

دولت الکترونیک در ایران، سندرم سامانه‌ها و دردهای پنهان دیگر

دولت الکترونیک در سال‌های گذشته با توسعه نامتوازن و بدون برنامه روبرو شد و موجب بروز مشکلات مختلف همچون سندرم سامانه و دردهای پنهان دیگر شد. کنترل دسترسی، تصدیق هویت، عدم انکار، محرمانگی، امنیت ارتباطات، جامعیت داده، در دسترس‌پذیری و حفظ حریم خصوصی از اهداف مهم امنیت در شبکه‌ها است و باید به گونه‌ای طراحی شود که دسترسی به هر یک نباید مانعی برای دسترسی به سایر اهداف باشد. به‌عنوان مثال ما نمی‌توانیم به دلیل امنیت ارتباطات و یا حفظ حریم خصوصی در دسترس‌پذیری اطلاعات را با اختلال مواجه کنیم.

به گزارش خبر شرکت ملی پست، مهدی گمرکی؛ کارشناس تجارت الکترونیک اداره کل پست استان اصفهان در مطلبی به چگونگی فعالیت سامانه‌های مختلف ارائه خدمات دولت الکترونیک در ایران و چالش‌های پیش رو پرداخته است. متن این یادداشت را در ادامه بخوانید. چند سالی است یکی از گفتمان‌های مهم شکل گرفته در همه نهادهای دولتی و بخش‌های خصوصی روند پیشرفت استقرار دولت الکترونیک بوده است. روندی که به نظر می‌رسد هرگز با یک برنامه جامع توسعه نیافته است و بیشتر بر مبنای بخشنامه و سایر موارد به‌صورت جزیره در دستگاه‌های مختلف به نحوی عملیاتی شده است. توسعه‌ای که به دلیل نداشتن برنامه جامع به مرور امنیت مردم را با مخاطرات جدی مواجه کرده است. گاه‌وبیگاه پیام‌هایی با موضوع کلاهبرداری و در آن‌سو پیامک‌های هشدار پلیس فتا و سایر نهادها با موضوع هوشیار شدن مردم نشان از عمق فاجعه‌ای است که در پس رشد بی‌برنامه و غیرعلمی دولت الکترونیک رخ داده است.

و این روند قطعاً با حضور سامانه‌های مختلف ارائه خدمات دولت الکترونیک که به‌صورت جزیره‌ای شکل گرفته است بیشتر خواهد شد. رشد سامانه‌های دولت الکترونیک که می‌توان به آن سندرم سامانه را اطلاق کرد باعث شده مردم در جهت انجام هر یک از خدمات خود در هر سازمانی به یک سامانه اختصاصی مراجعه کنند و در هر بار استفاده از این سامانه‌ها ملزم به احراز هویت بدون رعایت استانداردهای خاص می‌شوند. آنچه برای مردم بیشتر از هر چیزی ملموس است نام‌های کاربری و رمز عبور متعدد جهت استفاده از هریک از این سامانه‌هاست، اما در پس این اتفاق مخاطرات بزرگ امنیتی مخفی شده است که اصولاً به آن توجهی نمی‌شود.

این اتفاق (سندرم سامانه) به دلایل مختلفی رخ داده است که مهمترین آن بی‌برنامه بودن توسعه دولت الکترونیک، نداشتن یک حکمران مرکزی برای مدیریت و استقرار دولت الکترونیک در کشور و عدم همکاری نهادهای مختلف در کشور به دلیل کلیدواژه استقلال سازمانی، از قوا مختلف کشور گرفته تا نهادها و حتی وزارتخانه‌های دولت است.

این پدیده در آینده نه‌چندان دور می‌تواند تبعات جبران‌ناپذیری به همراه داشته باشد که مهم‌ترین آن سوءاستفاده کلاهبرداران از بی‌اطلاعی‌های فنی مردم و کلاهبرداری به نام سامانه‌های دولتی همانند آنچه امروز از طریق پیامک اتفاق می‌افتد، است.

بعد از مشکل سندرم سامانه که طبعاً تمام اهداف امنیتی به‌خصوص کنترل دسترسی، تصدیق هویت، عدم انکار و محرمانگی را تحت تأثیر قرار می‌دهد باید به مشکل دیگر توسعه دولت الکترونیک که اتفاقاً مهمترین مانع توسعه دولت الکترونیک است، پرداخت.

متأسفانه ناآگاهی مدیران از مقوله امنیت اطلاعات در سال‌های اخیر باعث شده است یکی از مهمترین اصول اساسی دولت الکترونیک که براساس چارچوب تعامل‌پذیری دولت الکترونیک یا EGIF تعریف شده است را با اشکالات جدی مواجه کند و آن اصل مهم مقوله‌ای است با عنوان Openness یا باز بودن داده‌ها است که به مواردی همچون دسترسی آسان و امکان مشارکت همه و عدم کنترل توسط گروهی خاص اشاره دارد.

یکی از مهمترین خروجی‌های Openness در چارچوب تعامل‌پذیری دولت استفاده اکوسیستم کسب‌وکار در ایجاد مزیت برای داده‌های موجود در سازمان‌هاست که در نهایت می‌تواند به خلق سرویس‌های جدید و ثروت برای بخش خصوصی ایجاد شود، اما متأسفانه به بهانه امنیت داده اکوسیستم از این سرمایه مهم محروم می‌ماند.

و البته یکی از مهمترین موانع توسعه دولت الکترونیک در ایران شاید مانع نیروی انسانی و مدیریتی باشد که مهمترین دلیل آن می‌تواند ترس از دست دادن موقعیت شغلی و یا عناوین باشد، که در خصوص این مقوله باید به‌صورت جداگانه و تفصیلی پرداخته شود.

و اما چه باید کرد؟

در گام اول باید همانند اتفاقی که در واگذاری اختیارات دولت در قالب اصل ۱۳۸ به وزارت ارتباطات باهدف توسعه اقتصاد دیجیتال افتاد برای بحث مهم دولت الکترونیک نیز یک نهاد فرا قوه‌ای با اختیارات جامع و کافی به‌عنوان رأس برنامه‌ریزی دولت الکترونیک در کشور قرار بگیرد و مصوبات آن توسط تمام دستگاه‌ها و نهادها اجرا شود.

یک سیستم مرکزی احراز هویت و احراز نشانی برای ارائه خدمات در دولت الکترونیک شکل بگیرد. در متون بالا اشاره کردیم که متأسفانه آنچه امروز در فرآیند احراز هویت اتفاق می‌افتد، کاملاً ناقص و دارای حفره‌های امنیتی بسیار زیادی است. متأسفانه یکی از مهمترین مولفه‌های احراز هویت افراد در دولت الکترونیک که نشانی محل سکونت و یا محل اشتغال شهروندان است در این فرآیند مورد بررسی قرار نمی‌گیرد و می‌تواند منبع اصلی بسیاری از تخلفات کلاهبرداران در آینده باشد. همچنین امروز نیز بانک‌ها و بسیاری دیگر از ارائه‌دهندگان سرویس با چنین پدیده‌ای مواجه شده‌اند و با خیل زیادی از کلاهبرداران دارای نام و نشان ولی بدون آدرس پستی روبرو شده‌اند.

این سیستم مرکزی احراز هویت و نشانی باید دارای راهکارهای جامع برای شناسایی افراد و تأیید محل سکونت آنها باشد. براساس قانون در حال حاضر شرکت ملی پست به‌عنوان نشانی افراد به‌صورت کاملاً الکترونیکی و از طریق پروژه ملی GNAF به ارائه سرویس احراز آدرس می‌پردازد و از سوی دیگر سازمان ثبت احوال نیز خدمات جامع احراز هویت را می‌تواند به این مرکز ارائه کند.

بنابراین اگر پروژه‌های دولت الکترونیک به‌صورت فازبندی عملیاتی شود درنهایت بر اساس برنامه توسعه به ساختار ارائه خدمت از طریق پنجره واحد دولت الکترونیک دست می‌یابیم.

آنچه بیان شد بخشی از مشکلات و راهکارها بود و می‌توان با حضور نخبگان علمی و اداری کشور موضوع دولت الکترونیک را در کشور با سرعت به سرانجام برسانیم.