی”، موسسه فرهنگی هنری دیباگران تهران، ۱۳۸۴